T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ETHERCAT TABANLI İÇME SUYU SİSTEMİ ÜZERİNDE MITRE ICS SALDIRI SİMÜLASYONU VE TESPİTİ

YÜKSEK LİSANS TEZİ

Firdevs Sevde TOKER

Enstitü Anabilim Dalı	**:**	**BİLGİSAYAR VE BİLİŞİM MÜHENDİSLİĞİ**
Tez Danışmanı	**:**	**Prof. Dr. İbrahim ÖZÇELİK**

Temmuz 2020

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ETHERCAT TABANLI İÇME SUYU SİSTEMİ ÜZERİNDE MITRE ICS SALDIRI SİMÜLASYONU VE TESPİTİ

YÜKSEK LİSANS TEZİ

Firdevs Sevde TOKER

Enstitü Anabilim Dalı : BİLGİSAYAR VE BİLİŞİM MÜHENDİSLİĞİ

Bu tez 29.07.2020 tarihinde aşağıdaki jüri tarafından oybirliği / oyçokluğu ile kabul edilmiştir.

Prof. Dr.	**Prof. Dr.**	**Dr. Öğr. Üyesi**
Resul KARA	**İbrahim ÖZÇELİK**	**Murat İSKEFİYELİ**
Jüri Başkanı	**Üye**	**Üye**

BEYAN

Tez içindeki tüm verilerin akademik kurallar çerçevesinde tarafımdan elde edildiğini, görsel ve yazılı tüm bilgi ve sonuçların akademik ve etik kurallara uygun şekilde sunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, tezde yer alan verilerin bu üniversite veya başka bir üniversitede herhangi bir tez çalışmasında kullanılmadığını beyan ederim.

Firdevs Sevde TOKER

29.07.2020

TEŞEKKÜR

Yüksek lisans eğitimim boyunca değerli bilgi ve deneyimlerinden yararlandığım, her konuda bilgi ve desteğini almaktan çekinmediğim, araştırmanın planlanmasından yazılmasına kadar tüm aşamalarında yardımlarını esirgemeyen, teşvik eden, aynı titizlikte beni yönlendiren değerli danışman hocam Prof. Dr. İbrahim ÖZÇELİK'e teşekkürlerimi sunarım.

Bu süreçte değerli tecrübe ve desteğini her zaman paylaşan hocam sevgili Arş. Gör. Dr. Kevser OVAZ AKPINAR'a teşekkür ederim.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

ADS	: Otomasyon Cihazı Özellikleri
AoE	: EtherCAT üzerinden ADS
API	: Uygulama Programlama Arayüzü
APT	: Gelişmiş Kalıcı Tehdit
BT	: Bilgi Teknolojileri
CPU	: Merkezi işlem birimi
CSRF	: Siteler arası istek sahteciliği
CSV	: Virgülle Ayrılmış Değerler
C&C	: Komut ve Kontrol Sunucusu
DCS	: Dağıtılmış kontrol sistemleri
DMZ	: Arındırılmış Bölge
DNP3	: Dağıtılmış Ağ Protokolü
DoS	: Servis Dışı Bırakma
EAP	: EtherCAT Otomasyon Protokolü
EKS	: Endüstriyel Kontrol Sistemleri
ELK	: Elasticsearch, Logstash, Kibana Yığını
HIDS	: Host Tabanlı Saldırı Tespit Sistemi
HMI	: İnsan makine arabirimi
IDE	: Akıllı elektronik cihaz
IDS	: Saldırı tespit sistemi
IP	: Internet Protokol
MITM	: Aradaki adam
OPC	: Açık Platform İletişimi
OT	: Operasyonel teknoloji
PLC	: Programlanabilir lojik kontrolör
POU	: Program organizasyon birimi

RAT	: Uzaktan erişim truva atı
RTU	: Uzak terminal birimi
SCADA	: Merkezi denetleme kontrol ve veri toplama
SIEM	: Güvenlik bilgileri ve olay yönetimi
SIS	: Güvenlik Enstrümanlı Sistemler
SVM	: Destek Vektör Makinesi
SQL	: Yapılandırılmış Sorgu Dili

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar kelimeler: Endüstriyel kontrol sistemleri, saldırı tespit sistemi, MITRE ICS ATT&CK Matrisi

Endüstriyel kontrol sistemleri, içerdiği teknoloji ve protokol çeşitliliğinden dolayı karmaşık sistemlerdir. Ancak kritik sistemler olduğundan olası herhangi bir saldırı durumunda yıkım etkisi de aynı oranda büyük olmaktadır. Bu yüzden kritik alt yapıların siber saldırılara karşı korunması ve sürekli izlenebilirliği önemli ve gereklidir.

EKS çalışma yapısı olan OT, standart bilişim alt yapısından farklı performans ve güvenlik gereksinimlerine sahiptir. EKS sistemler, operasyonel süreçlerin gerçekleştiği saha cihazları ve bu cihazların yönetimini sağlayan kontrol sistemlerinden oluşmaktadır. Saldırganlar kontrol katmanından erişim sağladıktan sonra bütün sürece dahil olmaktadırlar. Bu durumun sonucu olarak kritik alt yapı sistemleri siber saldırılara karşı tehdit altındadır. Dolayısıyla sürekli izleme ve güvenlik denetimleri, kritik alt yapılar için de gerekli bir süreçtir.

Bu çalışmada, kritik alt yapılardan biri olan su yönetim prosesi üzerinde siber saldırı ve tespit sistemine yönelik çalışmalar yapılmıştır. EtherCAT tabanlı çalışan su yönetim prosesi üzerinde saha cihazlarına yönelik toplamda 6 farklı saldırı vektörü MITRE ICS ATT&CK matrisindeki tekniklere göre geliştirilmiş ve bu saldırılar ağ trafiğinden elde edilen veriler ayrıştırılarak SVM algoritmasıyla tespit edilmiştir. Aynı proses üzerinde mühendislik bilgisayarı aracılığıyla kontrol merkezindeki SCADA sistemine yapılan saldırılarda ise MITRE ICS ATT&CK matrisinde bulunan 7 farklı teknik seçilerek saldırı senaryoları oluşturulmuştur. SCADA sistemine yönelik saldırı tespit sistemi için Wazuh HIDS kullanılmıştır. Her iki saldırının görselleştirilmesi ELK üzerinde yapılmıştır.

MITRE ICS SIMULATION AND INTRUSION DETECTION ON ETHERCAT BASED DRINKING WATER SYSTEM

SUMMARY

Keywords: Industrial control systems, Intrusion detection system, MITRE ICS ATT&CK Matrix

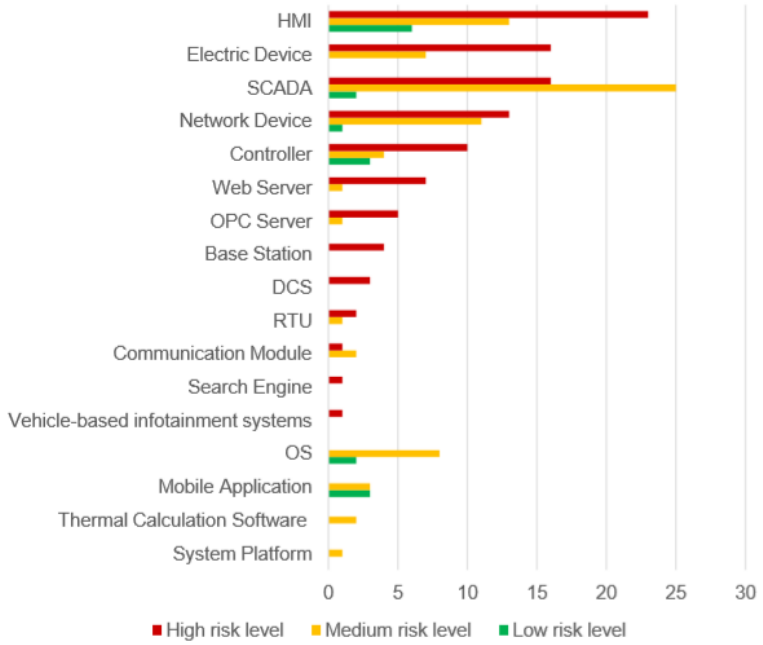
Industrial control systems are complex systems due to the technology and protocol diversity they contain. However, since there are critical systems, the destruction effect is equally great in any possible attack. Therefore, the protection and traceability of critical infrastructures against cyber attacks are important and necessary.

OT, which has an EKS operating structure, has different performance and security requirements than the standard IT infrastructure. EKS systems consist of field devices where operational processes take place and control systems that provide management of these devices. Attackers are involved in the whole process after gaining access from the control layer. As a result, critical infrastructure systems are threatened by cyber attacks. Therefore, continuous monitoring and security audits are also a necessary process for critical infrastructures.

In this study, studies on cyber attack and detection system were carried out on water management process, which is one of the critical infrastructures. On the EtherCAT based water management process, 6 different attack vectors for field devices were developed in accordance with the techniques in the MITRE ICS ATT&CK matrix, and these attacks were separated by data obtained from network traffic and determined by the SVM algorithm. Attack scenarios were created by selecting 7 different techniques in the MITRE ICS ATT&CK matrix for attacks on the SCADA system in the control center via the engineering computer on the same process. Wazuh HIDS was used for the intrusion detection system for the SCADA system. Visualization of both attacks was done on ELK.

BÖLÜM 1. GİRİŞ

Endüstriyel kontrol sistemleri, endüstriyel sektörlerde ve kritik altyapılarda sıklıkla bulunan çeşitli kontrol sistemlerini kapsayan genel bir terimdir [1]. Bu sistemler genel olarak kullanıcıların güvendiği fiziksel süreçlerin verimli otomasyonunu sağlayan sistemlerdir [1]. Hava trafik kontrolü, elektrik ve nükleer santraller, atık su arıtma tesisleri, rafineriler, boru hatları ve barajlar gibi dünyanın kritik altyapısının büyük bir yüzdesini bu sistemler yönetmektedir [2]. Endüstriyel kontrol sistemleri standart bilgi teknolojileri (BT) alt yapısı ve çalışma prensibinden farklı olarak operasyonel teknoloji (OT) alt yapısını kullanmaktadır. Farklı alt yapıların getirdiği güvenlik yönetimi ve riskleri de aynı oranda farklılık göstermektedir. EKS ağları fazlasıyla heterojen ortamlardır. Bu durumun sonucu olarak da ortamda birçok çeşit yazılım, donanım platformu ve protokol bulunmaktadır [3]. Dolayısıyla güvenlik süreçlerinin yönetimini de aynı oranda karmaşıklaştırmaktadır. Bu durumun bir sonucu olarak siber saldırılara karşı savunma düzeyleri düşüktür ve hedef odaklı saldırılarda açık hedef haline gelmektedir. 2015 yılında Kaspersky tarafından yapılan bir araştırmada [4] endüstriyel kontrol sistemlerdeki bileşenlerin tipine göre güvenlik zafiyetlerinin risk seviyelerinin dağılımı Şekil 1.1.'de belirtilmiştir.



Şekil 1.1. EKS bileşenlerinin güvenlik zafiyetlerine göre risk seviyeleri [4]

Şekil 1.1.'de en çok risk altında olan bileşenlerden, HMI cihazına ait açıklıklar; ara bellek taşmaları (buffer overflow), iletişimde hassas bilgilerin şifrelenmeden açık bir şekilde iletilmesi gibi sömürülmeye açık yapılar bulunmaktadır. Bir diğer yüksek risk altındaki bileşenlerden biri olan SCADA sistemlerine ait açıklıklar; XSS, ara bellek taşmaları (buffer overflow), CSRF, sınırlandırılmamış dosya yükleme ve SQL Injection saldırıları gibi farklı tipte saldırılar mevcuttur [4].

Kurumlar, kritik alt yapıların ilk kullanımında bütün sistemleri izole bir şekilde yönetmişlerdir; ancak bu durum zamanla büyüyen endüstri için zahmetli ve maliyetli bir süreç olmaya başlamıştır. Üretim ve operasyonel maliyetleri azaltma, üretkenliği artırma ve gerçek zamanlı bilgilere erişim sağlama gereksinimlerinin artması, kuruluşların EKS'yi iç ve dış ağlarla birbirine bağlamak için modern ağ sistemlerini kullanma yolunda ilerlemelerinin temel nedenlerinden bazıları olmuştur. Bu eğilim, EKS ağlarında daha önce bulunan yalıtımı azaltarak kritik altyapıyı çok çeşitli iç ve dış tehditlere, yanlış yapılandırmalara ve bilgi işlem hatalarına karşı savunmasız kalmasına neden olmuştur [2].

EKS çalışma yapısı olan OT alt yapısı, BT alt yapısından farklı performans ve güvenlik gereksinimlerine sahiptir. Başlıca farklılıklar, OT sistemler çalışma ortamı olarak daha yüksek riskli yerlerdir. Bu ortamda sisteme dahil olan bir yazılım veya donanımın entegrasyonu, güvenlik testlerinin uyumluluğu sırasında oluşabilecek zararlar yer almaktadır. OT sistemlerde meydana gelebilecek herhangi bir aksama sürecin kritikliğine bağlı olarak BT sistemlerde yaşanan aksamaya göre daha hayati olumsuzluklara yol açmaktadır. OT sistemlerin güvenlik denetimini sağlamak için gerekli personel ihtiyacı BT sistemlere göre daha fazladır. Çünkü OT sistemler karmaşık ve standart bilişim alt yapısından farklı çalışma tipinde cihazlar olduğundan bu sistemleri önce öğrenmek gerekmektedir. OT personellerinin ise güvenlik farkındalıkları ve sistemin güvenlik kontrollerinin sağlıklı yapılabilmesi için yeterli bilgi ve tecrübeye sahip olması gerekmektedir. IBM tarafından yapılan bir araştırmada [5], 2019 yılında OT siber güvenlik saldırılarında yüzde 2.000'lik bir artış olduğunu göstermektedir. Operasyonel kurumlar ve endüstriler ağ yapılarını genişlettikçe, saldırganlar için yeni atak yüzeyleri oluşmaktadır. Bu risklerin azaltılmasına yardımcı olmak için kurumlar, operasyonel teknoloji güvenlik stratejisi belirlemeli ve periyodik olarak güvenlik süreçlerini yeni saldırılara göre güncellemelidirler.

17 Aralık 2016 yılında büyük elektrik kesintisi yaşandığı Ukrayna'da "*Crashoverride*" zararlı yazılımının sebep olduğu doğrulanmıştır. *Dragos* güvenlik firmasının incelemesine göre [6], zararlı yazılım, elektrik dağıtımını bozmak için birkaç EKS protokolüne özgü saldırı yükünü (payload) dağıtmak için tasarlanmış modüler bir zararlı yazılım yapısındadır. Bir EKS bileşenini etkilemesi ve modüler bir yapıda olması aslında sürecin karmaşık ve yönetiminin zahmetli olduğunu ofansif tarafta da göstermektedir. Bu saldırı enerji sektörüne yönelik ikinci saldırıdır. Birinci saldırı Bölüm 2.4 içerisinde detaylı aktarılan Stuxnet saldırısıdır. Tüm bu saldırılar hem insana yönelik hem de devletlere yönelik maliyet açısından oldukça zarar vermektedir.

2019 yılında Fortinet tarafından yayınlanan rapora göre [7]; EKS piyasasının hızla büyüdüğü ve küresel EKS pazarının tek başına 2014'te 58 milyar dolardan 2021'de

81 milyar dolara çıkacağını; 2015 ile 2021 arasında yıllık %4,9 büyüme oranıyla büyüyeceğini öngörüyorken, EKS'ye grafik kullanıcı arayüzü olarak hizmet veren SCADA yazılımları ise yıllık %6,6 büyüme oranında büyüdüğü belirtilmektedir. Ciddi yatırımların beraberinde getirdiği kolaylıklar işlevselliği arttırmaktadır. Ancak IT ve OT sistemlerin kesişimi söz konusu olduğundan güvenlik riskini de beraberinde getirmektedir. Bu risk verilen yetkilerin kullanım kolaylığı açısından geniş tutulması ve üçüncü parti yazılımların sistemlere dahil olmasıyla oluşmaktadır. Fortinet raporunda, her 10 kuruluştan 6'sı ortaklarına ya da devlet kuruluşlarına tam veya üst düzey erişim sağladığı belirtilmektedir. Aynı raporda kurumların EKS/SCADA sistemleri için aldığı önlemler de belirtilmiştir. Kuruluşların risklere karşı aldığı bir dizi önlemler, %70'inin tüm ağ trafiğini sürekli olarak günlüğe kaydedip analiz ettiğini ve bunun %24'ünün mevcut güvenlik analizi dağıtımlarını genişlettiği bildirilmiştir. Yaklaşık üçte ikisi ağ güvenlik kontrolleri uygulamakta ve %62'si parmak izi veya yüz tanıma gibi biyometrik tabanlı güvenlik kontrolleri kullanmaktadır. Tüm bu önlemlere rağmen güvenlik denetimi kontrol edilmeyen, güvenli iletişim alt yapısının yeterli denetlenmemesinden kaynaklanan en az bir güvenlik zafiyeti bile saldırganların hedeflerine ulaşmalarına fırsat vermektedir. Bu yüzden kırmızı takım çalışmalarıyla güncel saldırı vektörleri kullanılarak kurumların güvenlik zafiyetleri raporlanmalı ve mavi takımlar çalışmalarıyla da güvenlik açıklıkları kapatılmalıdır.

Tez çalışmasında saldırı vektörlerinin belirli tekniklere dayandırılarak uygulanmasını sağlayan MITRE ICS ATT&CK matrisi kullanılarak örnek senaryolar oluşturulmuştur. ICS matrisi 7 Ocak 2020 itibariyle sunulduğu için bu alanda henüz kapsamlı bir çalışma bulunmamaktadır. Oluşturulan saldırıların tespitine yönelik saha cihazları ve SCADA sistemleri olmak üzere iki farklı tespit yöntemi geliştirilmiştir. Uç sistemlere yapılan saldırılar makine öğrenmesi yöntemiyle tespit edilirken, SCADA sistemine ait saldırılar Wazuh HIDS ile tespit edilmektedir.

Kritik alt yapılı sistemlerde kırmızı ve mavi takımın da kullanabileceği, Purdue mimarisi temel alınarak oluşturulan MITRE ATT&CK ICS matrisi saldırılara yönelik çeşitli teknikler sunmaktadır. MITRE ATT&CK ICS matrisi herkese açık

olduğundan kötü niyetli kullanıcılar için de oldukça önemli bir kaynak oluşturmaktadır. Bölüm 2.3 içerisinde daha detaylı aktarılan matris, uygulanacak saldırı tekniğinin hangi amaçla, hangi cihazlara yapılabileceğine kadar detaylı içerikler sunmaktadır. Kırmızı takımlar için kapsamlı APT saldırı senaryoları, saldırı tekniklerini gerçekleştirmek için kullanıcıya komut satırı veya arayüz sağlayan CALDERA [8], metasploit [9], Purple Team ATT&CK Automation [10], Atomic Red Team [11] gibi araçlarla oluşturup gerçekleyebilme olanakları mevcuttur. Mavi takımlar için de benzer şekilde kendi sistemlerinin güvenlik durumlarını test etmek amacıyla aynı yöntemler kullanarak çıkan sonuçlar doğrultusunda sistem üzerinde gerekli sıkılaştırma ve güvenlik kontrollerinin yapılandırılması gözden geçirilebilir. Bu tür sistemlerde periyodik aralıklarla rapor tutmak ileride oluşabilecek olağandışı durumlar ve sistemin değerlendirilmesi açısından da oldukça önemli ve gereklidir.

1.1. Literatür Araştırması

Bu bölümde endüstriyel kontrol sistemlerine yapılan saldırıların önlenmesine yönelik çalışmalar ve makine öğrenmesi yöntemleriyle tespitine göre iki farklı başlıkta literatürde yer alan çalışmalara yer verilmiştir.

1.1.1. EKS'ne yapılan saldırıların tespitine yönelik çalışmalar

BT sistemlerde, Saldırı tespit ve engelleme sistemleri genel olarak uç sistemler ve ağ tabanlı sistemler olarak iki kategoride çalışmaktadır. Ancak EKS'de uç sistemler SCADA olarak kabul edilirse bu sistemlere yapılan saldırıların düşük *false positive* oranıyla tespiti için farklı anomali kontrollerinin yapılması zorunluluğunu ortaya çıkarmaktadır. Shitharth ve Winston bu soruna çözüm olarak gelişmiş izinsiz giriş tespiti ve sınıflandırma sistemi sunmuşlardır [12]. Bu çalışmada SCADA ağındaki saldırıları doğru bir şekilde sınıflandırmak için Hiyerarşik Nöron Mimarisi tabanlı Sinir Ağı (HNA-NN) sınıflandırma tekniği geliştirmişlerdir. Önerilen sistemin performansını değerlendirmek için bu sistemde güç sistemi saldırı veri seti kullanmışlardır. Siber fiziksel yapının bir diğer güvenlik zafiyetinin bulunduğu nokta SCADA sistemlerinin ağ yapısından izole olduğu düşünülerek göz ardı edilen kimlik

doğrulama mekanizmalarının denetimsizliğinden kaynaklanmaktadır. Güçlü parola yönetimi ya da kimlik doğrulama alt yapısının güvenli ve periyodik olarak denetlenmemesi, kurumsal ağa başarılı bir şekilde giren saldırganın, sömürebileceği açıklıklar arasında yer almaktadır. Zhang ve ark., SCADA sistemleri için PT-IDS adlı bir saldırı tespit sistemi (IDS) önermişlerdir. Önerilen bu sistemde, tipik SCADA sistemlerindeki periyodikliği ve ağ telemetri modellerini araştırarak dört farklı çeşit saldırının tümünü tespit etmek için etkili bir mekanizma kurmuşlardır; alarmları kritik, yüksek, orta ve düşük olmak üzere dört öncelik seviyesine göre otomatik önceliklendirmeye yönelik bir yaklaşım sunarak yöneticilerin sorunları ve çözümlerini yorumlamaları için sezgisel bir yol sağlamayı amaçlamışlardır [13]. Bu yaklaşımla uygulanan simülasyon sonucuna göre *false negative* oranı %0,37; *false positive* oranı ise %0,72 başarı oranına ulaşmışlardır. Ullah ve ark., SCADA ağları için anomali tabanlı saldırı tespit ve özellik seçimi için hibrit bir model önermişlerdir. Önerilen modelin amacı saldırı tespit oranını arttırmaktır. Önerilen teknik, basitleştirilmiş bir özellik alt kümesi nedeniyle düşük bir hesaplama ve zaman karmaşıklığına sahiptir [14]. Kritik alt yapıların önemli bileşenlerinden biri olan akıllı enerji şebekelerine yönelik saldırıların tespiti hayati önem taşımaktadır. Birçok tespit sisteminin çalışma prensibi saldırıların belirli kriterlere göre sınıflandırılması olumlu sonuçlar oluşturmaktadır. Ferrag ve ark., akıllı şebekelere yapılan saldırı girişimlerinde kullanılan saldırıları anahtar tabanlı (key-based), veri tabanlı (data-based), yetkili kişi bilgileri elde edilerek yetkiyi kötüye kullanma ve fiziksel tabanlı saldırılar olmak üzere 4 farklı sınıflandırma içerisinde alt saldırıları da oluşturmuşlardır [15]. Saldırı tespit sistemlerinde manuel geliştirilen yöntemler olmakla birlikte var olan açık kaynak kodlu saldırı tespit ve önleme sistemleri kullanılarak da yeni saldırı tespit sistemi yaklaşımı geliştirilebilir. Granat ve ark., EtherCAT tabanlı bir sistemde, ilk olarak potansiyel saldırı vektörleri tanımlamışlardır. Bu saldırıları tespit etmek için açık kaynaklı saldırı tespit sistemi olan Snort, EtherCAT için bir dizi önişlemci ile genişletilerek EtherCAT tabanlı sistemlere yapılan saldırıların tespiti için ihtiyaç duyulan kuralların yazılması için araç geliştirilmiştir [16]. Ovaz Akpınar, yaptığı doktora çalışmasında EtherCAT protokolü kullanılan bir SCADA sisteminde bilinen ve bilinmeyen saldırıların tespitine yönelik kural ve anomali tabanlı çözüm yöntemi sunmuştur [17]. Al-Shaer

ve ark., MITRE ATT&CK matrisini kullanarak TTP zincirinde çeşitli teknikler arası bağımlılıkları temsil eden hiyerarşik kümelenme teknolojisini kullanan yeni bir yaklaşım geliştirmişlerdir. %95 doğruluk oranı ile saldırı davranışının öngörülebilirliğini destekleyen teknik ilişkilerini bulmaktadır [18].

1.1.2. SCADA sistemlerde makine öğrenmesi tabanlı anomali tespitine yönelik çalışmalar

Son zamanlarda IT sistemler üzerinde de sıkça kullanılan makine öğrenmesi yöntemleri oldukça efektif sonuçlar vermektedir. Yüksek doğruluk oranlara sahip yöntemlerle maliyet ve zaman işlevselliğinden dolayı sıkça tercih edilen yöntemlerden biri olmuştur. Makine öğrenmesi ve yapay zeka teknikleri, EKS'ye adanmış akıllı ve verimli bir Saldırı Tespit Sistemi (IDS) oluşturmak için yaygın olarak kullanılmaktadır. Bununla birlikte, araştırmacılar genellikle halka açık veri kümelerinden elde edilen ağ verilerini kullanarak makine öğrenmesi tabanlı güvenlik sistemlerini geliştirmektedirler [19]. Kötü amaçlı yazılımların gelişimi ve saldırı stratejilerindeki değişiklikler nedeniyle, bu veri kümeleri sistemi yeni saldırı türlerinden koruyamaz ve sonuç olarak karşılaştırma veri kümeleri periyodik olarak güncellenme zorunluluğunu getirmektedir.

SCADA sistemlere yönelik yapılan saldırıların tespitinde de gerek ağ üzerinden gerek sistem üzerinden ilgili verilerin doğru algoritmalarla kullanılarak düşük *false positive* oranıyla oldukça olumlu sonuçlar alınabilmektedir.

Endüstriyel kontrol sistemleri için anomali tespiti, sistem işleyişindeki normal olayların parametreleriyle beraber davranışların tanımlanması ile ilgilidir [20]. Bu anormallikler, saha cihazlarını kontrol eden kontrol cihazlarına, ağa veya fiziksel ortama saldırılardan kaynaklanabilir, aynı zamanda, operatör hatalarından veya iletişim ve prosesin işleyişini sağlayan yazılımdaki standart hatalardan kaynaklanabilir [20]. Inoue ve ark., anormal durum tespiti için denetimsiz makine öğreniminin siber fiziksel sistemlerin modellerinin oluşturulup uygulanmasını araştırmışlardır. Gözetimsiz makine öğrenmesinin avantajı, hedef CPS'nin

karmaşıklıklarının anlaşılmasını gerektirmemesidir; bunun yerine, yalnızca tarihçilerden normal olarak elde edilebilen veri günlüklerinden modeller oluşturur [20]. Bu modeller iki denetimsiz yöntemle uygulama yapılıp karşılaştırılmıştır: İlk olarak, bir Derin Sinir Ağı (DNN); ikincisi, anomali tespiti için yaygın olarak kullanılan bir *one-class* Destek Vektör Makinesi (SVM) algoritmalarını kullanmışlardır. Ovaz Akpınar ve Özçelik, EtherCAT tabanlı sistemlerde makine öğrenme yöntemlerinin anomalilerin varlığını ve türünü belirlemedeki başarısı ve performansı değerlendirilmiştir. 16 atak çeşidinin test edildiği çalışmada ANN, karar ağacı (DT), SVM GA, k-NN makine öğrenmesi algoritmaları kullanılmıştır ve tahmin sonuçlarının başarı oranları sırasıyla; %98,28, %98,17, %99,81, %100,00 elde edilmiştir [17]. Teixeira ve ark., SCADA test ortamından normal ve anormal ağ paketlerini yakalayıp test verilerini oluşturarak makine öğrenmesi algoritmalarının fizibilite çalışmasını sunmuşladır. Tespit için veri setinin kullanıldığı Random Forest, Karar Ağacı, Lojistik Regresyon, NaïveBayes ve KNN algoritmalarının verimliliğine yönelik çalışma yapmışlardır [19]. Wang ve ark., güç şebekesine yapılan siber saldırıların, temel olarak sistemdeki davranışları tespit etmek için geçmiş verileri ve ilgili log bilgilerini, öğrenme verisi olarak kullanmışlardır. Çalışmada kullanılan gözetimsiz öğrenmenin, sıfırıncı gün saldırıları tespit etmede eğitme işlemi gerektirmediğinden avantajlı, ancak öğrenmenin yüksek *false positive* oranına sahip olacağını belirtmişlerdir [21]. Yang ve ark., SCADA sistemler için ağ tabanlı siber saldırı ilkelerini tespit eden evrişimli sinir ağı (CNN) kullanarak derin öğrenme tabanlı bir ağ saldırı tespit sistemi (IDS) önermişlerdir [22]. Alhaidari ve AL-Dahasi, SCADA sistemlerine Dağıtılmış Servis Dışı Bırakma (DDoS) saldırılarını tespit etmek için makine öğrenimi tekniklerini kullanan bir simülasyon çerçevesi aracılığıyla olası bir güvenlik çözümü sağlamaya yönelik çalışma gerçekleştirmişlerdir. J48, Naif Bayes, saldırı düzenlerini belirlemek için Rastgele Orman olarak üç makine öğrenimi algoritmasını kullanmışlardır [23]. Robles-Durazno ve ark., SCADA sistemlerine odaklanmakta ve temiz su tedarik sisteminde anormallik tespiti için denetimli enerji izleme tabanlı makine öğrenme yaklaşımı sunmaktadır [24]. Perez ve ark., çeşitli IDS sınıflayıcılarını uygulamak için SVM ve RF algoritmalarını kullanmışlardır. Bu algoritmalar arasında rastgele hiper-parametre arama sonuçları ile bir karşılaştırma çalışması yapmışlardır [25].

1.2. Çalışmanın Amacı ve Geliştirilen Çözüm Yöntemi

Tez kapsamında, kritik altyapılı sistemlerde kullanılan EtherCAT tabanlı bir içme suyu prosesi sisteminde hem saha cihazlarına hem de SCADA sistemine yönelik saldırı vektörleri oluşturularak tespitine yönelik sistem geliştirilmiştir. MITRE ICS ATT&CK matrisi 7 Ocak 2020'de sunulmuştur. Bu süreç içerisinde planlanan saldırı vektörleri henüz var olan MITRE ICS ATT&CK matrisine göre teknikler belirlenip ilgili saldırı senaryoları oluşturulmuştur.

Bu çalışmaların aşamaları şöyle listelenebilir:

a) Her saldırı için su sistemi prosesinin kullanılarak test ortamının yazılımsal ve donanımsal olarak hazırlanması
b) Kritik alt yapı sistemlerinde yaygın olarak kullanılan EtherCAT protokolünün fabrika iletişiminin incelenmesi
c) Saha cihazlarından olan PLC cihazlarının yapılandırma modlarının değişmesini sağlayan kodun geliştirilmesi
d) Su prosesindeki tank seviyelerinin EAP iletişimi üzerinden manipüle ederek yanlış motorların çalışmasına sebep olarak sistem bütünlüğünü bozan saldırı vektörünün geliştirilmesi
e) C ve D maddelerindeki saldırıların tespitine yönelik SVM algoritması kullanılarak makine öğrenmesi yöntemiyle tespit eden programın geliştirilmesi
f) Su prosesinde çalışan sistemde, senaryoya bağlı motorların çalışma durumlarının değiştirilmesine neden olan saldırı vektörünün geliştirilmesi
g) Oluşturulan saldırıların tespiti ve görselleştirilmesi için Wazuh HIDS, Sysmon ve ELK Stack araçlarının entegrasyonunun sağlanması

1.3. Tez Organizasyonu

Yapılan çalışmanın sunulduğu tez, aşağıdaki biçimde yapılandırılmıştır.

Bölüm 1: Giriş, problemin tanımı, çalışmanın amacı ve tez organizasyonu hakkında bilgi sunulmaktadır.

Bölüm 2: Endüstriyel İletişim Sistemleri ve İlişkili Çalışmalar, endüstriyel iletişim sistemlerine yönelik çalışmalar EtherCAT protokolü, makine öğrenmesi tabanlı anomali tespiti çalışmaları, Wazuh HIDS saldırı tespit sistemi ve MITRE ICS ATT&CK matrisi genel bir bakış açısı ile sunulmaktadır.

Bölüm 3: Su prosesinde fabrika seviyesi iletişimi kullanılarak test ortamı ve saldırı vektörlerinin geliştirilmesi, SVM algoritması kullanılarak makine öğrenmesi yöntemiyle tespiti sunulmaktadır.

Bölüm 4: MITRE ICS ATT&CK matrisi kullanılarak bazı APT ataklarında da kullanılan tekniklerle su prosesine yönelik saldırı senaryolarının gerçekleştirilmesi ve Wazuh HIDS ile alarmların üretilerek ELK Stack yapısında görselleştirilmesi sunulmaktadır.

Bölüm 5: Yapılan çalışmalardan elde edilen sonuçlar belirtilmiş ve bunlar üzerine değerlendirmelere yer verilerek yapılan çalışmanın gerek bilime gerekse endüstriye getireceği katkılar tartışılmıştır.

BÖLÜM 2. TEORİK ARKA PLAN

2.1. Endüstriyel Kontrol Sistemleri ve Güvenlik

Endüstriyel kontrol sistemlerindeki varlıklar, özel uygulamalar çalıştırabilen Windows iş istasyonlarından analog giriş ve çıkışlara sahip gömülü cihazlara kadar sistemde işlevsel her şeyi kapsamaktadır [1]. Tüm varlıkların kendileriyle ilişkili platformları vardır, ancak çoğunlukla amaca yönelik gömülü sistemler için hangi platformların kullanıldığı her zaman açık değildir [1]. Benzer ürün sınıflarına sahip iki üretici veya aynı satıcının farklı ürün sınıfları arasında, temeldeki platformlar önemli ölçüde farklılık gösterebilmektedir. Örneğin, İnsan Makine Arayüzü (HMI) uygulamaları birçok platformda (Windows, Linux, Android vb.) çalışabilir. Bununla birlikte, temel platformdan bağımsız olarak, HMI'lerin operatörlere endüstriyel süreci izlemek ve kontrol etmek için bir arayüz sağlaması beklenmektedir. Ancak hangi üreticinin desteklediğine bağlı olarak bu varlığın kullanımı ve entegrasyonu farklılık göstermektedir. EKS ortamlarında yaygın olarak kullanılan varlıklar ve işlevleri şöyle listelenebilmektedir:

a. Kontrol Sunucu (Control Server) [1]: Hem sunucu hem de denetleyici işlevi gören ve ICS ağındaki (örneğin RTU'lar ve PLC'ler) alt seviye kontrol cihazlarıyla iletişimde kullanılan kontrol yazılımını barındıran bir cihazdır.

b. Veri Tarihçisi (Data Historian) [26]: İstatistiksel süreç kontrolü ve diğer teknikler kullanılarak arşivleme ve analiz için kullanıcı veri erişimini destekleyen kontrol sistemi DMZ'de kurulu bir bilgisayarda bulunan merkezi bir veritabanı işlevi görmektedir.

c. Mühendislik İş İstasyonu (Engineering Workstation) [26]: Genellikle kontrol sistemi uygulamalarının ve diğer kontrol sistemi ekipmanlarının konfigürasyonu veya bakımı için tasarlanmış üst seviye bir makinedir. Sistem genellikle yedek sabit disk sürücüleri, yüksek hızlı ağ arabirimi, güvenilir CPU'lar, performans grafik donanımı ve sistem değişikliklerinin kontrol sistemi uygulama geliştirme, derleme ve dağıtımını yapmak için yapılandırma ve izleme araçları sağlayan uygulamalardan oluşur.

d. Alan denetleyicisi/PLC/RTU/IED [26]: RTU veya PLC olarak adlandırılan denetleyiciler, genellikle modüler işleme ve arabirim kartlarıyla rafa veya panele monte edilen bilgisayarlı kontrol birimleridir. Üniteler, çeşitli sensörlere ve kontrollü cihazlara giriş ve çıkış modülleri aracılığıyla proses ekipmanı ve arayüz ile yerleştirilir. Birçoğu, I/O arayüz modüllerine veya I/O arayüz modüllerinden veri tarama ve yazma sağlayan, seri ve ağ iletişimi de dahil olmak üzere çeşitli iletişim yöntemleri aracılığıyla kontrol sistemi ağı ile iletişim kuran programlanabilir mantık tabanlı bir uygulama kullanır.

e. İnsan-Makine Arayüzü (Human-Machine Interface) [26]: Bilgisayar bilimi ve insan-bilgisayar etkileşimlerinde, İnsan Makine Arayüzü (HMI), programın bilgisayar monitörleri ve alt sistemleri kullanarak kullanıcıya (operatöre) sunduğu grafiksel, metinsel ve işitsel bilgileri bilgisayar klavyesi, bilgisayar faresinin hareketleri ve dokunmatik ekranla seçimler yaparak kullanıcının programı kontrol edilmesini sağlar. Sistem, farklı kullanıcı türlerine hizmet etmek için çeşitli kullanıcı arayüzlerini ortaya çıkarabilir. Kullanıcı arayüzü ekranları, operasyon kullanıcılarına, mühendislik kullanıcılarına ve yönetim kullanıcılarına uygun bilgi ve kontrol arayüzünü sağlayacak şekilde optimize edilebilir. HMI türleri en yaygın olanlar:

a) Grafik kullanıcı arabirimleri (GUI), bilgisayar klavyesi ve fare gibi aygıtlar aracılığıyla girişi kabul eder ve bilgisayar monitöründe eklemli grafik çıkışı sağlar.

b) Web tabanlı kullanıcı arabirimleri, ağ üzerinden taşınan ve kullanıcı tarafından bir web tarayıcı programı kullanılarak görüntülenen web sayfaları oluşturarak girişi kabul eder ve bu girişe göre çıktı sağlar.

- Giriş/Çıkış Sunucusu (Input/Output Server) [26]: Giriş/Çıkış (G/Ç) sunucusu, kontrol sistemi LAN uygulamaları ile kontrol sistemi uygulamaları tarafından izlenen ve kontrol edilen saha ekipmanı arasındaki arabirimi sağlar.
- Güvenlik Enstrümanlı Sistem/Koruma Rölesi [1]: Güvenlikle çalışan bir sistem (SIS), bir tesisi güvenli bir durumda tutmak veya anormal koşullar mevcut olduğunda onu güvenli bir duruma getirmek için otomatik işlem yapar. SIS, tesisinizdeki çeşitli proses tehlikelerine karşı koruma sağlamak için tek bir fonksiyon veya birden fazla fonksiyon uygulayabilir. Koruyucu rölenin işlevi, bir güç sisteminin bir elemanının kısa devreye maruz kalması ya da hasara neden olabilecek veya diğerlerinin etkin çalışmasına müdahale edebilecek herhangi bir anormal şekilde çalışmaya başladığında hızlıca kaldırılmasını sağlar.

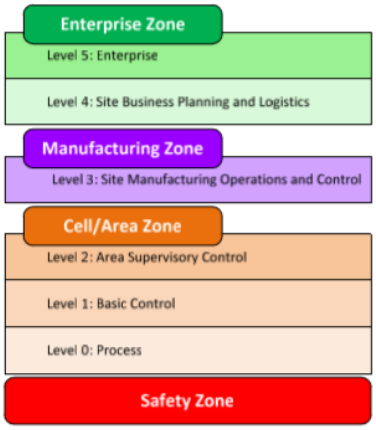
Endüstriyel alandaki iletişim alt yapısında kullanılan protokollerden kaynaklanan güvenlik açıklıklarının yanında cihazların kendi yazılım veya donanım bileşenlerinden kaynaklanan güvenlik açıklıkları da bulunmaktadır. Bu güvenlik açıklıklarının yönetilmesi, kritik alt yapıların hayati önem derecesine bağlı olarak oldukça önem arz etmektedir. Zhu ve ark., SCADA sistemlerine yönelik saldırı vektörlerini şu şekilde listelemişlerdir [27]:

- Ağ üzerinden açık bırakılan arka kapılar,
- İletişimde kullanılan protokollerden kaynaklı güvenlik zafiyetleri,
- Saha cihazlarına yapılan saldırılar,
- Veritabanı kaynaklı saldırlar,
- MITM kaynaklı saldırılar,
- Saha cihazlar ile saha cihazlarının kontrolörleri arasında ele geçirilen ağ veya denetleyici cihazın ele geçirilerek iletişimin manipüle edilmesi,
- Servis dışı bırakma saldırıları,

Bu ataklar, olay gerçekleştiğinde tespit, izleme ve cevap vermek sistemleri yeterli sıkılaştırma ve takibi yapılandırılmadığından BT sistemlerine göre daha sömürülebilir olmaktadır. Cihazların üzerindeki kimlik doğrulama mekanizmalarının aktifleştirilmemesi ya da zayıf parola yönetimi sebebiyle de benzer durumlar söz konusu olmaktadır. Güvenlik zafiyetleri sadece protokol ve ağ üzerinde değil cihazların üzerinde operasyonel işlemlerin yapılmasını sağlayan kendilerine özgü işletim sistemlerinde bulunan donanımsal zafiyetler de bulunmaktadır. Stuxnet ve diğer birçok APT saldırısında olduğu gibi sıfırıncı gün zafiyetleri de bu kategori içerisinde ele alınmaktadır. Bölüm 2.3 içerisinde belirtilen saldırılardan da anlaşılacağı üzere kritik alt yapıların olumsuz bir şekilde işlevselliğine müdahale edilmesi insan hayatında direkt olarak olumsuz etki oluşturmaktadır. Bu yüzden sistemin bir güvenlik ihlalinin olmadığından emin olmak ve sürecin olağan şekilde yürütülmesinin devamlılığını sağlamak adına sürekli izlenebilirlik, güvenlik yönetimi, risk yönetimi, ağ segmentasyonunun ve ağ cihazlarının güvenlik sıkılaştırmalarını doğru şekilde konfigüre etmek gibi siber güvenlik süreçlerinin uygulanması kritik derecede önem arz etmektedir.

Kritik alt yapılı sistemlerde, güvenlik açıklıklarının yönetilmesi için global olarak kabul görmüş ağ tasarım mimarisi olan Purdue modeli referans olarak önerilmektedir.

Purdue Kurumsal Referans Mimarisi modeli, 1990'larda bilgisayarla entegre üretim için Purdue Üniversitesi Konsorsiyumu üyeleriyle iş birliği içinde Theodore J. Williams tarafından geliştirilen kurumsal mimari için bir referans modelidir [28]. Purdue referans mimarisi, EKS'de kritik kabul edilen erişim kontrolü, log yönetimi, ağ güvenliği ve uzaktan erişim olarak dört güvenlik alanında tanımlanan mimari kalıpları sunmak için temel olarak kullanılmaktadır [3]. Purdue modeli, bir EKS ağını benzer işlevleri yerine getiren veya benzer gereksinimleri olan sistemlerden oluşan mantıksal bölümlere bölmek için bölgeler kavramını kullanır. 6 seviye ve 4 bölgeden oluşan model Şekil 2.1.'de belirtilmiştir.



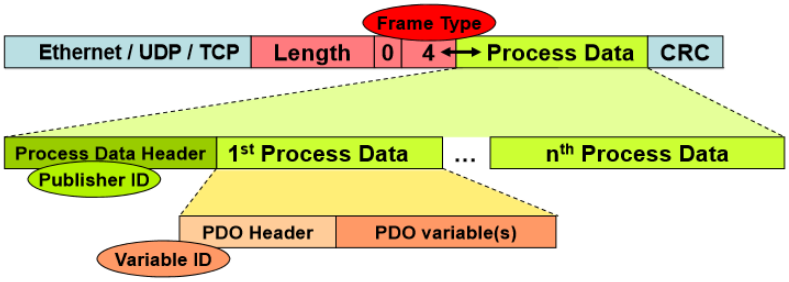
Şekil 2.1. Purdue referans modeli

Seviye 5, kurumsal BT altyapı sistemlerinin ve uygulamalarının bulunduğu yerdir. Tipik olarak, VPN uzaktan erişim ve kurumsal internet erişim hizmetleri bu seviyede yaşamaktadır. Bu seviyede bulunan sistemler ile EKS ortamı arasındaki doğrudan iletişim, genellikle kuruluşun maruz kalacağı risk düzeyine bağlı olarak önerilmez. Bu iletişim yerine, Demilitarized Zone (DMZ) aracılığıyla EKS ortamına erişimin sağlanmasıdır. Seviye 5'in bir uzantısı olarak görülen Seviye 4; raporlama, zamanlama, envanter yönetimi, kapasite planlama, operasyonel ve bakım yönetimi, e-posta, telefon ve baskı hizmetleriyle ilgilenen BT sistemlerini barındırır. Seviye 4 ve 5'teki hizmetler, sistemler ve uygulamalar normalde BT organizasyonu tarafından yönetilir ve işletilir. Üretim alanında yer alan 3. Seviye OT alanına ön girişi sağlayan saha üretim işlemleri ve kontrolünün yapıldığı seviyede, uzak erişim servisleri, ürün raporlama sistemleri, mühendislik bilgisayarı gibi alt seviye kontrol cihazlarının yönetimini sağlayan varlıklar ve hizmetler yer almaktadır. Bu seviyedeki sistemler ve uygulamalar DMZ ağı aracılığıyla *Enterprise* alandaki cihazlarla iletişim kurar. Seviye 1 ve Seviye 2'deki sistemlerle direkt iletişimde bulunabilir. Seviye 2, içerisinde HMI, alarm sistemleri ve kontrol odası iş istasyonlarını içeren üretim operasyonları ekipmanlarını içerir. Seviye 1, sensörlerden girdi alan, girilen verileri kontrol algoritmalarını kullanarak işleyen ve çıkarılan verileri bir uç elemana gönderen proses kontrol ekipmanını içerir. Bu seviyede bulunan bazı cihazlar DCS, PLC ve RTU olabilir. Bu cihazlar üreticiye özgü işletim sistemlerini çalıştırır ve mühendislik iş istasyonlarından programlanıp yapılandırılır. Seviye 0, üretim sürecine doğrudan bağlanan ve kontrol eden sensörleri ve aktüatör elemanlarını içerir. Bu cihazlar Seviye 1'de bulunan cihazlar tarafından kontrol edilir.

Endüstriyel kontrol sistemlerin operasyonel süreçleri yürütebilmesi için aralarında iletişim standartının olması gerekmektedir. Bu iletişim için endüstriyel protokoller tercih edilmektedir. Yaygın olarak kullanılan endüstriyel protokollerden biri olan EtherCAT protokolü bir sonraki bölümde açıklanmıştır.

2.2. EtherCAT Protokolü

Endüstriyel Ethernet, düşük maliyetli, esnek ağ, yüksek veri iletim hızı, güçlü kaynak paylaşım kabiliyetleri, internete bağlantıda sağladığı esneklik gibi kolaylıklar sayesinde endüstriyel sistemlerin iletişiminde gün geçtikçe daha popüler hale gelmektedir. 2003 yılında endüstriyel protokol olarak geliştirilen EtherCAT, Beckhoff Automation tarafından geliştirilen gerçek zamanlı bir Endüstriyel Ethernet teknolojisidir. IEC61158, IEC standardında açıklanan EtherCAT protokolü, otomasyon teknolojisinde, test ve ölçümde ve diğer birçok uygulamada gerçek zamanlı gereksinimler için uygundur [29].



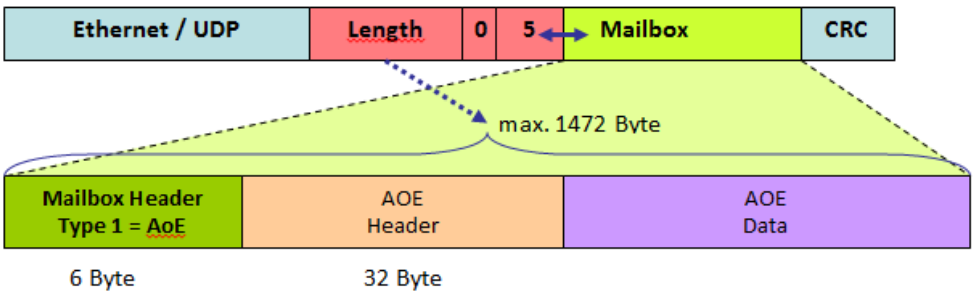
Şekil 2.2. EtherCAT çerçeve yapısı [29]

EtherCAT, endüstriyel ortamlarda hem fabrika seviyesi hem saha seviyesi iletişimleri desteklemektedir. Saha seviyesi ve fabrika seviyesindeki kullanım amaçlarına göre farklı alt protokoller kullanılmaktadır. Ethernet tabanlı bir protokol olduğundan Ethernet çerçevesini (Şekil 2.2.) içinde bulundurmaktadır. Çerçevede EtherType alanı, 0x88A4 ile tanımlanır. Böylece başlık hariç toplamda en fazla 1498 bayt veriyi tek bit Ethernet yapısında veri taşıma işlemini yapabilmektedir.

EAP protokolü fabrika seviyesinde, Mailbox ve Process Data iletişimini sağlayan bir alt protokoldür. Asenkron veri transferi yapılması için Mailbox alt protokolü kullanılmaktadır [17]. Process Data alt protokolü efendi istasyon cihazları arasında

veri iletişimini sağlamaktadır [17]. EtherCAT Otomasyon Protokolü (EAP) cihazı, Ethernet ile bağlı bilgisayarlar arasında istenen değişkenlerin döngüsel ve kararlı değişimini sağlar. EAP cihazları arasındaki iletişim Yayıncı/Abone prensibine göre gerçekleşir [30]. İstenilen alt protokolün kullanımı ve PLC cihazlara ilgili programın geliştirilip yüklenebilmesi için TwinCAT yazılım programına ihtiyaç vardır. TwinCAT programı, endüstriyel sistemlerde mühendislik bilgisayarında konumlandırılır ve saha cihazlarının kontrolüne yönelik programlar bu bilgisayar üzerinden geliştirilir. EAP bilgilerinin gönderileceği Ağ Arabirim Kartı (NIC) ve EAP cihazına ADS/AMS tarafından erişilebilecek AMS NetID'si, EAP cihazının yapılandırma seçenekleri yardımıyla belirtilir. Ağ Arabirim Kartı seçildiğinde, EAP aygıtına erişilebilecek IP adresi otomatik olarak belirlenir. Cihazlar arası EAP iletişimi üzerinden verilerin okunabilmesi için EAP cihaza ait bir AMS Net ID ve yönlendirme işlemlerinin olması gerekmektedir. EAP mesajı, tip 4 EtherCAT protokolüne (EAP) göre aktarılır. Gerekli hedef MAC adresi ARP ve yapılandırılmış AMS NetID değerine göre belirlenir. MAC adreslemede olduğu gibi, EAP mesajı yalnızca alt ağ içinde gönderilebilir [30]. AMS Net ID adresi, TwinCAT ağındaki yerel bilgisayarın adresidir. "AMS Net Adresi" 6 bayttan oluşur ve bir nokta gösteriminde belirtilir. "Net Adresleri" proje yöneticisi tarafından verilmeli ve TwinCAT ağında tek değer olarak tanımlanmalıdır. Sistemin IP adresinden (varsa) bir AMS Net Kimliği kurulumundan standart + "1.1" oluşturulur. Kurulum sırasında IP adresi belirlenemiyorsa. AMS Net Kimliği ".1.1.1.1.1.1" şeklinde oluşturulur [31]. ADS, donanım veya yazılım tabanlı cihazlar arasında veri alışverişi için Beckhoff tarafından geliştirilen ve açıklanan bir alt protokoldür. TwinCAT EAP cihazı AoE protokolünü de destekler. ADS/AMS iletişimi ve AoE iletişimi arasındaki fark, ADS/AMS iletişiminin aksine, AoE iletişiminin TwinCAT yönlendiricisi gerektirmemesidir. AoE protokolü, Posta Kutusu İletişimi kategorisi altında TwinCAT'de sınıflandırılan protokollerden biridir. AoE'nin iletişimi için tip 5 bir EtherCAT telgrafı (posta kutusu iletişimi) kullanılır. Bir posta kutusu telgrafı TwinCAT EAP cihazından iletilebilir:

- Ethernet üzerinden (EtherType = 0x88A4) veya
- UDP / IP üzerinden (UDP Bağlantı Noktası = 0x88A4)



Şekil 2.3. AoE iletişimi çerçeve yapısı [32]

Posta kutusu iletişimi ile çeşitli protokolleri taşımak (tünellemek) mümkündür. Tünel oluşturulacak protokol Posta Kutusu Üstbilgisindeki alan türüne göre tanımlanır. AoE protokolü 1 değeriyle belirtilir (Şekil 2.3.). Posta Kutusu Başlığını doğrudan AoE Başlığı ve ardından AoE verileri izler. Yapısı ADS/AMS protokolü ile aynıdır [32].

EtherCAT protokolü de diğer endüstriyel protokoller gibi operasyonel teknolojilerin işletilmesi için bir araç olarak kullanılmaktadır. Kritik alt yapılardan biri olan su yönetim prosesinde EtherCAT protokolü kullanılmıştır. Su yönetim prosesine ait bilgiler bir sonraki başlıkta incelenmiştir.

2.3. Su Yönetim Prosesi

Kritik alt yapılardan biri olan su yönetimi oldukça önemli bir süreçtir. Hem insan sağlığı hem de diğer canlıların sağlığına direkt etkisi olan bu yapının doğru bir şekilde işleyebilmesi de aynı oranda önem teşkil etmektedir. Suyun toplanması, arıtılması ve yeniden kullanımı için farklı kimyasal işlemler gerekmektedir. Bu işlemler sırasında endüstriyel cihazlar birbirleriyle entegre olarak çalışmaktadır. Su yönetiminde temel olarak su tankları, motorlar, vanalar, kimyasal bileşenler, şamandıralar ve kontrol merkezi bileşenleri bulunmaktadır. Su prosesinin kontrolü için PLC veya RTU gibi programlanabilir saha cihazları kullanılmaktadır. Çalışan bir prosese müdahale etme, görüntüleme, sistem izlemesi gibi bir üst seviye işlemler SCADA yazılımlarında gerçekleştirilmektedir. Şekil 2.4.'te verilen su yönetim

prosesi kullanılarak yapılan çalışmalara ait topolojiler Bölüm 3 ve Bölüm 4 içerisinde verilmiştir.

Şekil 2.4. Su yönetimi proses sistemi

Su prosesinde seviye, motorların çalışma durumu, çalıştırılacak senaryo seçimi vb. gibi kontrol eden otomasyon programı TÜBİTAK 1005 desteğiyle gerçekleştirilen 118E263 numaralı "SCADA Sistemlerinde Kullanılan EtherCAT Protokolüne Ait Yeni Bir Saldırı Tespit Sistemi" isimli projesinde oluşturulmuştur. Bölüm 3 ve Bölüm 4 içerisinde yapılan çalışmalar bu otomasyon programına göre gerçekleştirilmiştir.

2.4. MITRE ICS ATT&CK Matrisi

MITRE ATT&CK Matrisi, gerçek dünya gözlemlerine dayanan siber saldırı taktik ve tekniklerin küresel olarak erişilebilir olduğu bir bilgi havuzudur. ATT&CK havuzu, özel sektörde, devlette ve siber güvenlik ürün ve hizmet topluluğunda belirli tehdit modellerinin ve yöntemlerinin geliştirilmesi için bir temel olarak kullanılır [33]. Açık ve ücretsiz olan bu yapı sürekli geliştirilmeye açıktır. Kırmızı ve mvi takımlar için çeşitli testlerin sistemli bir şekilde yapılabilmesine büyük ölçüde katkı sağlar. MITRE ATT&CK teknikleri ve prosedürleri, ağdan ve uç sistemlerden toplanan bilgileri analiz ederek saldırıları tespit etmek için davranışsal gözlemlenebilirliği sağlamaktadır [18].

MITRE ATT&CK ICS Matrisi, EKS teknoloji alanındaki siber olumsuz davranışlar için düzenlenmiş bir bilgi tabanıdır. Bir saldırganın, saldırı yaşam döngüsünün çeşitli aşamalarını ve hedeflediği bilinen varlık ve sistemleri yansıtır. Endüstriyel kontrol sistemlerindeki varlıkların çeşitliliği göz önüne alındığında doğru sınıflandırma yapmak için ICS ATT&CK matrisi Purdue mimarisinin ve varlık sınıflarının işlevsel düzeylerine odaklanılarak oluşturulmuştur [1]. Var olan sistemde 11 taktik ve 81 adet teknik bulunmaktadır. Bu sayılar, geliştirilen saldırı yöntemlerine göre güncellenebilir. Taktikler ve teknikler arasındaki ilişki ATT&CK Matrisinde görselleştirilebilir. Şekil 2.5.'de [34] MITRE ICS Matrisi verilmiştir. Matristeki her başlık bir taktik ismini tanımlarken her başlığın altında ilgili taktiğin amacına uygun kullanılabilecek teknikler tanımlanmıştır. Bir teknik kullanım amacına göre birden fazla taktiğin altında sınıflandırılabilir.

ICS matrisindeki taktikler, içinde barındırdıkları tekniklerin nedenini temsil ederler. Saldırganların, eylemleri gerçekleştirme nedeni taktiksel amaçlarını belirler. Tekniğin amacını belirlediğinden etiketleme olarak da kullanılmaktadır. Teknikler ise saldırganın hedefe ulaşmak için nasıl bir yol izlediğini belirtir.

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

Şekil 2.5. MITRE ICS Matrisi [34]

Kritik alt yapılar, siber dünyada devletler arasında siber dünyadaki savunma alanı oldukça önemli olarak kabul edilmiştir. Geçmişten günümüze kritik alt yapılara karşı yapılan saldırılarda zararlar göz önüne alınırsa oldukça kritik bir konu haline gelmiştir. Diğer saldırganlar gibi APT grupları da veri çalmaya, operasyonları aksatmaya veya altyapıyı yok etmeye çalışan süreçler geliştirir. Çoğu siber saldırgandan farklı olarak, APT saldırganları hedeflerini aylar veya yıllar boyunca takip ederler [35]. Siber savunmalara uyum sağlayıp aynı hedefi yeniden hedeflemektedirler. Güvenlik ekibinin en aktif APT gruplarının farkında olmalı ve önceki APT saldırılarına bağlı kötü amaçlı yazılımları tespit ettiklerinde ekstra önlemler almalıdır [35]. Bazı APT gruplarının ataklarına dair bilgiler ve MITRE ICS ATT&CK matrisindeki sınıflandırmaları aşağıda verilmiştir.

a. Stuxnet

Stuxnet, İran'ın nükleer çalışmalarını sekteye uğratmak için kullanılan solucan yazılımdır. Haziran 2010'da varlığı açığa çıkan virüs İran'ın Buşehr ve Natanz'daki nükleer tesislerini etkilemiştir. Stuxnet zararlı yazılımı, özellikle endüstriyel kontrol sistemleri cihazlarını hedefleyen halka açık ilk kötü amaçlı yazılım olarak kabul edilmektedir. Stuxnet, birden fazla sıfırıncı gün güvenlik açığı, gelişmiş bir Windows rootkit ve ağ bulaşma yordamları dahil olmak üzere birçok farklı karmaşık taktik kullanan büyük ve karmaşık bir zararlı yazılım parçasıdır. Yazılım içerisindeki kod nesne yönelimlidir ve Windows işletim sistemi, Microsoft SQL Server, Siemens yazılımı ve Siemens PLC'ler de dahil olmak üzere birçok alanda ileri düzey bilgi gerektiren birçok programlama tekniği kullanır [36]. Kötü amaçlı yazılım ayrıca tersine mühendisliği zor ve zaman alıcı hale getiren birçok gelişmiş anti-analiz tekniği kullanır. ICS-CERT, USB sürücüler birincil bulaşma yöntemi gibi görünse de Stuxnet'in ağ paylaşımları ve SQL veritabanları yoluyla da sistemlere bulaşabileceğini tespit etmiştir. Stuxnet kötü amaçlı yazılımı, bırakılan dosyaları hedef sistemdeki birçok konumda saklar. Bulaşma mekanizması karmaşıktır ve bırakılabilecek dosyalar bulaştığı sisteme bağlı olarak değişecektir. Bir sisteme bulaştıktan sonra, kötü amaçlı yazılım MS SQL sunucusundan, Windows kayıt defterinden ve uygulama yazılımından kapsamlı veriler toplar [36].

Stuxnet zararlı yazılımının MITRE ICS ATT&CK matrisinde kullandığı taktik ve tekniklerin haritalandırılması Şekil 2.6.'da verilmiştir.

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

Şekil 2.6. Stuxnet zararlı yazılımı MITRE ICS ATT&CK teknikleri

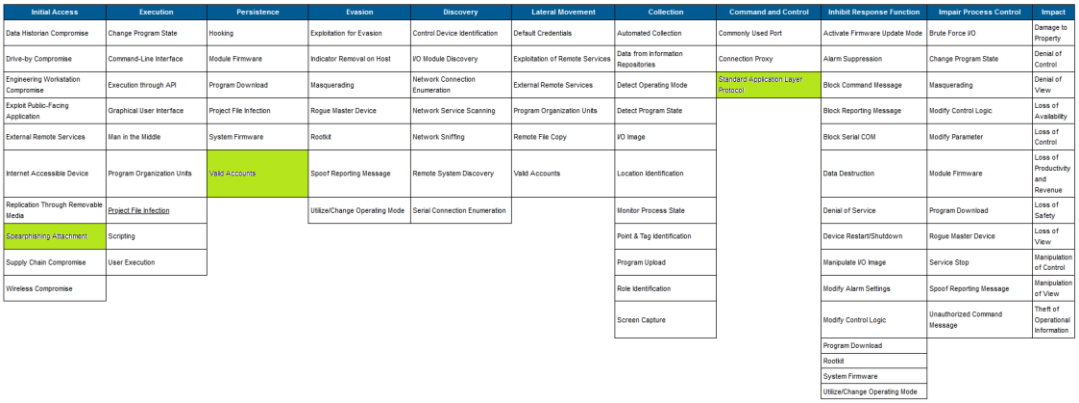
b. Ukrayna Güç Şebekesi Saldırısı/Black Energy

2015 yılında, Noel'den iki gün önce, bir siber saldırı gerçekleşmiş ve yaklaşık çeyrek milyon Ukraynalının elektriğinin kesilmesine neden olmuştur. Bu saldırı, bir güç şebekesine bilinen ilk başarılı siber saldırıdır. Saldırganlar 30 trafo merkezinde gücü kapatarak ve 230.000 kişiyi altı saate kadar elektriksiz bırakmıştır. SCADA ekipmanı çalışmaz hale getirilmiş ve güç restorasyonunun manuel olarak tamamlanması gereken cihazları daha da geciktirmiştir [37]. Araştırmacılar, saldırganların Microsoft Excel belgelerindeki makrolardan yararlanmak için BlackEnergy kötü amaçlı yazılımını kullanarak kesintiyi kolaylaştırdığını keşfetmişlerdir. Kötü amaçlı yazılım, spear-phising yöntemiyle e-postaları kullanarak şirket ağına dahil olunması sağlanmıştır [37].

Blackenergy zararlı yazılımını bir varyantı olan BlackEnergy 3, hem siber saldırganlar hem de APT grupları tarafından kullanılan kötü amaçlı yazılım aracıdır. KillDisk'in bir çeşidi de dahil olmak üzere çeşitli eklentileri destekler. Ukrayna elektrik şebekesine karşı kullanıldığı bilinmektedir. BlackEnergy 3 zararlı yazılımı şu ana kadar Ukrayna endüstrilerinde hedefli saldırılarda kullanılmıştır. Yetkilendirme isteklerinden ve kullanıcı yönetiminden sorumlu sunucu olarak kullanılan Active Directory Etki Alanı Denetleyicileri ve masaüstü iş istasyonları

gibi genel Microsoft Windows platformlarını ve sunucularını hedeflemektedirler [38]. Black Energy 3, 2014'ten bu yana farklı saldırılardan sorumludur.

Blackenergy 3 zararlı yazılımının MITRE ICS ATT&CK matrisinde kullandığı taktik ve tekniklerin haritalandırılması Şekil 2.7.'de verilmiştir.

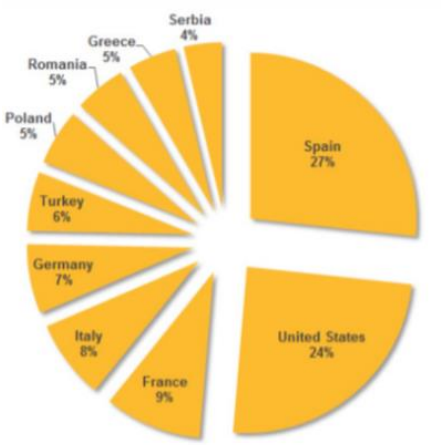


Şekil 2.7. Blackenergy 3 zararlı yazılımı MITRE ICS ATT&CK teknikleri

c. Havex

Havex/Dragonfly zararlı yazılımını içeren APT saldırısı, 2010'un sonlarında başlamıştır, ancak 2013 yılına kadar keşfedilememiştir. Dragonfly zararlı yazılımının ilk hedefleri ABD ve Kanada'daki havacılık ve savunma endüstrileriydi ancak 2013'ün başında enerji sektörüne yayıldı [39]. F-Secure ve Symantec'teki siber güvenlik araştırmacıları tarafından keşfedilmiştir ve ICS-CERT tarafından 2014 yılında bu firmaların her ikisinden de bilgiler kullanılarak bildirilmiştir. Sisteme giriş için spear-phishing yöntemi kullanılmıştır. PHP programlama dilinde yazılmış bir RAT ve C&C sunucu iletişimde olan başka bir modül olarak iki ana yapıdan oluşan bir zararlı yazılımdır. Ayrıca ağdaki endüstriyel cihazları aramak için kullanılan bir OPC tarama modülü içerir. OPC tarama modülü 44818, 105 ve 502 bağlantı noktalarında çalışan TCP aygıtlarını taramak için tasarlanmıştır [40].

Havex zararlı yazılımının, sanayi ve enerji kuruluşlarını hedef alan dünya çapında farklı oranlarda yaygın bir şekilde gerçekleştirilmiştir. Bu oransal Symantec 2014 güvenlik raporuna göre Şekil 2.8.'de en çok etkilenen ilk 10 ülke gösterilmiştir [39].



Şekil 2.8. Havex zararlı yazılımından en çok etkilenen 10 ülke [38]

Havex zararlı yazılımının MITRE ICS ATT&CK matrisinde kullandığı taktik ve tekniklerin haritalandırılması Şekil 2.9.'da verilmiştir.

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

Şekil 2.9. Havex zararlı yazılımı MITRE ICS ATT&CK teknikleri

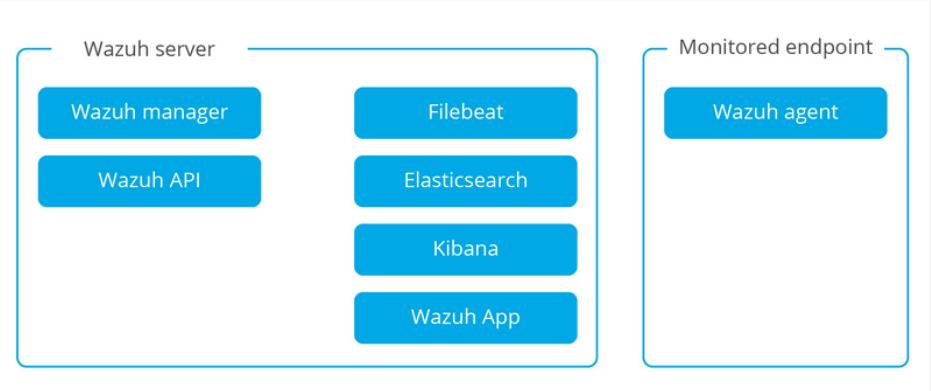
2.5. Wazuh HIDS ve Sysmon ile Sistem İzleme ve Saldırı Tespiti Yapısı

Wazuh, ana bilgisayarların üzerinde olayların ve anomalilerin izlenebilirliğini sağlayan açık kaynak kodlu bir saldırı tespit sistemidir. İlgili olayların sistemde tetiklenmesiyle alarmlar oluşturarak olası tehditlerin erkenden belirlenmesiyle önemli saldırıların önüne geçilmesi sağlanır. Varsayılan alarm kurallarına ek alarm kuralları da yazılabilmektedir. Böylece kurumsal ağın içinde bulunduğu sektöre

yönelik farklı saldırı senaryolarına karşı özel alarm kuralları oluşturulabilir. Host tabanlı saldırı tespit sistemi olduğundan, izleme yapılacak makinelere *agent* kurulumu ve *agentların* gönderdiği bilgileri analiz eden Wazuh sunucusu iki ana yapıyı oluşturmaktadır. Wazuh HIDS aracının başlıca özellikleri şöyle listelenebilir:

a. Log yönetimi ve analizi: Wazuh *agentları* işletim sistemi ve uygulama loglarını okur. Kural tabanlı analiz ve depolama için güvenli bir şekilde merkezi yöneticiye iletir [41].
b. Dosya bütünlüğü izleme: Gözden geçirilmesi gereken dosyaların içerik, izinler, sahiplik ve niteliklerindeki değişiklikleri belirleyerek dosya sistemini izler [41].
c. Olay ve anomali tespiti: *Agentlar*, kötü amaçlı yazılım, *rootkit* veya şüpheli anormallikler için sistemi tarar. Gizli dosyaları, gizli işlemleri veya kayıt dışı ağ dinleyicilerini ve sistem çağrısı yanıtlarındaki tutarsızlıkları tespit edilebilir [41].
d. Politika ve uygunluk izleme: Güvenlik politikaları ve standartlarla uyumlu olduklarından emin olmak için yapılandırma dosyalarını izler. *Agentlar*, savunmasız, toplu olmayan veya güvenli olmayan şekilde yapılandırılmış olduğu bilinen uygulamaları algılamak için periyodik taramalar gerçekleştirir [41].

Wazuh kullanım amacına göre çeşitli mimarilerde kurulumu yapılır. Elasticsearch kümesi, dizinlerde okuma ve yazma işlemlerini gerçekleştirmek için birbirleriyle iletişim kuran bir veya daha fazla düğümün (sunucunun) topluluğudur. Küçük Wazuh konuşlandırmaları (<50 agent), tek düğümlü bir küme tarafından kolayca yönetilebilir. Çok sayıda izlenen sistem olduğunda ya da çok sayıda veri bekleniyorsa veya yüksek kullanılabilirlik gerektiğinde çok düğümlü kümeler önerilmektedir [42].



Şekil 2.10. Wazuh Sunucu-İstemci mimari yapısı [41]

Wazuh sunucusu ve Elasticsearch kümesi farklı ana bilgisayarlarda olduğunda, Filebeat, Wazuh uyarılarını veya arşivlenmiş olayları TLS şifrelemesi kullanarak Elasticsearch sunucularına güvenli bir şekilde iletmek için kullanılır [42]. Şekil 2.10.'da verilen şema, Wazuh sunucusu ve Elasticsearch kümesi farklı ana bilgisayarlarda çalıştığında bileşenlerin nasıl dağıtıldığını gösterir. Şekil 2.10.'da Wazuh HIDS içerisindeki bileşenler gösterilmektedir.

Wazuh sunucusu TLS şifrelemesi kullanarak Elasticsearch sunucusuna uyarı ve olay verilerini göndermek için Filebeat aracını kullanır. Filebeat gelen verileri biçimlendirir ve Elasticsearch'e (port 9200/TCP) göndermeden önce isteğe bağlı olarak GeoIP bilgileriyle zenginleştirir. Veriler Elasticsearch'e indekslendikten sonra, bilgileri görselleştirmek için Kibana (port 5601/TCP) kullanılır [42]. Wazuh Uygulaması, sunucu ve aracıların yapılandırma ve durumla ilgili bilgilerini görüntülemek ve ayrıca istendiğinde aracıları yeniden başlatmak için Kibana içinde sürekli olarak RESTful API'yi (Wazuh yöneticisinde 55000/TCP port) sorgular. Bu iletişim TLS ile şifrelenir ve kullanıcı adı ve parola ile doğrulanır [42].

Wazuh ve Elastik Stack kurulumu için, farklı bileşenlerin aralarında düzgün iletişim kurabilmesi için birkaç ağ bağlantı noktası (port) bulunmalı ve açılmalıdır. Bu portlar açıklamalarıyla beraber Tablo 2.1.'de verilmiştir.

Tablo 2.1. Wazuh iletişimi için gerekli port numaraları [34]

Bileşen	**Port**	**Protokol**	**Amaç**
Wazuh Manager	1514	TCP	Agent'lardan toplanan olayların gönderilmesi

Tablo 2.1. (Devamı)

Bileşen	Port	Protokol	Amaç
Wazuh Manager	1514	UDP	Agent'lardan toplanan olayların gönderilmesi – Varsayılan Yapılandırma
	1515	TCP	Agent kayıt servisi
	1516	TCP	Wazuh cluster iletişimi
	514	TCP	Toplanan olayları syslog'dan gönderir
	514	UDP	Toplanan olayları sistem günlüğünden gönderir – Varsayılan Yapılandırma
Wazuh API	55000	TCP	Gelen HTTP İstekleri

Wazuh sunucuda toplanan ve analiz edilen veriler, kaydedilmesi için Elasticsearch yığınına aktarılır ve Kibana arayüzünde görselleştirilir. Bu iletişim için de Tablo 2.2.'de belirtilen portların açık olması gerekmektedir.

Tablo 2.2. Elasticsearch iletişimi için gerekli port numaraları [34]

Bileşen	Port	Protokol	Amaç
Elasticsearch	9200	TCP	Elasticsearch RESTful API iletşimi
	9300 – 9400	TCP	Elasticsearch cluster iletişimi
Kibana	5601	TCP	Kibana web arayüzü

Sistem Monitörü (Sysmon), sistem etkinliğini izlemek ve sistem olaylarını Windows olay günlüğüne kaydetmek için Windows sistem hizmeti ve aygıt sürücüsüdür. Süreç oluşturma işlemleri, ağ bağlantıları ve dosya oluşturma süresindeki değişiklikler hakkında ayrıntılı bilgi sağlar [43]. Windows Olay Koleksiyonu veya SIEM araçlarını kullanarak oluşturduğu olayları toplayarak ve ardından bunları analiz

ederek kötü niyetli veya anormal etkinlikleri tespit edebilir ve kötü amaçlı yazılımların ağ içerisinde nasıl çalıştığının takibi yapılabilir. Ancak Sysmon'un ürettiği olayların analizini sağlamadığından saldırganlardan korunmak için bir işlevselliği yoktur. Sysmon aracının başlıca özellikleri şöyle listelenebilir [43]:

- Hem mevcut hem de ebeveyn süreçler için komut satırı ile süreç oluşturmayı günlüğe kaydeder.
- SHA1 (varsayılan), MD5, SHA256 veya IMPHASH kullanarak süreçlerin imaj dosyalarını *hash* formatında kaydeder.
- Aynı anda çoklu *hash* formatı kullanma imkanı tanımaktadır.
- Windows proses kimliklerini yeniden kullansa bile olayların korelasyonuna izin vermek için proses oluşturma olaylarında bir proses GUID'si içerir.
- Sürücülerin veya DLL'lerin yüklenmesini imzaları ve hash bilgileriyle loglar.
- İsteğe bağlı olarak, her bağlantının kaynak prosesini, IP adresleri, port numaraları, ana bilgisayar adları ve port adları dahil ağ bağlantılarını loglar.
- Bir dosyanın ne zaman oluşturulduğunu anlamak için dosya oluşturma süresindeki değişiklikleri algılar. Dosya oluşturma zaman damgalarının değiştirilmesi, kötü amaçlı yazılımlar tarafından izlerini kaybettirmek için yaygın olarak kullanılan bir tekniktir.
- Kayıt defterinde değiştirilirse yapılandırmayı otomatik olarak yeniden yükler.
- Belirli olayları dinamik olarak dahil etmek veya hariç tutmak için kuralları filtreler.

BÖLÜM 3. ETHERCAT DESTEKLİ SAHA CİHAZLARINA YAPILAN SALDIRILAR VE MAKİNE ÖĞRENMESİ İLE TESPİTİ

Bu bölümde EtherCAT protokolünün fabrika seviyesinde kullanımının güvenlik yönü ele alınmıştır. Ethercat protokolü, bilişim teknolojilerinde kullanılan standart kimlik doğrulama, şifreleme ve yetkilendirme gibi temel güvenlik parametrelerini içermediği için ortam erişim denetimi sızdırma, uzaktan veri elde etme ve diğer ileri seviye bilgi gerektiren gelişmiş saldırılara açık olduğu görülmüştür.

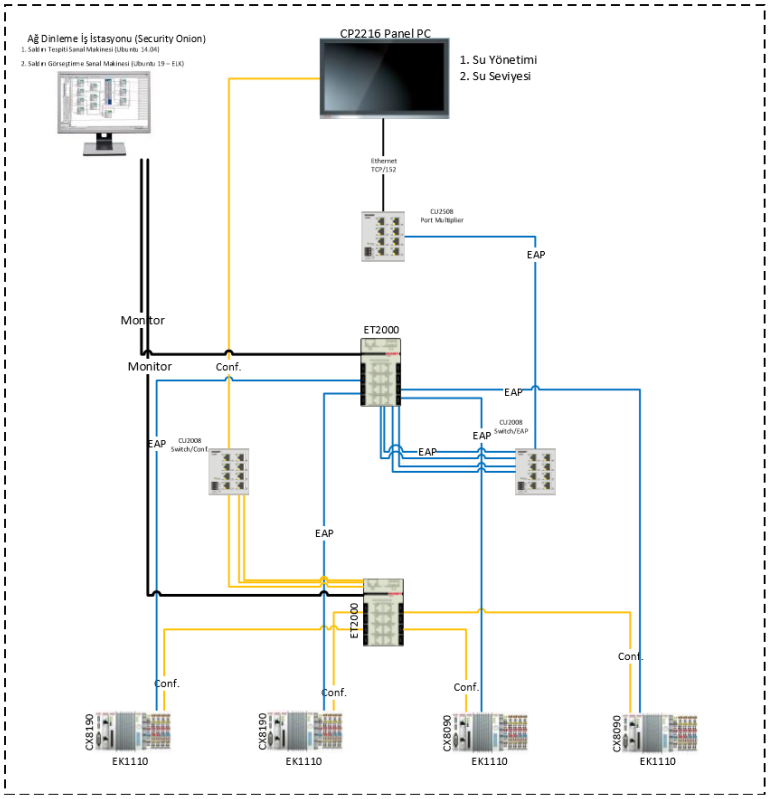
Ovaz Akpınar, doktora çalışmasında [17], EtherCAT alt yapısıyla çalışan saha seviyesi ile ilgili saldırılar gerçekleştirmiş ve bu saldırılara yönelik açık kaynak kodlu Snort saldırı tespit sistemine ön işlemci geliştirmiştir. Sıfırıncı gün saldırılarının tespiti için de makine öğrenmesi yöntemi kullanarak gerçekleştirmiştir. Bu bölümde endüstriyel sistemlerde saha seviyesinin bir üst seviye çalışma ortamı olan fabrika seviyesine yönelik MITRE ATT&CK ICS matrisi kullanılarak saldırı vektörleri oluşturulmuş ve SVM algoritmasıyla makine öğrenimi metodu kullanılarak saldırıların tespiti sağlanmıştır.

3.1. Test Ortamı

Tez çalışmasının 3 ve 4. bölümünde yapılan çalışmalar, Sakarya Üniversitesi- Siber Güvenlik Araştırma ve Uygulama Laboratuvarı bünyesinde yer alan donanımlardan Windows CE tabanlı Beckhoff PLC, mühendislik istasyonu, ağ Probe cihazı ve su proses sistemi ile oluşturulan test ortamında yapılmıştır.

Test ortamı topolojisi, 1 adet arıtma istasyonu, 2 terfi istasyonu ve 1 adet depo olmak üzere toplam 4 istasyonun yönetimini kapsamaktadır. Her istasyonda kontrol için PLC ve I/O donanımları yer almaktadır. Bunun dışında anahtar cihazlar, yapılandırma ve programlama için mühendislik istasyonu, pasif ağ dinleme yapmak için 2 adet ET2000 *probe* cihazı ve kontrol/gözlem için HMI panel yer almaktadır (Şekil 3.1.).

Test ortamında kullanılan ET2000 ağ *Probe* cihazı; EtherCAT protokolü için gerçek zamanlı sistemlere uygun olarak tasarlanmış, 4 adet giriş ve 4 adet çıkış kanalını desteklemektedir. Bu cihazın gerçek zamanlı iletişime ve ağın bant genişliğine herhangi bir etkisi bulunmamaktadır. Pasif modda ağı dinlemekte ve orijinal hallerini çıkış kanalından hedeflerine gönderirken kopyalanmış olan ağ paketlerini de *Uplink* kanalından ağı dinlemek için bağlanan cihaza iletmektedir.



Şekil 3.1. Su yönetimi proses sistemine ait topoloji

Fabrika seviyesinde saldırıların tespit edilmesi ve pasif ağ izleme yapılması için bir adet izleme bilgisayarı kurulmuş ve sisteme entegre edilmiştir. Bu makinada log toplama ve sorgular için Elasticsearch, Logstash, görselleştirme için ise Kibana platformlarından oluşan ELK Stack kurulmuştur. Topolojide hem PLC cihaz durum bilgilerinin iletildiği konfigürasyon hattından gelen bilgilerin alınması hem de PLC cihazlara bağlı prosesten gelen su seviyesi bilgilerinin iletildiği veri hattından gelen bilgilerin alınması için iki farklı ET2000 cihazı, saldırı tespiti ve görselleştirme makinesine bağlanmıştır.

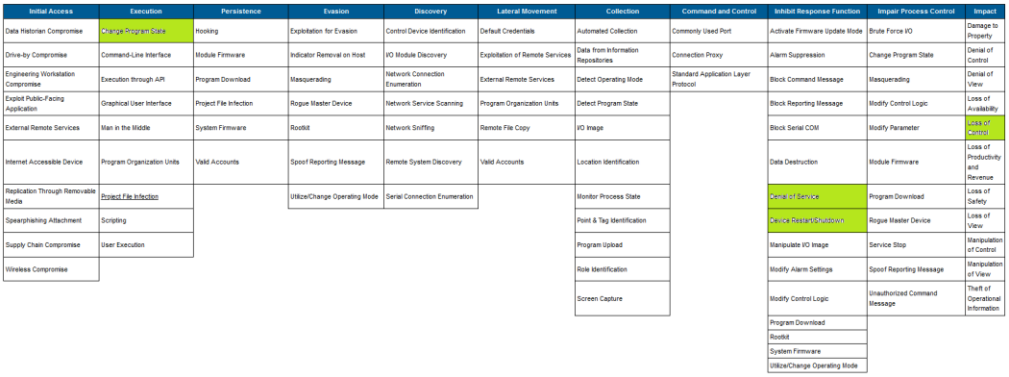
4 adet Windows CE tabanlı Beckhoff PLC şekildeki gibi su prosesine;

- Arıtma – CX8190
- Terfi 1 – CX8190
- Terfi 2 – CX8090
- Depo – CX8090
- Panel – CP2216

Modelindeki PLC'ler Şekil 3.1.'deki su prosesine bağlanmıştır.

3.2. Saldırı Vektörlerinin Oluşturulması

Siber güvenlik alanında yapılan DoS gibi geleneksel saldırılar EtherCAT tabanlı çalışan su yönetim sistemi üzerinde yapılmıştır. Saldırılarda genel olarak PLC cihazları arasındaki su seviyelerinin EAP iletişimi manipüle edilerek sistemin beklenen akışın dışında çalışması sağlanmıştır. Çalışan sistemin servis dışı kalmasına sebep olan DoS saldırısı da yapılmıştır. PLC çalışma durumları (başlatma, durdurma, yapılandırma vb.), PLC'nin yapılandırma ayarları ile ilgili olduğu için AMS iletişimi üzerinden işlem yapılmıştır. Fabrika seviyesi üzerinde yapılan bu saldırıların MITRE ICS ATT&CK matrisindeki tekniklerin haritalandırılması Şekil 3.2.'de verilmiştir. Bu aşamada yapılan saldırılar, aşağıda verilmiştir ve sıra bağımsız olduğundan tekniklerde herhangi bir sıralama yapılmamıştır.



Şekil 3.2. Saldırı senaryosunda seçilen tekniklerin MITRE ICS ATT&CK Matrisi

a. MITRE ICS ATT&CK Matris Kodu: T875

Taktik/Teknik Adı: Execution/ Change Program State

Saldırganlar, bir kontrol cihazındaki programın durumunu değiştirmeye çalışabilirler. Program durumu değişiklikleri, başka bir programın kontrolü ele geçirmesine veya cihaza yüklenmesine izin vermek için kullanılabilen bir tekniktir. Bu teknik EKS sistemlerdeki alan denetleyicileri, PLC, RTU veya IED cihazlar üzerinde etkili olmaktadır. Bu yöntemi kullandığı bilinen zararlı yazılımlar, *PLC-Blaster, Stuxnet* ve *Triton* yazılımlarıdır. *PLC-Blaster* bir PLC'ye aktarıldıktan sonra PLC, *PLC-Blaster*'ın zararlı yazılımını çalıştırmaya başlar. *Stuxnet* orijinal PLC kodunu durdurur ve kötü amaçlı PLC kodu, DP_RECV monitör aşamasında kaydedilen değerlere göre veri çerçeveleri göndermeye başlar. *Triton, TriStation* protokolü aracılığıyla bir programı durdurabilir veya çalıştırabilir. *TsHi.py* kodu yürütülen durdurma ve çalıştırma işlevlerinin örneklerini içerir [44].

Bu tekniğin tez içerisindeki uygulamasına dair ayrıntılar Bölüm 3.2.2 içerisinde verilmiştir.

b. MITRE ICS ATT&CK Matris Kodu: T814

Taktik/Teknik Adı: Inhibit Response Function/ Denial of Service

Saldırganlar, beklenen cihaz işlevselliğini bozmak için Hizmet Reddi (DoS) saldırıları gerçekleştirebilir. DoS saldırılarına örnek olarak, hedef cihazın kısa sürede yüksek oranda isteklerle boğulması ve hedef cihaza nasıl işleneceğini bilmediği bir istek gönderilmesi verilebilir. Cihaz durumunun kesilmesi, geçici olarak yanıt vermemesine neden olabilir, hatta bu durum yeniden başlatma gerçekleşene kadar

devam edebilir. Bu duruma getirildiğinde, aygıtlar istek gönderip alamayabilir ve ortamdaki diğer olaylara tepki olarak beklenen yanıt işlevlerini yerine getiremeyebilir [45]. Bu teknik EKS sistemlerdeki alan denetleyicileri, PLC, RTU, IED, SIS cihazları veya koruma röleleri üzerinde etkili olmaktadır. Bazı EKS cihazları DoS olaylarına karşı özellikle duyarlıdır ve basit bir *ping* taramasına bile tepki vermeyebilir. Bu yöntemi kullandığı bilinen zararlı yazılımlar, *Havex, Industroyer, PLC-Blaster* zararlı yazılımlarıdır. *Havex* zararlı yazılımı birden çok OPC platformunun zaman zaman servis dışı kalmasına sebep olmuştur. *Industroyer* SIPROTEC DoS modülü, bir Siemens SIPROTEC cihazının yanıt vermemesini sağlamak için CVE-2015-5374 güvenlik açığından yararlanmıştır. Bu güvenlik açığından başarıyla yararlanıldığında, hedef cihaz el ile yeniden başlatılıncaya kadar tüm komutlara yanıt vermeyi durdurur. Araç çalıştırıldığında, UDP kullanarak hedef IP adreslerinin 50000 numaralı port numarasına özel hazırlanmış paketler gönderir. UDP paketi 18 bayt uzunluğundaki 0x11 49 00 00 00 00 00 00 00 00 00 00 00 00 00 28 28E verisini içerir [45]. *PLC-Blaster*, DoS etkisi ile PLC içinde bir hata durumunu tetikleyen sonsuz bir döngü uygular.

Bu tekniğin tez içerisindeki uygulamasına dair ayrıntılar Bölüm 3.2.3 içerisinde verilmiştir.

c. MITRE ICS ATT&CK Matris Kodu: T816

Taktik/Teknik Adı: Inhibit Response Function/ Device Restart/Shutdown

Saldırganlar, ICS ortamındaki bir cihazı kesintiye uğratmak için zorla yeniden başlatabilir, kapatabilir ve kontrol etmeye yardımcı olduğu fiziksel süreçler üzerinde olumsuz etkilere neden olabilir. Cihazı yeniden başlatma ve kapatma yöntemleri, standart işlevler olarak mevcuttur. Bunlar arasında cihaz web ara yüzleri, komut satırı ara yüzleri ve ağ protokolü komutları bulunur. Endüstriyel cihazın yeniden başlatılması veya kapatılması, cihazın test veya ürün yazılımı yüklemesi için alternatif bir çalışma moduna değiştirilmesinin bir sonucu olarak da ortaya çıkabilir [46]. Kontrol sistemi cihazlarının beklenmedik şekilde yeniden başlatılması veya kapatılması, kötü amaçlı cihaz değişikliğinin bir işareti olabilir, çünkü birçok güncelleme etkili olmak için cihazın yeniden başlatılmasını gerektirebilir. Örneğin,

DNP3'ün fonksiyon kodu 0x0D, DNP3 dış istasyonlarını tam bir güç döngüsü gerçekleştirmeye zorlayarak sıfırlayabilir ve yeniden yapılandırabilir. 2015'te Ukrayna'nın güç şebekesine yapılan saldırıda, saldırganlar üç farklı enerji şirketinin kontrol ağlarına erişmiştir. UPS sistemleri için bağlantıyı kesmişlerdir, böylece güç trafo merkezlerinden kesildiğinde, cihazlar kapanır ve servis kurtarılamaz [46].

Bu teknikten korunmak için, Rol Tabanlı Erişim Kontrolü (RBAC) ile kullanıcı ayrıcalıkları kısıtlanmalıdır. Tanımlanan roller, en az ayrıcalık ilkesine göre yapılandırılmalı. Erişim düzeyleri, belirli ICS verilerini veya cihaz işlevlerini görüntüleme, kullanma ve değiştirme yeteneği de dahil olmak üzere çeşitli faktörleri belirlenmelidir [47]. Genel olarak, bir ICS ortamındaki cihazların sık sık kapanmalarla karşılaşması olası değildir. Bu nedenle, beklenmedik durum değişiklikleri için fiziksel cihazları ve olası şüpheli olaylar için ağ sürekli olarak izlenmelidir. Güçlü parola ilkelerini uygulamak ve çok faktörlü kimlik doğrulamayı etkinleştirmek, yalnızca doğrulanmış kullanıcıların kapatma özelliği tanımlanarak aygıtın kapatılmasına ek bir engel oluşturabilir [47].

Bu tekniğin tez içerisindeki uygulamasına dair ayrıntılar Bölüm 3.2.2 içerisinde verilmiştir.

d. MITRE ICS ATT&CK Matris Kodu: T827
Taktik/Teknik Adı: Impact/ Loss of Control
Saldırganlar, kötü niyetli girişim azalmış olsa bile, operatörlerin herhangi bir komut veremediği sürekli bir kontrol kaybına veya kaçak bir koşula ulaşmaya çalışabilirler.

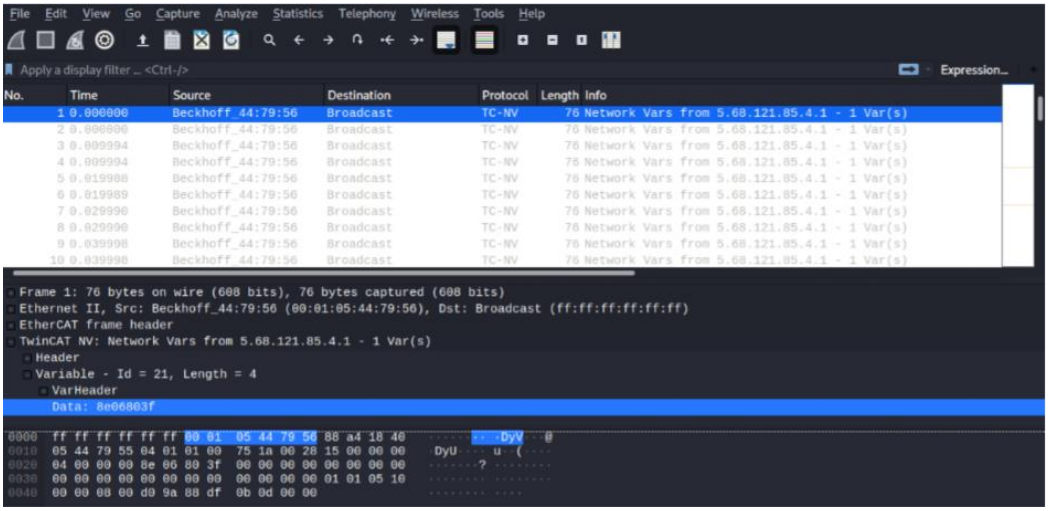
Bu teknik fabrika seviyesinde yapılan diğer üç saldırının bir sonucu olarak ortaya çıkmaktadır.

3.2.1. Su seviyesi değişimi

PLC cihazlar arası veri bilgisini taşıyan EAP iletişimi test ortamında bulunan Probe cihazından dinlenerek gönderilen su seviyesi değiştirilmiş ve dolu olan su kabına az

miktarda su varmış gibi su basılması sağlanmıştır. Benzer yöntemle çalışmaması gereken motorlar da çalıştırılarak sistem manipüle edilmiştir. Bu yöntemle motorların aşırı çalışmasıyla sisteme fiziksel zarar verilmesine sebep olunabilir. Test cihazlarına zarar gelmemesi açısından bu atak vektörü test edilmemiştir.

Seviye bilgisini manipüle etmek için sistem üzerinde bulunan ET2000 cihazından alınan ağ paketleri incelenmiştir ve ağ trafiği PCAP dosyası olarak kaydedilmiştir. Kaydedilen ağ akışı incelenerek Şekil 3.3.'te belirtilen *Data* alanı içerisindeki seviye bilgisini tutan değer tüm paketler için değiştirilip *Kali* işletim sistemine sahip sanal makinesinde bulunan *tcpreplay* aracı ile sisteme değiştirilmiş seviye yeniden gönderilerek yanlış motorların çalışması sağlanmıştır.



Şekil 3.3. Veri alanı değiştirilmiş paketler

Aynı ağda PLC cihazların kendi aralarındaki normal paket akışının saldırıyı engellememesi için *tcpreplay* aracına verilen *loop* parametresi büyük tutularak sistemde geçerli olan değerlerin saldırı vektörüne ait olması sağlanmıştır.

Şekil 3.3.'te bulunan EAP (TC_NV) paketlerinin *Data* alanları *little endian float* değer karşılığı "1.0002" olan "8e06803f" hex değeri yazılarak yanlış seviye bilgisi *tcpreplay* aracı ile sisteme tekrar gönderilerek yanlış motorların çalışması sağlanmıştır. Veri iletiminde normal trafiğin işlememesi için değiştirilmiş ağ trafiği dosyası 5000 kez gönderilmiştir.

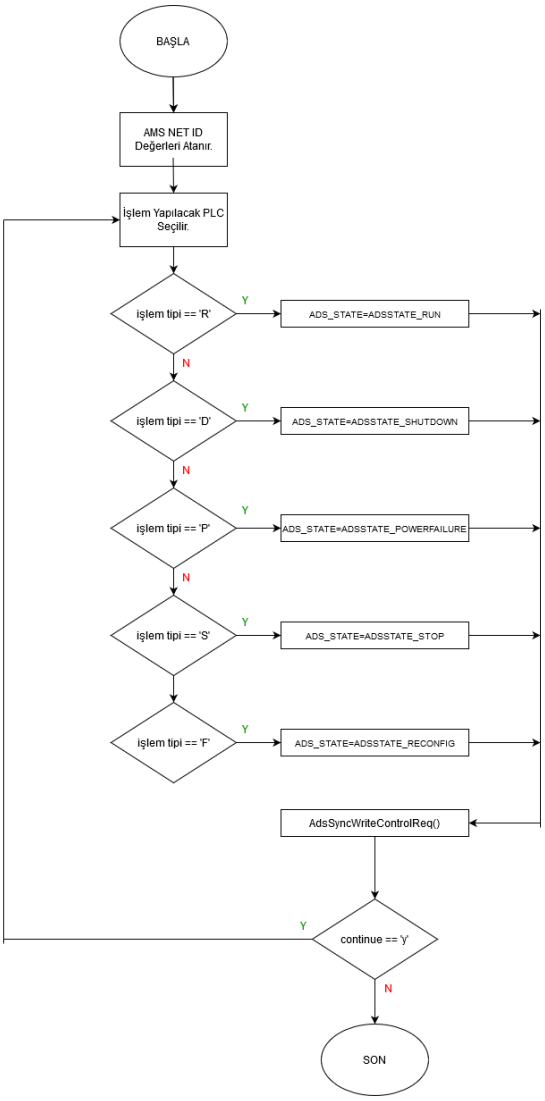
3.2.2. PLC çalışma durumlarının değiştirilmesi

PLC yapılandırma durumları AMS protokolü üzerinden iletilmektedir. AMS iletişimi için mühendislik bilgisayarı üzerinde çalışan TwinCAT programı ile PLC'lerin çalışır durumdan yapılandırma durumuna geçişi sırasında ET2000 cihazı ile ağ kaydı alınıp kaydedilmiştir. Kaydedilen AMS PCAP dosyası incelendiğinde PLC cihazların çalışır durumdan yapılandırma durumuna geçiş yapması için *ADS State* alanının 5 değerinden 15 değerine veya Tablo 3.1.'de belirtilen herhangi başka bir değere geçmesi gerekir. ADS değerlerinin tablosu Tablo 3.1.'de verilmiştir.

Tablo 3.1. PLC durumlarına göre ADS değerleri

PLC Durumu	**ADS Değeri**
Run	5
Stop	6
Shutdown	12
Config	15
Reconfig	16

Ek-1'de verilen C++ kodu geliştirilerek bu durumlara uygun olarak PLC cihazların Tablo 3.1.'de belirtilen durumlara geçmesi sağlanmıştır. Kodun akış diyagramı Şekil 3.4.'te verilmiştir.



Şekil 3.4. PLC cihaz durum değişimi akış diyagramı

Kod içerisinde sistemde bulunan 4 adet PLC cihazların AMS Net ID değerleri yazılmış olup (Şekil 3.4.) istenilen PLC cihazın çalışma durumunun değiştirilmesi sağlanmıştır. Bu değişimin sağlanması için saldırı yapılacak makine ile sistem arasında fiziksel "*Route"* eklenmesi gerekmektedir. Yapılan çalışmada saldırgan makineye kurulan TwinCAT üzerinden bu işlem yapılmıştır. PLC cihazların durum değişimleri (Şekil 3.5. ve Şekil 3.6.) cihazların üzerinde bulunan LED ışıklarının değişiminden gözlemlenmiştir.

```
--------------------------------------
1- AMS ID Aritma_PLC: 5.68.121.88.1.1
2- AMS ID Terfi1_PLC: 5.68.121.85.1.1
3- AMS ID Terfi2_PLC: 5.60.78.57.1.1
4- AMS ID Depo_PLC: 5.60.78.21.1.1
5- AMS ID Eng Station: 10.9.16.189.1.1
--------------------------------------
Please enter a number of AMSID

2

(R) -> Run
(D) -> Shutdown ->> shut down system and restart in run mode
(P) -> Power Failure ->>sytem completely stops, hard restart is required
(S) -> Stop
(F) -> Reconfig ->> shut down system and restart in config mode
```

Şekil 3.7. PLC durumlarının değiştirilmesini sağlayan program

Şekil 3.5. PLC Durdurulması

Şekil 3.6. PLC Yapılandırma moduna geçilmesi

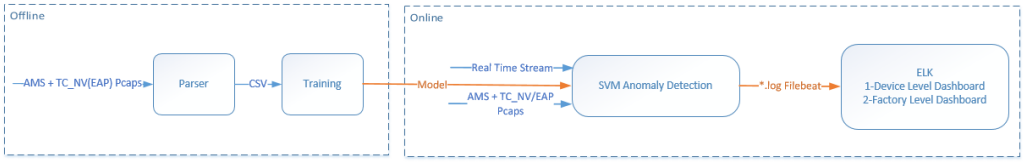
3.2.3. Servis dışı bırakma saldırısı

Çalışan sisteme tek bir kaynak üzerinden yüksek bir ağ trafiği ile su artıma işleminin durdurulması sağlanmıştır. Sistemden alınan PCAP dosyası Kali işletim sisteminde bulunan *tcpreplay* aracının *loop* parametresi 5000000 verilerek çok sayıda ağ akışı oluşturularak süreç durdurulmuştur.

3.3. Makine Öğrenmesi ile Anomali Tespiti ve Görselleştirilmesi

Bölüm 3.2 içerisinde oluşturulan saldırı vektörlerinin tespiti için SVM algoritması kullanılmıştır. SVM algoritması istatistiksel öğrenme temelli gözetimli öğrenme algoritmasıdır. Genellikle regresyon ve sınıflandırma gerektiren problemlerde kullanılmaktadır. Fabrika seviyesinde gerçekleştirilen saldırıların tespit programına göre gerçek zamanlı olarak akan trafikten öğrenme gerçekleştirilmektedir. Bu öğrenme akan trafikten saldırıların tespitinde kullanılacak parametreler ayrıştırılıp CSV dosyasına kaydedilerek gerçekleştirilmiştir. Öğrenme sonucunda oluşan model bir dosyaya kaydedilerek sonrasında yapılan saldırılar bu modele göre değerlendirilip PLC cihazlarının durumları sınıflandırılmıştır. Sınıflandırılan saldırılar ELK sistemine aktarılarak görselleştirilmiştir.

Şekil 3.8.'de verilen akış Ubuntu 19 üzerinde Python3.6 programlama dili ile gerçekleştirilmiştir. Doğrusal (lineer) SVM algoritması kullanılmıştır.



Şekil 3.8. Saldırı Tespit Sistemi Akışı

SVM algoritmasının öğrenme kısmında öznitelik olarak ilk önce 7 adet öznitelik kullanılmıştır. Bunlar, *cmd_id, data_len, ads_state, protocol, ethercat_datalen, packet_count* ve *tc_var_id.*

- *"Cmd_id"*, AMS alt protokolünün bir alanı olup PLC'ler arası iletişimde gönderilen ve alınan paketlerin komut türlerini belirlemektedir. Bu alanın alabileceği değerler Tablo 3.2.'de belirtilmiştir.
- Alınan paketlerin ilettikleri verilerin uzunlukları da taşınan veri kadar önem arz etmektedir. Veri uzunluğu, taşınan komut türü ve okuma/yazma isteklerine göre değişkenlik göstermektedir. Bu nedenle "*data_len*" alanı da öznitelik olarak seçilmiştir.
- "*Ads_state*" alanı PLC cihazların anlık durumlarını tutan bir değişkendir. Örneğin Run durumunda olan bir PLC'ye veri akışı sağlanabilirken, yapılandırma yapılamamaktadır. Bunun için Configuration durumuna alınması gerekmektedir. PLC ADS durum bilgilerinin iletişim şeklini belirlediğinden dolayı bu değer de öznitelik olarak belirlenmiştir.
- "*Protocol*" alanı da fabrika seviyesinde birçok alt protokol kullanıldığından, protokol bazlı tanımlamayı temsil etmektedir. Bu nedenle seçilmiştir. Test ortamında çalışan EtherCAT protokolünde AMS ve TC_NV alt protokolleri ile çalışmalar yapılmıştır bu yüzden bu öznitelik 2 değer alabilmektedir.
- EtherCAT fabrika seviyesindeki prosese özel veriler *data* alanında taşınmaktadır. Kullanılan topolojide istasyonların seviye bilgisi gibi verilerde bu alanda iletilmektedir. Bu nedenle ilgili alanın taşıdığı veri uzunluğu "*ethercat_data_len*" özniteliği olarak seçilmiştir.
- *"Packet_count"* özniteliği DoS gibi paket sayısının belirleyici olduğu durumlar için seçilmiştir. Öznitelik değeri, ardışık gelen 2 paket arasındaki varışlar arası zamana bakılarak belirlenmektedir.

Fabrika seviyesinde değişen verilerin bir ID numarası bulunmaktadır. Bu protokol alanı içinde "*tc_var_id"*" de saklanmaktadır. Bu nedenle ilgili değer öznitelik olarak başlangıçta belirlense de geliştirilen saldırı vektörlerinin tespitinde SVM tarafından, diğer özniteliklere göre etkisinin az olduğu görülmüş ve sonraki tespitlerde kullanılmamıştır.

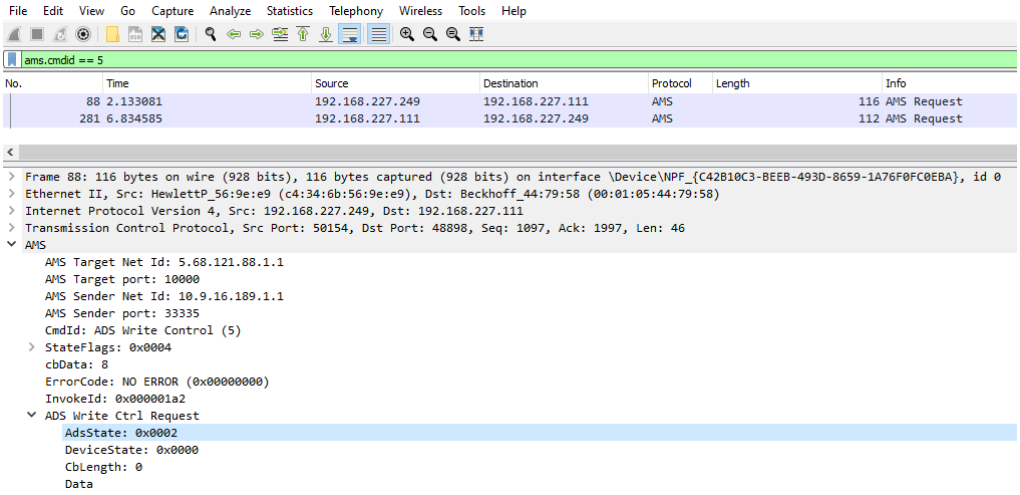
Ağ paketleri içeriğindeki değerler karmaşıklık göstermediğinden öznitelik seçiminde herhangi bir indirgeme yöntemi kullanılmamıştır.

Öğrenme sonucunda oluşan model bir dosyaya kaydedilerek sonrasında yapılan saldırılar bu modele göre değerlendirilip PLC cihazlarının durumları sınıflandırılmıştır. Sınıflandırılan saldırılar ELK sistemine aktarılarak görselleştirilmiştir.

PLC cihazlarının ADS durum değişimini yapmak için CMD ID değeri 5 olan *Write Control Request* fonksiyonu kullanılmıştır. CMD ID değeri 5 olan paketlerin içerisinde PLC cihazın durum bilgisini tutan *AdsState* alanı Şekil 3.9.'daki gibi bulunmaktadır.

Tablo 3.2. CMD ID değerleri

CMD ID	**Açıklama**
0	Geçersiz
1	ADS Read Device Info
2	ADS Read
3	ADS Write
4	ADS Read State
5	ADS Write Control
6	ADS Add Device Notification
7	ADS Delete Device Notification
8	ADS Device Notification
9	ADS Read Write



Şekil 3.9. AMS ağ paketi içeriği (CmdId=5)

Ads State alanı Şekil 3.4.'te akış diyagramı verilen kod içerisinde belirtildiği üzere değiştirilerek saldırılar yapılabilmektedir. Saldırı tespitinde bu değişimi algılayabilmek için öznitelik olarak ağ paketlerinden ayrıştırılma işlemi yapılmıştır. PLC cihazların durum kodlarının belirlendiği bu alandaki değerlerden *Stop, Power Failure, Reconfig* ve *Shutdown* durumları kullanılmıştır.

PLC cihazlar arasındaki iletişimin *Write Control Request* isteği içeren *Cmd ID* değerinin 5 olması durumunda;

- Eğer Ads_state = 6 ise PLC durumu STOP saldırı tipi A3,
- Eğer Ads_state = 9 ise PLC durumu POWER FAILURE saldırı tipi A4,
- Eğer Ads_state = 16 ise PLC durumu RECONFIG saldırı tipi A5,
- Eğer Ads_state = 12 ise PLC durumu SHUTDOWN saldırı tipi A6,
- Eğer bu durumlardan hiçbiri sağlanmıyorsa normal paket olarak algılanıp, atak tipi A100 olarak kabul edilmiştir.

EAP iletişimi üzerinden, seviye değişimi ve seviye değişimine bağlı motorların çalıştırılıp durdurulması saldırısı Bölüm 3.2 içerisinde açıklanmıştır. A6 atak tipine sahip bu saldırıyı tespit edebilmek için, her 1 saniyede art arda gelen paketlerde veri uzunluğu 4'ten büyük olan paketler kontrol edilmiştir. Eğer veri uzunluğu 4 ise su prosesindeki seviye değerini taşıyan veri alanı 0 gelmektedir. TC_NV paketlerindeki

veri alanının son 8 byte uzunluğundaki alan sondan başa okunup *float* değerine çevrilmiştir. Gelen paketler arasındaki fark her bir motorun su tanklarına bastığı su miktarı, PLC cihazlar üzerinde yapılan programlama baz alınarak hesaplanıp *false positive* saldırı alarmlarının oranını düşürmek için (-1.0) ve 1.0 aralığı seçilmiştir. Sistemde her PLC cihaz için gelen paketler arasındaki fark bu aralıkta ise bir sonraki pakete geçilir. Eğer bu aralığın dışına çıkma durumu oluşursa seviyedeki ani artış veya ani düşüş saldırı olarak algılanmaktadır.

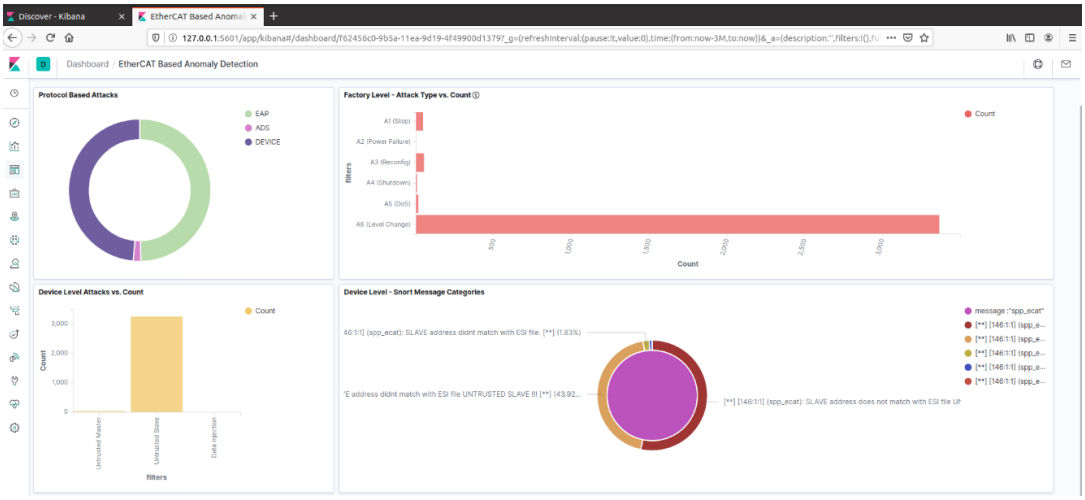
Fabrika seviyesi saldırı tespit sistemi, sadece test ortamında yer alan PLC cihazları değil, sisteme eklenen başka yayınlayıcı (*Publisher*) cihazların eklenmesi durumunda, cihaz bazlı seviye kontörlü yaptığından, seviye kontrolü yapılmaya devam edecektir. Bu kontrol her cihaz için tek değer olan AMS Net ID değeri ağ paketlerinden elde edilerek anahtar değer olarak kullanılmıştır. Her yayınlayıcıya özgü bu değer PLC cihazın kimliğini temsil etmektedir.

Saldırıların görselleştirilmesi için açık kaynak kodlu ELK Stack programı kullanılmıştır. Saldırıların SVM algoritması ile sınıflandırılmasından sonra oluşan *log* dosyaları *filebeat* ile ELK makinesine aktarılmış ve saldırılara ait detaylı verilerin grafiksel olarak görüntülendiği *dashboard* ekranları Kibana içerisinde bulunması sağlanmıştır.

Şekil 3.10.'da verilen grafiklerde protokol tabanlı *Pie Chart* grafiği oluşturulmuştur. Seviye değişim saldırısının yapıldığı A8 kodlu saldırı EAP alt protokolü ve PLC cihazların çalışma durumlarının değiştirilmesine yönelik yapılan A1-A5 kodlu saldırıların kullanıldığı ADS alt protokolüne ait yüzdesel dağılım belirtilmiştir. Bu grafik ayrıca Bölüm 1'de belirtilen Tübitak 1005 projesi kapsamında çalışan saha seviyesi alt protokollerine ait bilgiler de "*Device*" etiketi ile mevcuttur.

A1-A6 aralığındaki saldırıların makine öğrenmesi sonucunda üretilen alarmların sayılarına göre dağılımları çubuk grafik olarak görselleştirilmiştir. Son iki grafik Tübitak 1005 projesindeki saha seviyesine ait saldırı tespit alarmlarına ait grafiklerdir.

Tüm grafikler gerçek zamanlı olarak sistem üzerindeki değişimler gözlemlenebilmektedir. İstenirse belirli zaman aralığı seçilerek grafikler güncelleştirilebilmektedir.



Şekil 3.10. Saha cihazlarında saldırı tespit grafikleri

3.4. Sonuçlar

Bu bölümde fabrika seviyesindeki saha cihazları üzerinde DoS ve PLC durum değiştirme gibi yapılan saldırıların, makine öğrenmesi algoritmalarından biri olan SVM kullanılarak tespit edilmesi gerçekleştirilmiştir. Bu saldırılara ek başka saldırıların tespit edilmesi program içerisinde esnek bırakılarak model güncellenebilir ve ilgili çözüm hızlıca entegre edilebilmektedir. Tespit sistemi, bilinen ve eğitilmiş modelde yer alan saldırılara yönelik bir çözüm oluşturmaktadır. Elde edilen çözüm cihaz veya protokol temelinde çıkan herhangi bir sıfırıncı gün zafiyetini tespit edememektedir.

Saldırıların SVM algoritması ile sınıflandırılmasından sonra tespit edilen ataklar log dosyalarına kaydedilmiştir. Oluşan log dosyaları *filebeat* ile ELK makinesine aktarılmıştır. Saldırılara ait detaylı verilerin grafiksel olarak görüntülendiği *dashboard* ekranları Kibana içerisinde oluşturulmuştur. A3-A6 arasındaki aralığındaki saldırı tipleri, AMS tabanlı PLC cihazların çalışma durumlarına yönelik

atak tipi kodlarıdır. A7 Servis Dışı Bırakma (DoS) saldırısı ve A8 ise seviye değişimine bağlı motorların çalışma durumunun kontrol edilmesini ifade eder.

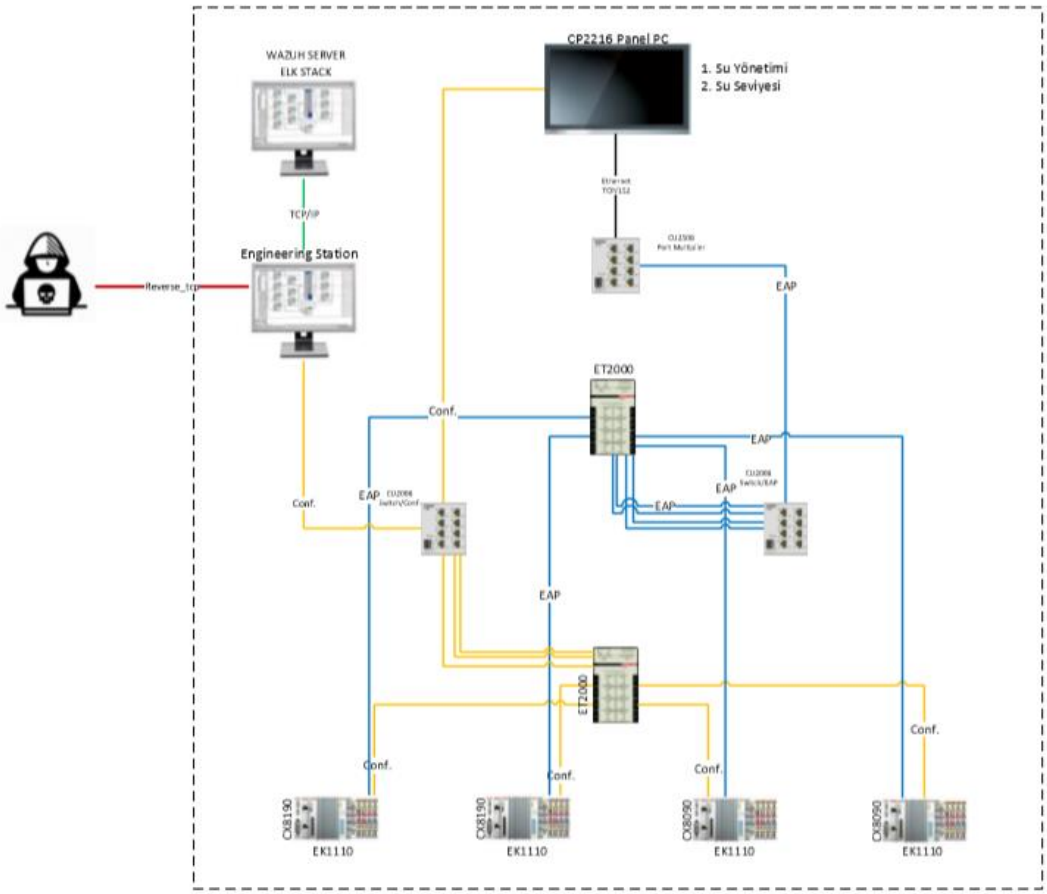
Fabrika seviyesinde yapılan saldırıların tespitine yönelik çalışmaların sonucunda ELK sisteminde görselleştirilmesi çeşitli grafiklerle sağlanmıştır. Bu grafikler, saldırıların hangi protokollerde yapıldığı, saldırıların yoğun olduğu zaman aralığı, saldırı çeşitlerine göre saldırı miktarları okunabilir ve yorumlanabilir olmaktadır. Ayrıca bu grafikler üzerinden sistem izleme işlemi zamanla ileriye dönük olası saldırıların tahmini veri bilimi alanı ile birleştirilerek elde etme imkânı sunabilir.

Fabrika seviyesinde sistemi izlemek için entegrasyonu sağlanan ELK sistemiyle cihazların takibi kolaylaştırılmıştır. Zamana göre saldırıların analizi, sistem açıklıklarının takibi gibi önemli kriterlerle ilgili hem görsel hem de sayısal oranlar üzerinden bilgi alınması sağlanmıştır. Test ortamında yapılan işlemlerden anlık bilgi alınmak istenirse görsel olarak eklenme yapılabilir durumdadır.

BÖLÜM 4. SCADA ve KONTROL MERKEZİ ATAKLARININ MITRE ICS ATT&CK MATRİSİNE GÖRE GERÇEKLEŞTİRİLMESİ VE TESPİTİ

4.1. Test Ortamı

EKS sistemlerinde saha cihazlarıyla iletişim halinde olan ve saha cihazlarını kontrol eden üst seviye makineler mevcuttur. Laboratuvar ortamında oluşturulan ve içerisinde endüstriyel kontrol sistemlerinin SCADA, OPC, mühendislik bilgisayarı vb. gibi çeşitli bileşenlerini içeren iş istasyonları bulunmaktadır. Gerçek sistemlerde yapılan APT saldırılarının birçoğu yanlış yapılandırılmış, güvenlik sıkılaştırmaları yapılmamış veya kimlik denetimi eksikliği gibi birçok güvenlik kontrollerinin eksikliğinden faydalanılarak gerçekleştirilmiştir. Sisteme dışarıdan ilk erişimi sağlamak için çeşitli sosyal mühendislik yöntemleri bulunmaktadır ancak EKS üzerinde yapılan bu çalışmada saldırganın Purdue mimarisinin 3. Katmanında olduğu varsayılarak var olan su prosesi üzerinde olası APT senaryoları gerçekleştirilmiştir. Gerçekleştirilen senaryolar MITRE ICS ATT&CK matrisindeki taktik ve tekniklere göre oluşturulmuştur. Senaryolar Şekil 4.1.'deki topoloji üzerinde uygulanmıştır.



Şekil 4.1. Saldırı senaryolarının gerçekleştirildiği topoloji

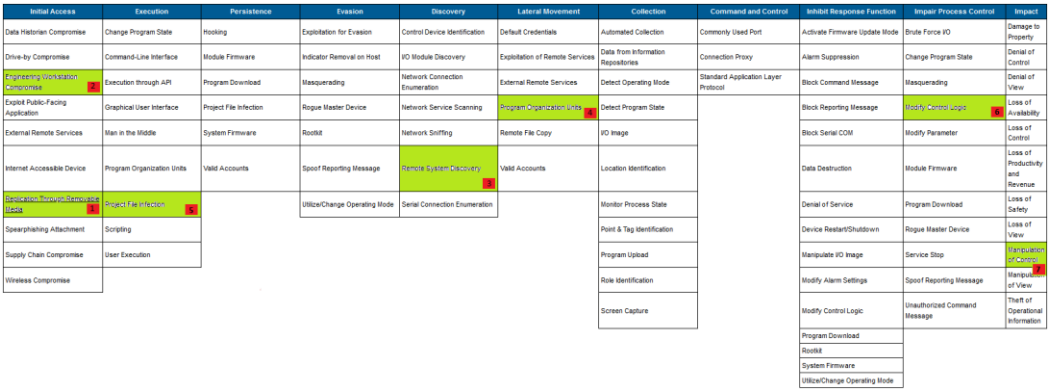
Test ortamında, Windows 10 işletim sistemine ait iş istasyonu, PLC cihazlara komut gönderen ve otomasyonun işleyişinin merkezi olan mühendislik bilgisayarı, Windows 10 iş istasyonu bulunmaktadır. Saldırgan bilgisayarının içinde VMWare Workstation Pro 15 ortamında Ubuntu 19 sanal makinesi oluşturulmuştur. Siber güvenlik araçlarını bir arada barındıran Kali Linux işletim sisteminin saldırgan bilgisayar olarak seçilmemesinin sebebi okul ağından Kali işletim sistemine indirilmesi için eklenen repoların güncellemesinde ağda engelleme yapmasından dolayıdır.

Sistem izlemede çok fazla olay meydana gelebilmektedir. Bu olayların önemlilik derecesine göre analiz edilip alarm oluşturulması gerekmektedir. Böylece doğru zamanda olay müdahalesi yüksek oranda gerçekleştirilmesi sağlanır. Saldırıların tespiti ve okunabilirliği için Wazuh HIDS CentOS 7 üzerine Cluster yapı olarak

kurulmuştur. Mühendislik iş istasyonuna *ossec agent* kurulumu yapılmıştır. Windows sistemler uygulama, sistem ve güvenlik loglarını varsayılan olarak üretmektedir. Ancak DNS sorguları, kullanıcı giriş-çıkış işlemleri gibi birçok olayın logları alınamamaktadır. Bu kritik logların alınabilmesi için mühendislik bilgisayarı üzerinde Sysmon kurularak varsayılanın dışındaki olayların da loglanması sağlanmıştır. Üretilen logların Wazuh sunucusuna aktarılması *ossec agent* ile sağlanmıştır. Wazuh sunucusunda analiz edilip oluşan alarmların görselleştirilmesi için ELK Stack yapısı kurulmuştur. Bu kurulum ve entegrasyonlar Ek 3'te verilmiştir.

4.1.1. Su prosesinde tahliye senaryosuna yapılan saldırı

Su prosesinde tahliye, sirkülasyon ve boşaltım olmak üzere motor ve vanaların farklı çalışma prensibine dayanan üç farklı senaryo bulunmaktadır. Tahliye senaryosunda sistemde bulunan barajın motorları normalde çalışmamaktadır. Burada amaç tahliye senaryosu seçildiğinde barajdaki motorların çalışmasını sağlamaktır. Bu amaçla MITRE ICS ATT&CK matrisinde kullanılan taktik ve tekniklerin haritalandırılması Şekil 4.2.'de belirtildiği gibidir. Şekil 4.2.'de görüldüğü üzere bir teknik birden fazla taktik altında yer almaktadır. İlgili işaretlemeler saldırı senaryosunun amacına uygun taktik seçilmesiyle yapılmıştır.



Şekil 4.2. Saldırı senaryosunda seçilen tekniklerin MITRE ICS ATT&CK Matrisi

Bölüm 4.1'de belirtildiği gibi saldırgan makinesi Purdue mimarisinin üçüncü katmanında olduğu varsayılmış olup ilk erişim için hedef, mühendislik bilgisayarıdır. Bu doğrultuda Şekil 4.2.'de belirtilen taktik ve tekniklerin uygulanma şekilleri sırasıyla önlemleriyle beraber aşağıda belirtilmiştir.

a. MITRE ICS ATT&CK Matris Kodu: T847

Taktik/Teknik Adı*: Initial Access/* Replication Through Removable Media

Siber saldırganlar, endüstriyel sistemlerin yönetimini sağlayan kontrol sistemleri ortamına yerleştirilebilen harici cihazlar kullanarak sisteme ilk giriş yapabilirler. Bu teknik, güvenilmeyen ağlara asla bağlanmayan, ancak fiziksel olarak erişilebilen hedef cihazlara ilk erişim sağlar. Bu yöntemi kullandığı bilinen zararlı yazılımlar, *Stuxnet* ve *Conficker* zararlı yazılımlarıdır. *Stuxnet*, çıkarılabilen sürücüler aracılığıyla kendini çoğaltma yeteneğine sahiptir. İç tehdit olarak veya bilinmeyen üçüncü taraf çıkarılabilir medyanın hedef ortama bulaştırmış olabilir [48]. *Conficker,* Windows işletim sistemi sürücü paylaşımlarından yararlanmaktadır. Bir bilgisayara bulaştıktan sonra, *Conficker* otomatik olarak kendini ağ içindeki diğer bilgisayarlardaki görünür tüm açık sürücü paylaşımlarına kopyalar. Nükleer enerji santrali yetkilileri, evden veya elektrik santralinin tesisinde bulunan bilgisayarlardan yanlışlıkla USB sürücüde *Conficker'a* getirilen birisinin şüpheli olduğundan şüphelenmektedir [48].

Test ortamında kullanılan bu teknik, Meterpreter kullanılarak saldırgan bilgisayara bağlantı açılmasını sağlayan exe dosyası oluşturulup mühendislik bilgisayarına USB cihaz ile aktarılıp çalıştırılması sağlanmıştır.

Bu tekniğe karşı alınabilecek önlemler, makineler üzerinde USB cihazların otomatik çalıştırılma özelliği devre dışı bırakılmalıdır. Güvenlik politikaları kapsamında izin verme veya belirli düzeye göre kısıtlama işlemleri uygulanmalıdır.

b. MITRE ICS ATT&CK Matris Kodu: T818
Taktik/Teknik Adı: Initial Access/Engineering Workstation Compromise
Bir mühendislik iş istasyonu, kontrol sistemi ekipmanlarını ve uygulamalarını yapılandıran, koruyan ve tanılayan güvenilir bir bilgi işlem platformu olarak tasarlanmıştır ve güvenliğinin aşılması, diğer kontrol sistemi uygulamalarına ve ekipmanlarına erişim ve kontrol sağlayabilir. Siber saldırganlar, kontrol sistemi ortamına ilk erişim olarak bir mühendislik iş istasyonunun kontrolünü ele geçirebilir. Bir mühendislik iş istasyonuna erişim, uzaktan erişimin bir sonucu olarak veya çıkarılabilir medyadan bulaşan bir zararlı yazılım gibi fiziksel yollarla gerçekleşebilir [49]. *Maroochy* saldırısında saldırgan, bir atık su sistemiyle iletişim kurmak için mühendislik yazılımı ile çalınan bir bilgisayar kullanmıştır. Bu yöntemi kullandığı bilinen zararlı yazılımlar, *Stuxnet* ve *Triton* zararlı yazılımlarıdır. *Stuxnet,* PLC cihazları için ilk erişim noktası olarak bir mühendislik iş istasyonu kullanmıştır. *Triton*, bir SIS mühendislik iş istasyonuna uzaktan erişim kazanarak bu yöntemi kullanmıştır [49].

Test ortamında kullanılan bu teknik, bir önceki tekniğin uygulanması sonucunda oluşan durumdur. Saha cihazlarına erişim ve kontrollerini sağlamak için mühendislik bilgisayarı, topoloji içerisinde sistem izlemesinin gerekli olduğu kritik öneme sahip makinelerden biridir.

c. MITRE ICS ATT&CK Matris Kodu: T846
Taktik/Teknik Adı: Discovery/ Remote System Discovery

Uzaktan Sistem Bulma, bir ağdaki ana bilgisayarların varlığını ve bunlarla ilgili ayrıntıları belirleme işlemidir. Bu süreç, makinelerin ve servislerin varlığını doğrulayan ağ yöneticileri ve gelecekteki saldırı hedefleri için bir ağı haritalayan saldırganlar için ortaktır [50]. Bir saldırgan, port taraması gibi ağ numaralandırma teknikleri aracılığıyla hedef ağ hakkında bilgi edinmeye çalışabilir. Uzak Sistem Bulma, saldırganların ağdaki ana bilgisayarların yanı sıra açık, kapalı veya filtrelenmiş TCP/IP bağlantı noktalarını haritalamasına izin verir [50]. Ayrıca hizmete bağlanmaya ve tam sürümünü belirlemeye çalışarak da yardımcı olur. Saldırgan, belirli bir sürüm için bilinen bir güvenlik açığı varsa kötüye kullanıma seçmek için bu bilgileri kullanabilir [50]. Bu yöntemi kullandığı bilinen zararlı yazılımlar, *Havex, Industroyer*, *PLC-Blaster, Stuxnet* ve *Triton* zararlı yazılımlarıdır. *Havex,* ağ üzerinden güvenliği ihlal edilen makine tarafından erişilebilen OPC sunucuları da dahil olmak üzere tüm sunucuları bulmak için Windows ağına (WNet) dayanır. *Industroyer,* IEC 61850 yükü etkilenen makinedeki arabirimler için alt ağ maskelerinin her biri için olası tüm IP adreslerini numaralandırır ve bu adreslerin her birinden bağlantı noktası 102'ye bağlanmaya çalışır. Bu nedenle, bu bileşen ağdaki ilgili cihazları otomatik olarak bulma yeteneğine sahiptir. *PLC-Blaster,* enfekte olacak diğer Siemens S7 PLC cihazlarını bulmak için ağı tarar. TCP bağlantı noktası 102'de dinleyerek bu aygıtları bulur. *Stuxnet*, ağı, hedeflediği Siemens PLC'leri tanımlamak için tarama yapmıştır. Triton, bağlantı noktası 1502 üzerinden belirli bir UDP yayın paketi göndererek ağ üzerindeki *Triconex* denetleyicilerini algılayabilen bir Python betiği kullanır.

Test ortamında kullanılan bu teknik, bağlantı kurulan mühendislik bilgisayarının ARP tablosundaki MAC adresleri üzerinden Ethernet kartlarının modeli belirlenmiştir. ARP tablosuna ulaşmak için *Metasploit* içerisinde bulunan *arp_scanner* aracı kullanılmıştır. Elde edilen MAC adresleri internetten arama yapılarak *Beckhoff* üreticisine sahip cihazlar olduğu belirlenmiştir.

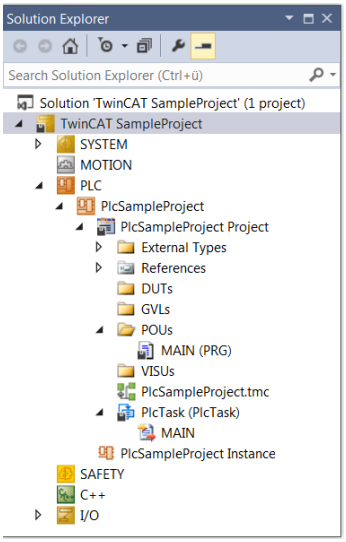
Bu tekniğe karşı alınabilecek önlemler, ağ izleme ve mümkünse kontrol sistemi cihazlarına ve bu cihazlardan erişim noktalarını azaltmak için beyaz liste gibi erişim kontrolü uygulaması gerçekleştirilmelidir.

d. MITRE ICS ATT&CK Matris Kodu: T844

Taktik/Teknik Adı: Lateral Movement/ Program Organization Units

Program Organizasyon Birimleri (POU'lar), programlar ve projeler oluşturmak için PLC programlamasında kullanılan blok yapılardır. POU'lar IEC 61131-3 dillerinde yazılan kullanıcı programlarını tutmak için kullanılabilir ve dört farklı türde yazılabilmektedir: Yapısal metin, Talimat listesi, İşlev bloğu ve Merdiven mantığı (Ladder Logic) [51]. Bu yöntemi kullandığı bilinen zararlı yazılımlar, *PLC-Blaster* ve *Stuxnet* yazılımlarıdır. *PLC-Blaster*, kendisini hedef aygıttaki çeşitli Program Organizasyon Birimlerine (POU) kopyalar. *Stuxnet*, hedef sistemin özelliklerine bağlı olarak PLC'leri farklı kodlarla enfekte eder. Bir enfeksiyon dizisi, davranışını değiştirmek için PLC'ye indirilecek kod blokları ve veri bloklarından oluşur [51].

Bir önceki teknik kullanılarak sistemde Beckhoff cihazların var olduğu tespit edilmişti. Beckhoff cihazların kontrolünü sağlayan programın geliştirilmesi ve cihazlara yüklenmesi için gerekli programın TwinCAT geliştirme ortamı internet ortamında yapılan araştırmada bulunmuştur. TwinCAT programının kendine özgü yazım biçimi ve proje yapısı mevcuttur. Hedef sistemdeki yapıyı daha iyi modellemek için saldırgan bilgisayarına ücretsiz lisansla kurulan TwinCAT programında örnek bir proje oluşturulmuştur. Böylece hedef sistemde olası kritik dosyalarla ilgili tahminler elde edilmiştir. Standart bir TwinCAT projesi oluşturulduğunda proje yapısı Şekil 4.3.'teki gibi oluşmaktadır.



Şekil 4.3. TwinCAT3 proje yapısı

Şekil 4.3.'te görüldüğü üzere MAIN yani PLC üzerinde çalışacak kodun bulunduğu dosya POUs klasörü içerisindeki MAIN dosyasıdır. Bu bilgilere dayanarak hedef bilgisayar üzerinde çalışan prosesler listelenerek hangi prosesin hangi dizin altında olduğu bulunmuştur. Böylece POUs dizinindeki MAIN dosyasına erişim için arama yapılacak alan daraltılmıştır. Mühendislik bilgisayarının masaüstünde "SU ARITMA" klasörünün içerisinde "Ethercat" dizininde bulunmuştur. Bulunan MAIN.TcPOU dosyası saldırgan makinesine indirilmiştir. MAIN.TcPOU kodu içerisinde yorum satırlarının yardımı ve önceden var olan programlama bilgilerine göre tahliye senaryosundaki motorların çalışması ile ilgili kısım normalde Şekil 4.4.'teki gibidir. Baraja ait motor değerleri Şekil 4.5.'teki gibi değiştirilip kaydedilmiştir.

```
        // Hızlı Boşalt Senaryo
        IF senaryo_secim=3 THEN
            baraj_veri.motor1:=FALSE;
            baraj_veri.motor2:=FALSE;
            baraj_veri.motor3:=FALSE;
            IF su_yeterli THEN
                IF terfi_1_suSeviyesi<24 THEN
                    aritma_veri.motor1:=TRUE;
                    aritma_veri.motor2:=TRUE;
                    aritma_veri.motor3:=TRUE;
                END_IF
                IF terfi_1_suSeviyesi>25 THEN
                    aritma_veri.motor1:=FALSE;
                    aritma_veri.motor2:=FALSE;
                    aritma_veri.motor3:=FALSE;
                END_IF
                ELSE //su yeterli else
                    aritma_veri.motor1:=FALSE;
                    aritma_veri.motor2:=FALSE;
                    aritma_veri.motor3:=FALSE;
            END_IF
        END_IF

    ELSE    //panel start else
                aritma_veri.motor1:=FALSE;
                aritma_veri.motor2:=FALSE;
                aritma_veri.motor3:=FALSE;
                baraj_veri.motor1:=FALSE;
                baraj_veri.motor2:=FALSE;
                baraj_veri.motor3:=FALSE;
END_IF
```

Şekil 4.4. MAIN.TcPOU baraj motor durumlarının orijinal hali

```
        // Hızlı Boşalt Senaryo
        IF senaryo_secim=3 THEN
            baraj_veri.motor1:=TRUE;
            baraj_veri.motor2:=TRUE;
            baraj_veri.motor3:=TRUE;
            IF su_yeterli THEN
                IF terfi_1_suSeviyesi<24 THEN
                    aritma_veri.motor1:=TRUE;
                    aritma_veri.motor2:=TRUE;
                    aritma_veri.motor3:=TRUE;
                END_IF
                IF terfi_1_suSeviyesi>25 THEN
                    aritma_veri.motor1:=FALSE;
                    aritma_veri.motor2:=FALSE;
                    aritma_veri.motor3:=FALSE;
                END_IF
                ELSE //su yeterli else
                    aritma_veri.motor1:=FALSE;
                    aritma_veri.motor2:=FALSE;
                    aritma_veri.motor3:=FALSE;
            END_IF
        END_IF

    ELSE    //panel start else
                aritma_veri.motor1:=FALSE;
                aritma_veri.motor2:=FALSE;
                aritma_veri.motor3:=FALSE;
                baraj_veri.motor1:=FALSE;
                baraj_veri.motor2:=FALSE;
                baraj_veri.motor3:=TRUE;
END_IF
```

Şekil 4.5. MAIN.TcPOU baraj motor durumlarının değiştirilmiş hali

e. MITRE ICS ATT&CK Matris Kodu: T873

Taktik/Teknik Adı: Execution/ Project File Infection

Saldırganlar proje dosyalarına zararlı kod bulaştırabilir. Bu proje dosyaları nesnelerden, program organizasyon birimlerinden, etiketler (tags), belgeler gibi değişkenlerden ve PLC programlarının çalışması için gereken diğer yapılandırmalardan oluşabilir [52]. Mühendislik yazılımının yerleşik işlevlerini kullanarak, saldırganlar, virüslü veya içeriği değiştirilmiş bir programı işletim ortamında bir PLC'ye indirerek daha fazla yürütme ve kalıcılık tekniği sağlayabilir [52]. Bu yöntemi kullandığı bilinen zararlı yazılım, *Stuxnet* zararlı yazılımıdır. *Stuxnet* zararlı yazılımı, kendisini *Step 7* projelerine yüklendiğinde otomatik olarak çalışacak şekilde *Step 7* projelerine kopyalayarak kendini çoğaltır.

Test ortamında kullanılan bu teknik, MAIN.TcPOU dosyasında yapılan mantıksal değişiklik saldırgan bilgisayarından mühendislik bilgisayarında aynı dizin içerisinde kaydedilmiştir.

f. MITRE ICS ATT&CK Matris Kodu: T833

Taktik/Teknik Adı: Impair Process Control/ Modify Control Logic

Saldırganlar, sisteme kötü amaçlı kod yerleştirebilirler, bu da prosesin kontrol mantığını değiştirerek sistemin arızalanmasına veya yanlış neden olabilir. Kontrol sistemi cihazları, çevre sensörü okumalarına dayanarak makinelerin çalışmasına neden olan aktüatörleri etkileyerek fiziksel süreçleri kontrol etmek için programlama dillerini kullanır [53]. Bu cihazlar genellikle uzak erişimle mantık güncellemelerini yapma görevini üstlenmektedirler. Saldırganlar, cihazın çalışma mantığını değiştirmek için ana bilgisayarın hedef IDE'sini kullanmaya çalışabilirler [53]. Üreticilerin sağladığı programlama mantığını kontrol etmek için tersine mühendislik veya açık kaynaklı araçların çoğaltılarak çalışma prensibi anlaşılabilir. Bu yöntemi kullandığı bilinen zararlı yazılım, *Triton* zararlı yazılımıdır. Triton zararlı yazılımı SIS çalışma yapısını değiştirerek güvenli olmayan çalışma ortamı ve kalıcılığı sağlamaktadır.

Test ortamında kullanılan bu teknik, bir önceki teknikte yapılan programsal değişikliğin (mantıksal değişiklik) PLC'lerde etkin olabilmesi için TwinCAT programı tarafından “Activate Configuration” işleminin yapılması gerekir. Bunun için saldırının 4. Adımında alınan proje dosyası saldırgan bilgisayarına kurulu olan TwinCAT programından “Activate Configuration” işlemi yapılarak Tahliye Senaryosuna ait baraj tankında bulunan motorların çalışması sağlanmıştır.

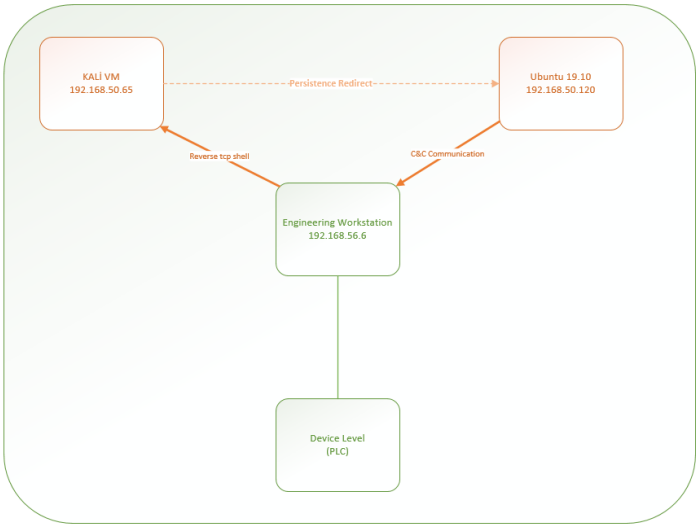
g. MITRE ICS ATT&CK Matris Kodu: T831
Taktik/Teknik Adı: Impact/ Manipulation of Control
Siber saldırganlar, endüstriyel ortamda fiziksel süreç kontrolünü manipüle edebilirler. Kontrolü manipüle etme yöntemleri, ayar noktası değerlerinde, etiketlerde veya diğer parametrelerde değişiklikler içerebilir [54]. Saldırganlar, fiziksel kontrol süreçleriyle iletişim kurmak ve komuta etmek için büyük oranda kendi cihazlarından yararlanırlar. Manipülasyon süresi, operatörün algılamasına bağlı olarak geçici veya daha uzun sürebilir [54].

Test ortamında kullanılan bu teknik, tüm adımların sonucunda su prosesinde bulunan HMI arayüzünden “Tahliye Senaryosu” seçildiğinde oluşan sonuç baraj için

çalışmaması gereken motorların çalışması sağlanarak kontrol yetkisiz olarak değiştirilmiştir.

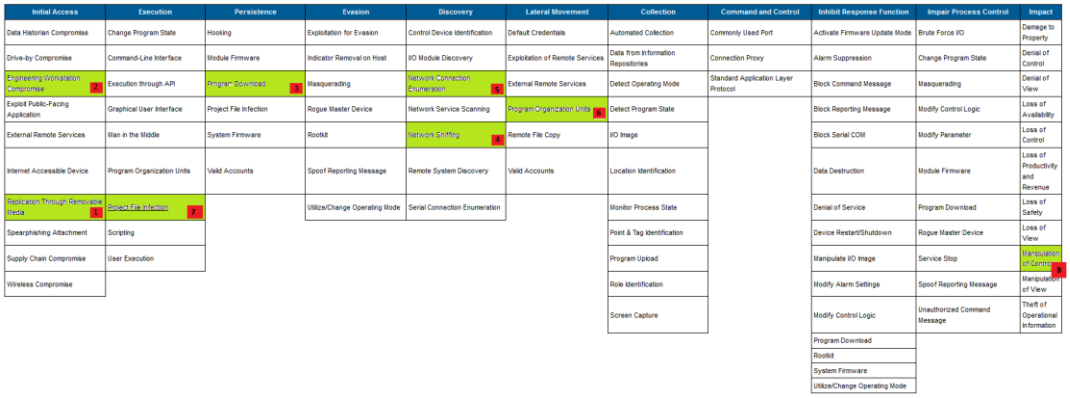
4.1.2. SCADA cihazına yapılan senaryo seçim saldırısı

Gerçekleştirilen saldırı senaryosunda, bir önceki topoloji üzerinde farklı teknikler kullanılarak Arıtma tankını kontrol eden PLC cihazına senaryo seçimine bakılmaksızın aynı işlemlerin yapılmasına yönelik işlemler gerçekleştirilmiştir. Bu saldırıda bir önceki saldırıdan farklı ve önemli bir adım olan mühendislik bilgisayarının C&C sunucuya yönlendirme işlemi üzerinden kalıcılığın sağlanmasıdır. C&C sunucusuna yönlendirme akış şeması Şekil 4.6.'da verilmiştir.



Şekil 4.6. Saldırı akış diyagramı

Şekil 4.6.'daki yapıya göre Kali VM makinesinden mühendislik bilgisayarına "*reverse shell*" bağlantısı ile C&C sunucu işlevi gören ve 4445 portundan dinleme yapan Ubuntu 19.10 sanal makinesine yönlendirme işlemi yapılmıştır. Bu işlemlerin MITRE ICS ATT&CK matrisindeki tekniklerin gerçekleştirilme sırasıyla beraber Şekil 4.7.'de verilmiştir.



Şekil 4.7. Saldırı senaryosunda seçilen tekniklerin MITRE ICS ATT&CK Matrisi

Bölüm 4.1'de belirtildiği gibi saldırgan makinesi Purdue mimarisinin üçüncü katmanında olduğu varsayılmış olup ilk erişim için hedef, mühendislik bilgisayarıdır. Bu doğrultuda Şekil 4.7.'de belirtilen 6 farklı taktik gruplarından seçilen 8 tekniğin uygulanma şekilleri sırasıyla önlemleriyle beraber aşağıda belirtilmiştir.

a. MITRE ICS ATT&CK Matris Kodu: T847

Taktik/Teknik Adı*: Initial Access/* Replication Through Removable Media

Bu teknik Bölüm 4.1.1'de belirtilen teknikle aynı yöntem uygulanarak gerçekleştirilmiştir.

b. MITRE ICS ATT&CK Matris Kodu: T818

Taktik/Teknik Adı: Initial Access/Engineering Workstation Compromise

Bu teknik Bölüm 4.1.1'de belirtilen teknikle aynı yöntem uygulanarak gerçekleştirilmiştir. Mühendislik bilgisayarında ayrıcalıklı modda devam etmek için "*Migrate*" işlemi yapılmıştır. "*Migrate*" işlemi yapılırken sistem kullanıcısına ait bir proses olan "*RtkAudioService64.exe*" proses numarasına göre yapılmıştır.

c. MITRE ICS ATT&CK Matris Kodu: T843

Taktik/Teknik Adı: Persistence/ Program Download

Saldırganlar, kalıcılık yöntemi olarak bir cihaza kötü amaçlı veya istenmeyen program yapısı yüklemek veya işlem denetimini bozmak için bir programın karşıdan yüklenmesini gerçekleştirebilir. PLC gibi cihazlara program indirme, saldırganların özel mantık uygulamasını sağlar. Kötü amaçlı PLC programları, fiziksel süreçleri

bozmak veya olumsuz kalıcılığı sağlamak için kullanılabilir [55]. Bu yöntemi kullandığı bilinen zararlı yazılımlar, *Stuxnet* ve *Triton* zararlı yazılımlarıdır. *Stuxnet,* hedef sistemin özelliklerine bağlı olarak PLC'leri farklı kodlar enfekte eder. Bu kodlar, davranışını değiştirmek için PLC'ye indirilecek kod blokları ve veri bloklarından oluşur. *Triton,* programları Triconex SIS'e indirmek için TriStation protokolünden yararlanmıştır.

Test ortamında kullanılan bu teknik, ICS matrisindeki bu teknik mühendislik bilgisayarı için tanımlanmamış olsa da benzer benzer etkiyi gösterdiğinden bu teknik içerisinde yorumlanmıştır. Kali sanal makinesinden Ubuntu 19.10 sanal makinesine bağlantı sağlayacak olan *.vbs* kodu mühendislik bilgisayarında oluşturulmuştur. Böylece saldırıya devam edecek komutların işletileceği C&C sunucusuna aktarılmıştır. Mühendislik bilgisayarında oluşturulan *.vbs* kodu bilgisayar kapanıp tekrar açıldığında da C&C ile iletişim kurabildiğinden sistem üzerinde kalıcılık sağlanmıştır.

d. MITRE ICS ATT&CK Matris Kodu: T842
Taktik/Teknik Adı: Discovery/ Network Sniffing
Ağ paketlerini yakalama, ağda dolaşan bilgileri izlemek veya yakalamak için bir bilgisayar sisteminde bir ağ arabirimi kullanma yöntemidir. Bir saldırgan, hedef hakkında bilgi edinmek için trafiği yakalamaya çalışabilir. Bu bilgi ağda dolaşan verilerin önem derecesine göre değişebilir. Önemli bilgiler kullanıcı kimlik bilgileri, ağ paketi analizi yoluyla yakalanabilen ve alınabilen Telnet gibi şifrelenmemiş bir protokol üzerinden gönderilebilir [56]. Ağ trafiği yakalama, kontrol cihazı tanımlaması ile ilgili bilgileri elde etmenin bir yolu olabilir.

Test ortamında kullanılan bu teknik, *meterpreter* içerisinde bulunan *sniffer* modülü ile mühendislik bilgisayarına ait trafik yakalanmıştır.

Bu tekniğe karşı alınabilecek önlemler [56]; ağda kablosuz çalışan cihazlar için kablosuz erişim noktalarını ve veri sunucularını, kontrol odasına ve fiziksel ortama yetki verilmesini sağlanması ve kısıtlanması, EKS ve BT ağ kablolarının ayrı

tutulduğundan ve cihazların mümkünse kilitlendiğinin kontrol edilmesi gibi yöntemler kullanılabilir.

e. MITRE ICS ATT&CK Matris Kodu: T840
Taktik/Teknik Adı: Discovery/ Network Connection Enumeration
Saldırganlar, cihaz iletişim standartları hakkında bilgi edinmek için ağ bağlantısı numaralandırması yapabilir. Bir saldırgan, Sistem *Firmware* ile *netstat* gibi araçlarla bir ağ bağlantısının durumunu incelerse, ağdaki belirli cihazların rolünü belirleyebilir. Saldırgan, ağ trafiğini izlemek için ağ paketi yakalama özelliğini de kullanarak kaynak, hedef, protokol ve içerik hakkında ayrıntılar elde edebilir. Bu yöntemi kullandığı bilinen zararlı yazılımlar, *Industroyer* zararlı yazılımıdır. *Industroyer*, TCP/IP alt ağ maskelerini belirlemek için tüm bağlı ağ bağdaştırıcılarını numaralandıran bir IEC 61850 modülü içerir [57].

Test ortamında kullanılan bu teknik, bir önceki teknikten elde edilen mühendislik bilgisayarına ait ağ trafiği dosyası incelenmiştir. Bu trafikte AMS protokolüne ait çerçeve yapıları olduğu tespit edilmiştir. Bu protokol incelendiğinde EtherCAT protokolünün alt protokolü olduğu tespit edilmiştir. AMS alt protokolü mühendislik bilgisayarı ile PLC cihazları arasında, PLC cihazlarına ait yapılandırma durumlarına yönelik komutları taşımaktadır. Böylece ağ içerisinde PLC cihazların olduğu ve ele geçirilen bilgisayarın mühendislik bilgisayarı olduğu tespit edilmiştir.

Bu tekniğe karşı alınabilecek önlemler [57]; kilitli ve fiziksel olarak güvenli olması gereken kontrol odalarına, taşınabilir cihazlara ve çıkarılabilir medyaya erişimin kısıtlanması, beyaz liste (*whitelisting*) gibi erişim denetimleriyle ağ üzerindeki cihazlarla iletişimin kısıtlanması, ağdaki anomali olaylarını tespit etmek için saldırı tespit sistemi kullanımı gibi yöntemler önerilmektedir.

f. MITRE ICS ATT&CK Matris Kodu: T844
Taktik/Teknik Adı: Lateral Movement/ Program Organization Units
Bu teknik Bölüm 4.1.1'de belirtilen teknikle aynı çalışma yapısına sahiptir. Ancak bu saldırıda POU dosyasını bulmak için kullanılan yöntem farklılık göstermektedir.

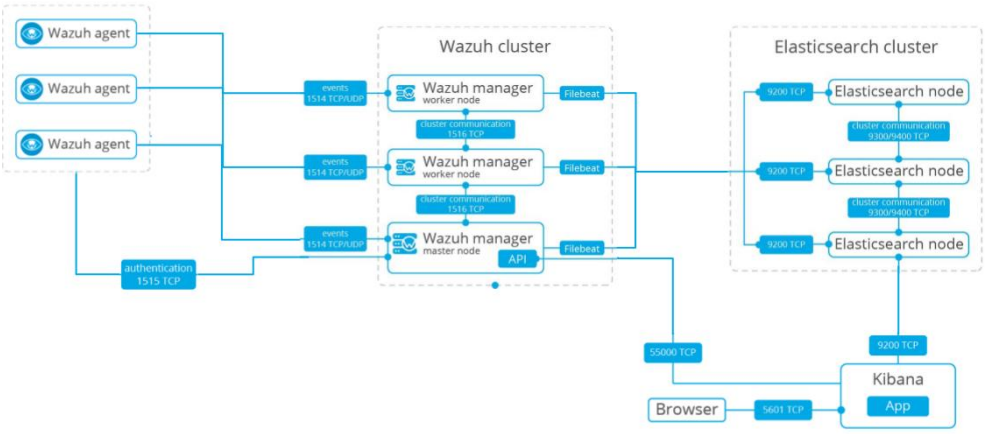
Bilgisayar içerisinde dosya sisteminde arama yapmak için *meterpreter* komut satırından "*search*" komutu ile "*.TcPOU" uzantısına sahip dosyalar listelenmiştir. Listede bulunan dosyalara "*shell*" üzerinden erişilebilmektedir.

g. MITRE ICS ATT&CK Matris Kodu: T873
Taktik/Teknik Adı: Execution/ Project File Infection
Bu teknik Bölüm 4.1.1'de belirtilen teknikle aynı çalışma yapısına sahiptir. Bu senaryoda artıma PLC cihazının senaryo seçimine göre değişen çalışma yapısının her senaryoda aynı şekilde çalışması sağlanması için elde edilen "MAIN.TcPOU" kod dosyası içinde değişiklikler yapılmıştır.

h. MITRE ICS ATT&CK Matris Kodu: T833
Taktik/Teknik Adı: Impact/ Manipulation of Control
Bu teknik Bölüm 4.1.1'de belirtilen teknikle aynı çalışma yapısına sahiptir. Bu saldırının sonucunda su prosesinde arıtma tankındaki su kontrolünü denetleyen PLC cihazının SCADA ekranından seçilen senaryoya bakılmaksızın çalışma prensibi değişmediğinden kontrol merkezinde manipülasyon meydana gelmiştir.

4.2. Wazuh HIDS ile Oluşturulan Alarmların ELK Stack Ortamında Gözlemlenmesi

Bölüm 4.1'de gerçekleştirilen saldırıların tespiti için host tabanlı saldırı tespit sistemi olan Wazuh açık kaynaklı yazılım kullanılmıştır. Wazuh aracı çalışma yapısı gereğince agent bileşeni, sistem içerisindeki bütün makinelere dağıtılıp Wazuh merkez sunucusuna loglarını göndermektedir. Merkez sunucuda oluşan alarmlar Kibana üzerine kurulan Wazuh eklentisi sayesinde Kibana ara yüzünde görüntülenecektir. İletişim detayları tez çalışması içerisinde Bölüm 2.4 içerisinde verilmiştir. Test ortamında gerçekleştirilen saldırıların tespiti için kurulu Wazuh ve ELK Stack mimarisi Şekil 4.8.'de belirtildiği gibidir.



Şekil 4.8. Saldırı tespiti için kullanılan Wazuh HIDS mimarisi

Şekil 4.8.'de belirtilen yapıda Wazuh cluster ve Elasticsearch makineleri CentOS 7 işletim sistemine kurulmuştur. Wazuh agent, mühendislik bilgisayarına kurulmuştur. Kimlik doğrulama için Nginx kurulmuştur, ilgili kurulum ve yapılandırma Ek 2'de belirtilmiştir.

Mühendislik bilgisayarında varsayılan logların haricinde sistem güvenliği ile ilgili üretilen Sysmon olayları, "*Applications and Services Logs/Microsoft/Windows/Sysmon/Operational*" olay günlüğüne kaydeder.

Sysmon kurulduğu zaman varsayılan konfigürasyon dosyası ile kurulum yapar. Eğer sisteme özel logların alınması gerekiyorsa xml formatında harici konfigürasyon dosyası da kullanılabilir. Sysmon konfigürasyon dosyası "*HashAlgorithms*" ve "*EventFiltering*" olarak iki ana bölümden oluşmaktadır. "*HashAlgorithms*" bölümünde sistemde oluşturulan proseslerin kullanacağı *hash* algoritmaları belirtilirken; "*EventFiltering*" alanında özellikle izlenen veya hariç tutulan olayları belirtmek için yazılan kuralların bulunduğu bölümlerdir. Sysmon V11 ile gelen toplam 23 "*Event Filter*" özelliği Tablo 4.1.'de işlevleri ile belirtilmiştir:

Tablo 4.1. Sysmon Event Filter listesi [43]

ID	Tag
1 ProcessCreate	Proses oluşturulması
2 FileCreateTime	Dosya oluşturulma zamanı

Tablo 4.1. (Devamı)

ID	Tag
3 NetworkConnect	Ağ bağlantısı algılanması
4 n/a	Sysmon servis durumu değişikliği-filtrelenemez
5 ProcessTerminate	Proses sonlandırılması
6 DriverLoad	Driver yüklenmesi
7 ImageLoad	Image yüklenmesi
8 CreateRemoteThread	CreateRemoteThread algılanması
9 RawAccessRead	RawAccessRead algılanması
10 ProcessAccess	Process erişimi sağlanması
11 FileCreate	Dosya oluşturulması
12 RegistryEvent	Registry objesi eklenmesi/silinmesi
13 RegistryEvent	Registry değer ataması yapılması
14 RegistryEvent	Registry objesi yeniden isimlendirilmesi
15 FileCreateStreamHash	Dosya akışı oluşturulduğunda
16 N/A	Sysmon konfigürasyonun değiştirilmesi-filtrelenemez
17 PipeEvent	İsimlendirilmiş kanal oluşturulması
18 PipeEvent	İsimlendirilmiş bağlantı oluşturulması
19 WmiEvent	WMI filtrelenmesi
20 WmiEvent	WMI tüketicisi
21 WmiEvent	WMI tüketici filtresi
22 DNSQuery	DNS sorguları
23 FileDelete	Dosya silinmesi

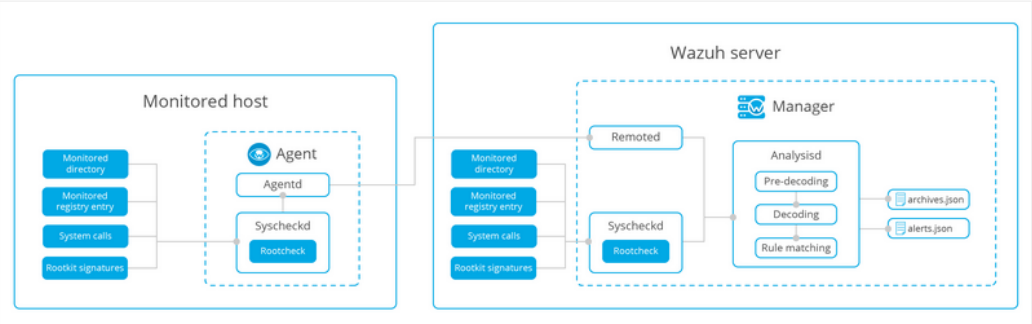
Sysmon kural yapısı temel olarak bir olayın/prosesin/servisin dahil edilmesi (*include*) ya da hariç tutulması (*exclude*) mantığına dayanmaktadır. Tablo 4.1.'de verilen *EventFilter* parametrelerinden herhangi bir tanesi eşleşiyorsa "*onmatch*" anahtar kelimesi ile belirtildikten sonra içerikte hem dahil etme hem de hariç tutma kurallarını içeren senaryolar oluşturulabilir. Her filtre sıfır veya daha fazla kural içerebilir. Bir *EventFilter* içerisinde süreçlerin özel durumlarına göre kural yazmak istenilirse "*is/is, not/, contains/begin with/end with*" vb. ifadelerle koşullar belirtilebilir. Örnek bir kural bloğu Şekil 4.9.'da verilmiştir.

```
<RuleGroup name="" groupRelation="or">
  <!-- Event ID 2 == File Creation Time. -->
  <FileCreateTime onmatch="include">
    <Image name="technique_id=T1099,technique_name=Timestomp" condition="begin with">C:\Temp</Image>
    <Image name="technique_id=T1099,technique_name=Timestomp" condition="begin with">C:\Windows\Temp</Image>
    <Image name="technique_id=T1099,technique_name=Timestomp" condition="begin with">C:\Tmp</Image>
    <Image name="technique_id=T1099,technique_name=Timestomp" condition="begin with">C:\Users</Image>
  </FileCreateTime>
</RuleGroup>
```

Şekil 4.9. Sysmon kural örneği

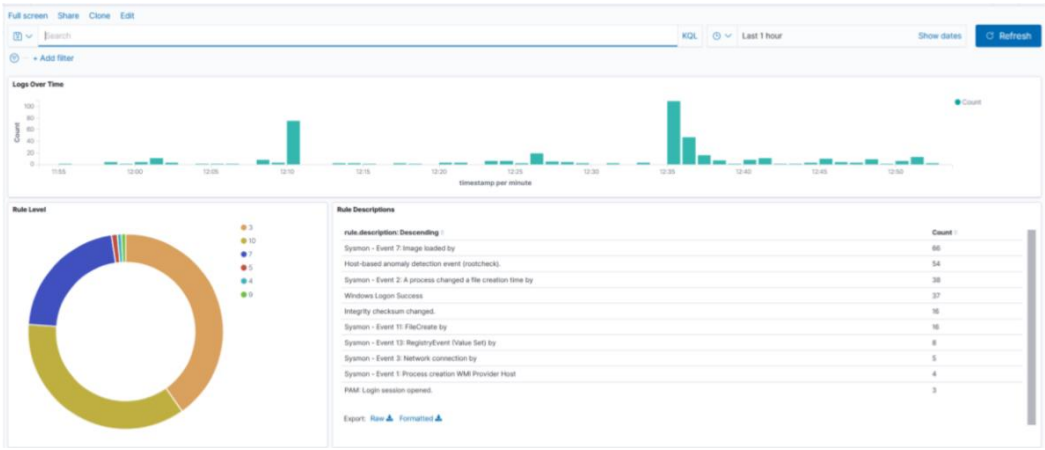
Şekil 4.1.'de belirtilen test ortamında yapılan saldırıların ossec-agent tarafından toplanan olayların wazuh sunucusunda analiz edildikten sonra Kibana arayüzünde görselleştirilmiştir. Saldırılar gerçekleştirilirken oluşan alarm ve grafiklerden bazıları resimlerde belirtilmiştir.

Wazuh HIDS anomali ve zararlı yazılım tespitine yönelik çalışma yapısı Şekil 4.10.'da verilmiştir.



Şekil 4.10. Wazuh anomali ve zararlı yazılım tespiti çalışma yapısı [58]

Zararlı yazılım analizi dosya bütünlük izleme yöntemiyle yapılmaktadır. Bir sistemin ana dizinlerinde dosya bütünlüğü denetimleri yapmak, bu eylemlerin algılanmasına olanak tanımaktadır [58]. Saha cihazlarına yönelik saldırı vektörlerinde yapılan saldırın gerçekleşmesi sırasında Wazuh HIDS analiz sonuçlarının Kibana üzerindeki alarmlarına ait grafikler Şekil 4.11.'de belirtilmiştir.



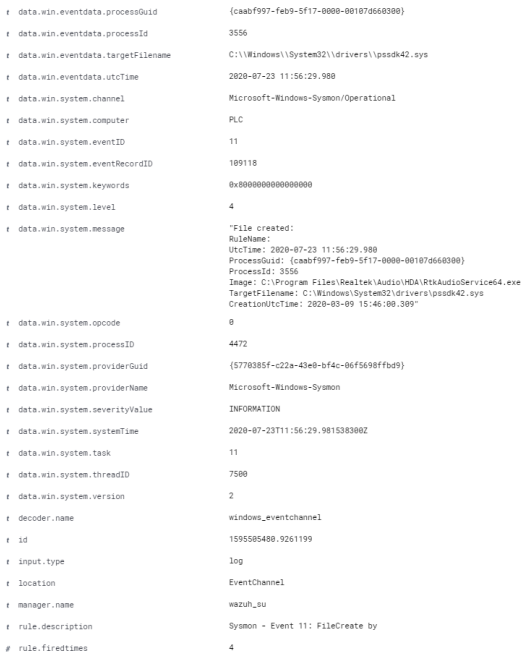
Şekil 4.11. Wazuh alarmlarının Kibana arayüzünde görselleştirilmesi

Wazuh host tabanlı saldırı tespit sistemi olduğundan ağ tabanlı yapılan aktivitelere ait davranışsal analiz yapılamamıştır. Mühendislik bilgisayarına kurulan Sysmon aracının ürettiği logları analiz etmek için Wazuh içerisinde kural dizininde "*0595-win-sysmon_rules.xml*" dosyası bulunmaktadır. Bu dosya Sysmon olaylarına ait üretilen logların analiz edildikten sonra alarm verilmesini sağlar. Wazuh kurulumu yapıldığında bu kuralların alarm seviyeleri varsayılan olarak "0" gelmektedir. Wazuh sunucusundaki kurallar, proseslerin kritikliğine göre alarm seviyeleri yeniden düzenlenmiştir. Bu düzenleme 0-15 aralığında olmalıdır ancak Wazuh sunucudaki *ossec.conf* dosyasında alarm seviyesi 3 olarak belirtilmiştir bu yüzden alarm oluşması gereken kurallarda 3'ten büyük alarm seviyelerinin olması gerekir.

Yapılan konfigürasyonlardan sonra bölüm 4.1.1'de ve 4.1.2'de yapılan saldırıların tespitine yönelik tetiklenen alarmlar ve Kibana arayüzündeki grafikleri aşağıda belirtilmiştir.

Bölüm 4.1.2'de yapılan saldırının (b) adımında gerçekleşen "*migrate*" işleminin sonucunda aynı prosesin altında çalışan yeni bir proses oluşmaktadır. Bu durum, Sysmon'da Tablo 4.1'de belirtilen 11 *Event ID* değerine sahip "*File Create*" tipinde log oluşmasına sebep olur. "*File Create*" olayı, yeni oluşturulan şüpheli dosyaları tespit ettiğinden dolayı çok önemlidir. Bu, bellekte "*reverse shell*" oluşturan bir

dosya, *Office* makrolarından çalıştırılabilir dosya olabilir. Bu olayın alarmı Şekil 4.12.'de belirtilmiştir



t	data.win.eventdata.processGuid	{caabf997-feb9-5f17-0000-00107d660300}
t	data.win.eventdata.processId	3556
t	data.win.eventdata.targetFilename	C:\\Windows\\System32\\drivers\\pssdk42.sys
t	data.win.eventdata.utcTime	2020-07-23 11:56:29.980
t	data.win.system.channel	Microsoft-Windows-Sysmon/Operational
t	data.win.system.computer	PLC
t	data.win.system.eventID	11
t	data.win.system.eventRecordID	109118
t	data.win.system.keywords	0x8000000000000000
t	data.win.system.level	4
t	data.win.system.message	"File created: RuleName: UtcTime: 2020-07-23 11:56:29.980 ProcessGuid: {caabf997-feb9-5f17-0000-00107d660300} ProcessId: 3556 Image: C:\Program Files\Realtek\Audio\HDA\RtkAudioService64.exe TargetFilename: C:\Windows\System32\drivers\pssdk42.sys CreationUtcTime: 2020-03-09 15:46:00.309"
t	data.win.system.opcode	0
t	data.win.system.processID	4472
t	data.win.system.providerGuid	{5770385f-c22a-43e0-bf4c-06f5698ffbd9}
t	data.win.system.providerName	Microsoft-Windows-Sysmon
t	data.win.system.severityValue	INFORMATION
t	data.win.system.systemTime	2020-07-23T11:56:29.981538300Z
t	data.win.system.task	11
t	data.win.system.threadID	7500
t	data.win.system.version	2
t	decoder.name	windows_eventchannel
t	id	1595505480.9261199
t	input.type	log
t	location	EventChannel
t	manager.name	wazuh_su
t	rule.description	Sysmon - Event 11: FileCreate by
#	rule.firedtimes	4

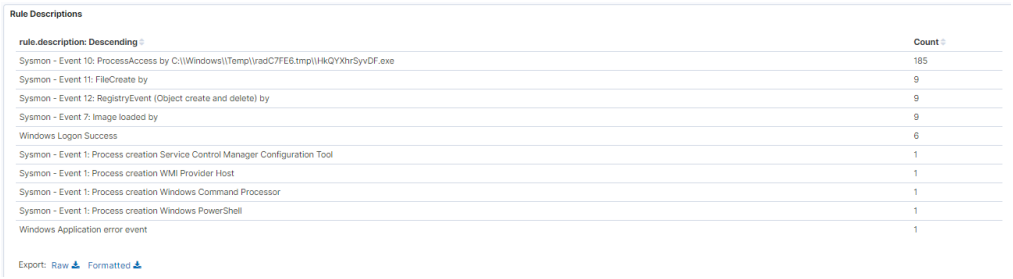
Şekil 4.12. File Create alarmı

Bölüm 4.1.2'de yapılan saldırının (c) adımında gerçekleşen, *.vbs* kodunun C&C sunucuya yönlendirmesi ve kalıcılık sağlamasına yönelik yapılan işlemde mühendislik bilgisayarında rastgele harflerden oluşan bir dosya oluşturulmaktadır. C&C sunucu ve mühendislik bilgisayarı iletişimi bu dosyaya erişerek yapmaktadır. Bu yüzden Şekil 4.13.'te belirtilen alarm oluşmaktadır.

t	data.win.eventdata.callTrace	C:\\WINDOWS\\SYSTEM32\\ntdll.dll+9c534|C:\\WINDOWS\\System32\\wow64.dll+ba94|C:\\WINDOWS\\System32\\wow64.dll+7123|C:\\WINDOWS\\System32\\wow64cpu.dll+1783|C:\\WINDOWS\\System32\\wow64cpu.dll+1199|C:\\WINDOWS\\System32\\wow64.dll+c77a|C:\\WINDOWS\\System32\\wow64.dll+c637|C:\\WINDOWS\\SYSTEM32\\ntdll.dll+718eb|C:\\WINDOWS\\SYSTEM32\\ntdll.dll+717d3|C:\\WINDOWS\\SYSTEM32\\ntdll.dll+7177e|C:\\WINDOWS\\SYSTEM32\\ntdll.dll+7208c(wow64)|C:\\WINDOWS\\System32\\KERNELBASE.dll+f1088(wow64)|UNKNOWN(00000000144049B)|UNKNOWN(00000000144B0F5)|UNKNOWN(0000000001491A44)|UNKNOWN(000000000044748F)|UNKNOWN(0000000000447349)|UNKNOWN(000000000044784C)|C:\\WINDOWS\\System32\\KERNEL32.DLL+16359(wow64)|C:\\WINDOWS\\SYSTEM32\\ntdll.dll+67c24(wow64)|C:\\WINDOWS\\SYSTEM32\\ntdll.dll+67bf4(wow64)
t	data.win.eventdata.grantedAccess	0x1410
t	data.win.eventdata.ruleName	technique_id=T1036,technique_name=Masquerading
t	data.win.eventdata.sourceImage	C:\\Windows\\Temp\\radC7FE6.tmp\\HkQYXhrSyvDF.exe
t	data.win.eventdata.sourceProcessGUID	{caabf997-7fb2-5f19-0000-0010b974c20a}
t	data.win.eventdata.sourceProcessId	2168
t	data.win.eventdata.sourceThreadId	13024
t	data.win.eventdata.targetImage	C:\\WINDOWS\\system32\\cscript.exe
t	data.win.eventdata.targetProcessGUID	{caabf997-7fb1-5f19-0000-00103155c20a}
t	data.win.eventdata.targetProcessId	10928
t	data.win.eventdata.utcTime	2020-07-23 12:17:17.584
t	data.win.system.channel	Microsoft-Windows-Sysmon/Operational
t	data.win.system.computer	PLC
t	data.win.system.eventID	10
t	data.win.system.eventRecordID	109314
t	data.win.system.keywords	0x8000000000000000
t	data.win.system.level	4
t	data.win.system.message	"Process accessed: RuleName: technique_id=T1036,technique_name=Masquerading UtcTime: 2020-07-23 12:17:17.584 SourceProcessGUID: {caabf997-7fb2-5f19-0000-0010b974c20a} SourceProcessId: 2168 SourceThreadId: 13024 SourceImage: C:\Windows\Temp\radC7FE6.tmp\HkQYXhrSyvDF.exe
t	data.win.system.opcode	0
t	data.win.system.processID	4472
t	data.win.system.providerGuid	{5770385f-c22a-43e0-bf4c-06f5698ffbd9}
t	data.win.system.providerName	Microsoft-Windows-Sysmon

Şekil 4.13. Prosese erişim alarmı

Komut gönderimi sırasında ve sürekli bağlantı sağlandığından bu prosese en çok erişim (185) sağlandığından "*Process Access*" kuralı tektiklenmektedir (Şekil 4.14.).



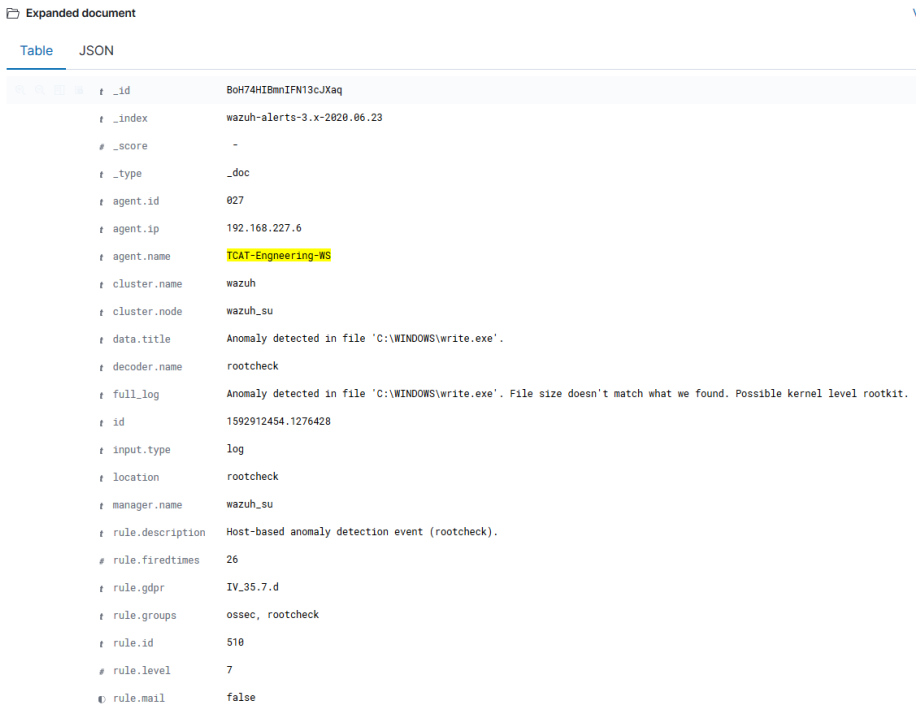
Rule Descriptions

rule.description: Descending	Count
Sysmon - Event 10: ProcessAccess by C:\\Windows\\Temp\\radC7FE6.tmp\\HkQYXhrSyvDF.exe	185
Sysmon - Event 11: FileCreate by	9
Sysmon - Event 12: RegistryEvent (Object create and delete) by	9
Sysmon - Event 7: Image loaded by	9
Windows Logon Success	6
Sysmon - Event 1: Process creation Service Control Manager Configuration Tool	1
Sysmon - Event 1: Process creation WMI Provider Host	1
Sysmon - Event 1: Process creation Windows Command Processor	1
Sysmon - Event 1: Process creation Windows PowerShell	1
Windows Application error event	1

Export: Raw Formatted

Şekil 4.14. Oluşturulan alarmların sayılarına göre dağılımı

Kötü amaçlı bir işlem, örneğin "*ps*" komutunun trojan sürümü gibi bir sistemin proses listesinde görünmesini engelleyebilir. Rootcheck, farklı sistem çağrıları (*getsid*, *getpgid*) ile tutarsızlıkları tarayan tüm işlem kimliklerini (PID) inceler [58]. Yapılan saldırıda meterpreter oturumu açıldığında Wazuh çalışan prosesleri bu prensiple tarar ve Şekil 4.15.'teki alarmı üretir.



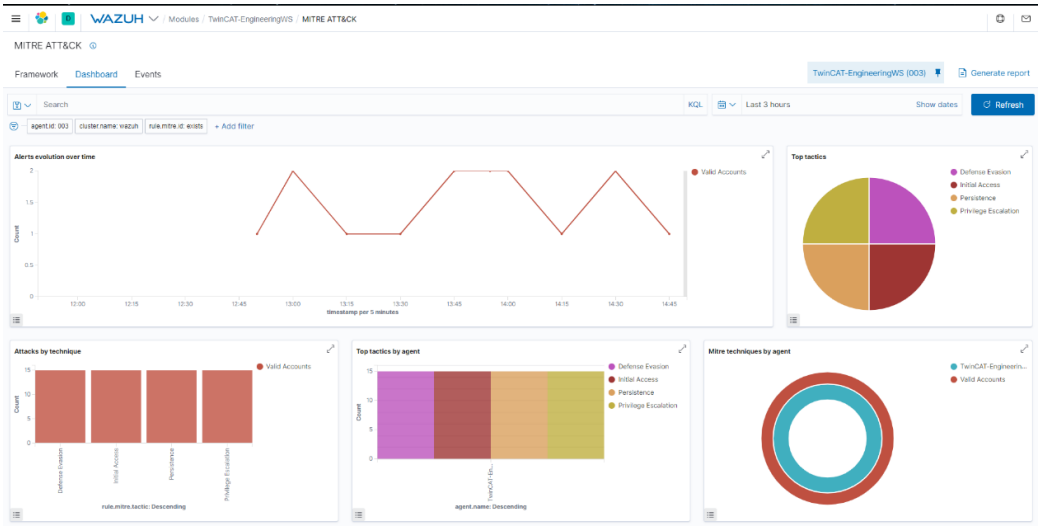
Expanded document

Table JSON

t _id	BoH74HIBmnIFN13cJXaq
t _index	wazuh-alerts-3.x-2020.06.23
# _score	-
t _type	_doc
t agent.id	027
t agent.ip	192.168.227.6
t agent.name	TCAT-Engneering-WS
t cluster.name	wazuh
t cluster.node	wazuh_su
t data.title	Anomaly detected in file 'C:\WINDOWS\write.exe'.
t decoder.name	rootcheck
t full_log	Anomaly detected in file 'C:\WINDOWS\write.exe'. File size doesn't match what we found. Possible kernel level rootkit.
t id	1592912454.1276428
t input.type	log
t location	rootcheck
t manager.name	wazuh_su
t rule.description	Host-based anomaly detection event (rootcheck).
# rule.firedtimes	26
t rule.gdpr	IV_35.7.d
t rule.groups	ossec, rootcheck
t rule.id	510
# rule.level	7
◐ rule.mail	false

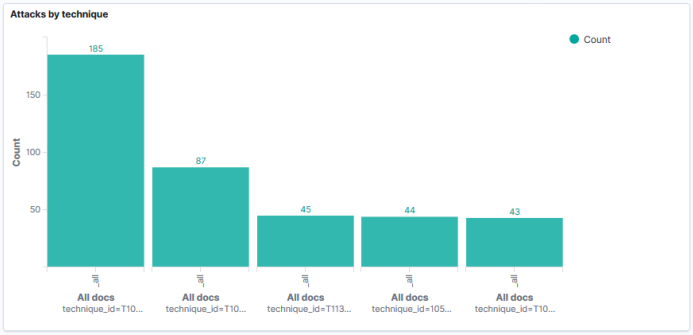
Şekil 4.15. Wazuh rootcheck alarmı

ELK sistemi üzerinde MITRE ATT&CK matrisine göre taktik bazlı grafikler Şekil 4.16.'da belirtilmiştir.



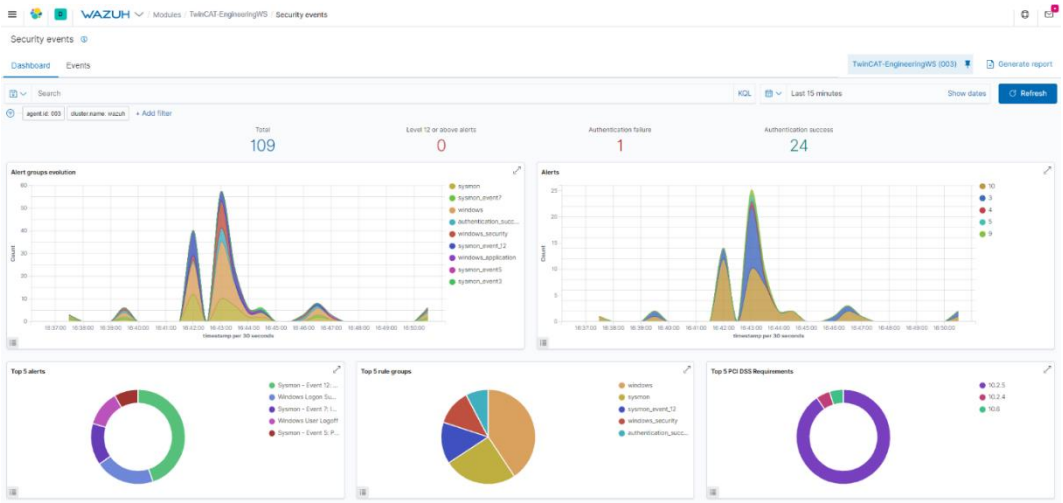
Şekil 4.16. Wazuh alarmları MITRE ATT&CK tekniklerine göre grafikleri

Şekil 4.16.'da verilen dashboard grafikleri MITRE ATT&CK matrisine ait taktiklere göre dağılımı göstermektedir. Bu matris BT taktiklerine göre sınıflandırma yaptığından farklı taktik isimleriyle etiketleme yapılmıştır. Teknik sınıflandırması yapılmadığından var olan dashboard ekranı üzerinde teknik isimlerine göre Şekil 4.17.'deki grafik oluşturulmuştur.



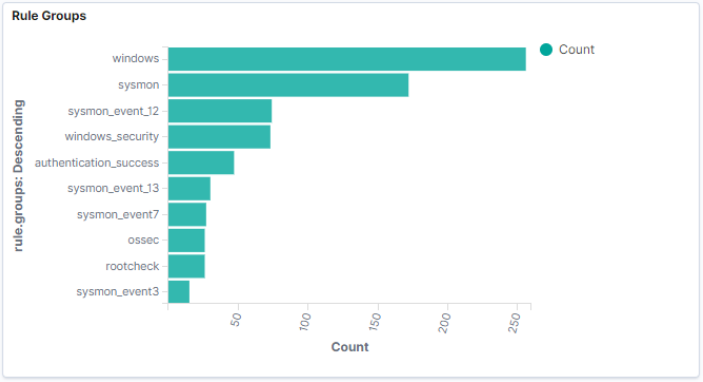
Şekil 4.17. MITRE ATT&CK tekniklerine göre dağılım grafiği

Saldırının diğer adımları ağ tabanlı işlemler veya elde edilen verilerin analiz edilip bir sonraki saldırı vektörünün oluşmasına yönelik çıkarımlar olduğundan saldırının direkt karşılığı olan alarm oluşmamaktadır. Sistemde saldırı sürecinde mühendislik bilgisayarında oluşan alarmlara göre Kibana *dashboard* grafikleri Şekil 4.18.'de belirtilmiştir.



Şekil 4.18. Mühendislik bilgisayarı dashboard ekranı

Alarmların oluşturulduğu log kaynaklarına göre dağılım grafiği Şekil 4.19.'da verilmiştir. Şekil 4.19.'daki grafiğe göre Windows kaynaklı kurallar 250+; Sysmon kaynaklı kurallar 180+ civarındadır. Takip eden diğer alarm grupları da Sysmon kurallarından oluştuğu göz önüne alınırsa Sysmon üzerinde yazılabilecek host tabanlı veya ağ tabanlı birçok olaya ait kural ile anomali tespiti yapılabilmesi mümkündür.



Şekil 4.19. Kural gruplarına göre alarm dağılımı

BÖLÜM 5. TARTIŞMA VE SONUÇ

Endüstriyel kontrol sistemlerinde, var olan ve her gün bir yenisi eklenen saldırılar kurumları tehdit etmeye devam etmektedir. Hem maddi hem de insan hayatına olan kritik etkisinden dolayı bu saldırıların önlenmesine yönelik güvenlik açıklıklarının yönetimi, tespit edilmesi ve önlenmesi oldukça önemlidir. OT sistemler için yeni teknoloji, standartlar ve farklı yetenekte cihazlar üretilmeye devam etmektedir. Bu sistemler maliyet ve zaman açısından süreci kolaylaştırmakla birlikte yeni güvenlik açıklıklarına da sebebiyet vermektedir. Bu yüzden kritik alt yapıların ağ ve uç sistemlere ait verilerin toplanması ve sürekli izleme yapılması gerekmektedir. Böylece olası ön görülebilir saldırıların önlenmesine yönelik süreçler işletilebilir. Kritik alt yapılara ait saldırı tespit ve engellenmesine yönelik birçok yöntem mevcuttur. Tez kapsamında EtherCAT tabanlı çalışan bir su prosesinde hem uç cihazlara hem de SCADA sistemine olası saldırılar ve tespitini sağlayan bir çözüm önerisi geliştirilmiştir. Yapılan saldırılar ve tespit sistemi sıfırıncı gün açıklılarına yönelik bir çözüm sunmamaktadır.

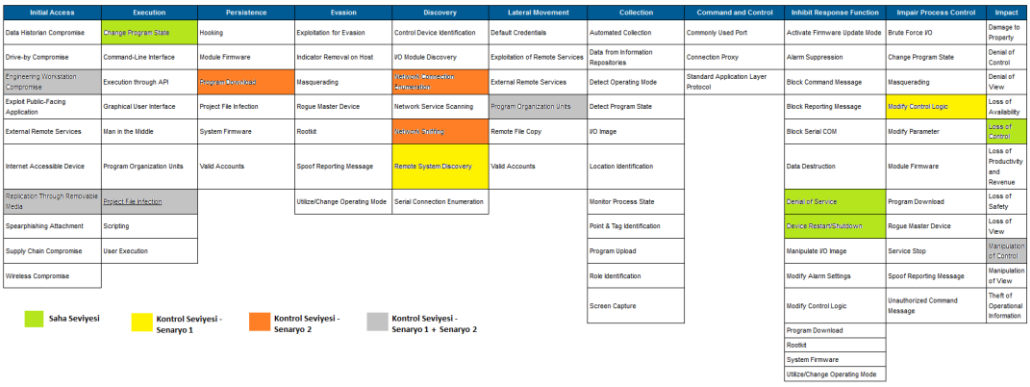
Tez kapsamında yapılan çalışmalar;

a. EtherCAT protokol yapısının fabrika seviyesinde ilgili alt protokollerin belirlenmesi,
b. Fabrika seviyesindeki saha cihazları için, MITRE ICS ATT&CK matrisinde sınıflandırılan 6 çeşit saldırının gerçekleştirilmesi,
c. Fabrika seviyesindeki saha cihazlarına yapılan saldırıların SVM algoritması kullanılarak tespit edilmesi ve ELK ortamında görselleştirilmesi,
d. SCADA sistemine yönelik saldırıların MITRE ICS ATT&CK matrisi üzerinde senaryolaştırılarak gerçekleştirilmesi,
e. SCADA sistemine yapılan saldırıların Wazuh HIDS ve Sysmon aracılığı ile alarm üretilmesi ve ELK ortamında görselleştirilmesi,

f. Çalışma içerisinde oluşturulan saldırı vektörleri, 7 Ocak 2020 tarihinde ortaya çıkan MITRE ICS ATT&CK matrisine göre hızlıca uyarlanmıştır. Kırmızı ve mavi takımlar için oldukça kullanılışlı ve her geçen gün geliştirilmektedir.

Çalışmaları başarıyla tamamlanmıştır. Böylece EtherCAT tabanlı bir sistemde hem uç cihazların hem de sistemin yönetimini sağlayan SCADA sisteminin güvenliği ve izlenebilirliğini sağlayan bütüncül bir yapı sunulmuştur.

EtherCAT tabanlı su prosesinde hem saha cihazlarına hem de kontrol merkezine gerçekleştirilen atakların MITRE ICS ATT&CK matrisinde kullanılan teknikler Şekil 5.1.'de belirtilmiştir.



Şekil 5.1. Saha cihazları ve kontrol merkezine yapılan saldırıların MITRE ICS matrisi

Bu çalışma ile EtherCAT protkolüne yönelik fabrika seviyesinde oluşabilecek siber saldırıların tespitine yönelik saha seviyesi için makine öğrenmesi algoritması; kontrol merkezi için Wazuh HIDS ile saldırı tespit sistemi geliştirilerek bilime katkı sağlanmıştır.

İlerleyen çalışmalarda bu matris üzerinde hem saldırı hem de tespitine yönelik çözümler çeşitlendirilebilir. Sistemin sürekli izlenebilirliği de bu matrisin periyodik güncel çalışmalarla sağlanabilir. Wazuh sunucu tarafından üretilen logların belirli seviyelerde üretildiğinde SIEM ürününe yönlendirerek daha kapsamlı korelasyon yapılmasına olanak tanır. Su prosesi iletişiminde NIDS kurularak Wazuh sunucusuna analiz için ağ tabanlı olaylar gönderilerek ağ tabanlı izleme yapılabilir.

KAYNAKLAR

[1] J. Steele, “MITRE ATT & CK ® for Industrial Control Systems : Design and Philosophy Authors : Otis Alexander Misha Belisle,” March, 2020.

[2] L. Obregon, “Secure Architecture for Industrial Control Systems,” 2020.

[3] https://collaborate.mitre.org/attackics/index.php/All_Assets, Erişim Tarihi: 10.06.2020.

[4] Andreeva, O., Gordeychik, S., Gritsai, G., Kochetova, O., Potseluevskaya, E., Sidorov, S.I., Timorin, A.A., Industrial Control Systems Vulnerabilities Statistics, p. 19, 2016.

[5] https://securityintelligence.com/posts/modernizing-threat-management-for-the-evolving-attack-surfaces-of-ot-iot-and-iomt/, Erişim Tarihi: 07.06.2020.

[6] J. Slowik, Anatomy of an attack: Detecting and defeating Crashoverride, *Virus Bull. 2018 Montr.*, June 2017, pp. 1–23, 2018.

[7] Fortinet, “Pinpoints Significant SCADA / ICS Security Risks.”

[8] https://www.mitre.org/research/technology-transfer/open-source-software/caldera, Erişim Tarihi: 08.03.2020.

[9] https://www.metasploit.com/, Erişim Tarihi: 05.02.2020.

[10] https://github.com/praetorian-code/purple-team-attack-automation, Erişim Tarihi: 03.04.2020.

[11] https://atomicredteam.io/ Erişim Tarihi: 05.05.2020.

[12] Shitharth, S., Winston, D. P., An enhanced optimization based algorithm for intrusion detection in SCADA network. *Comput. Secur.*, vol. 70, pp. 16–26, 2017.

[13] Zhang, J., Gan, S., Liu, X., Zhu, P., Intrusion detection in SCADA systems by traffic periodicity and telemetry analysis. *IEEE Symp. Comput. Commun.*, vol. 2016-Augus, pp. 318–325, 2016.

[14] Ullah, I., Mahmoud, H.Q., A Hybrid Model for Anomaly-Based Intrusion Detection System. *2017 IEEE International Conference on Big Data*, 2017.

[15] Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., Shu, L. A systematic review of data protection and privacy preservation schemes for smart grid communications. *Sustain. Cities Soc.*, vol. 38, January, pp. 806–835, 2018.

[16] Granat, A., Höfken, H., SCHUBA, M., Intrusion Detection of the ICS Protocol EtherCAT. DEStech Trans. Comput. Sci. Eng., 2017.

[17] Ovaz A, K. 2019. Ethercat tabanli bir scada sisteminde saldiri tespiti, Doktora Tezi.

[18] Al-Shaer, R., Spring, J. M., Christou, E., Learning the Associations of MITRE ATT&CK Adversarial Techniques. 2020.

[19] Teixeira, M. A., Salman, T., Zolanvari, M., Jain, R., Samaka, M., SCADA System Testbed for Cybersecurity Research Using Machine Learning Approach.

[20] Inoue, J., Yamagata, Y., Chen, Y., Poskitt, C. M., Sun, J., Anomaly detection for a water treatment system using unsupervised machine learning. *IEEE Int. Conf. Data Min. Work. ICDMW*, vol. 2017-Novem, pp. 1058–1065, 2017.

[21] Wang, D., Wang, X., Zhang, Y., Jin, L., Detection of power grid disturbances and cyber-attacks based on machine learning. *J. Inf. Secur. Appl.*, vol. 46, pp. 42–52, 2019.

[22] Yang, H., Cheng, L., Chuah, M. C., Deep-Learning-Based Network Intrusion Detection for SCADA Systems. *2019 IEEE Conf. Commun. Netw. Secur. CNS 2019*, 2019.

[23] Alhaidari, F. A., Al-Dahasi, E. M., New approach to determine DDoS attack patterns on SCADA system using machine learning. *2019 Int. Conf. Comput. Inf. Sci. ICCIS 2019*, pp. 2–7, 2019.

[24] Robles-Durazno, A., Moradpoor, N., McWhinnie, J., Russell, G., A supervised energy monitoring-based machine learning approach for anomaly detection in a clean water supply system. *2018 Int. Conf. Cyber Secur. Prot. Digit. Serv. Cyber Secur. 2018*, 2018.

[25] Lopez, P. R., Adamsky, F., Soua, R., Engel, T., Machine Learning for Reliable Network Attack Detection in SCADA Systems. *Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018*, pp. 633–638, 2018.

[26] https://www.us-cert.gov/ics/Secure-Architecture-Design-Definitions, Erişim Tarihi: 25.06.2020.

[27] Zhu, B., Joseph, A., Sastry, S., A Taxonomy of Cyber Attacks on SCADA Systems. *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, Oct. 2011, pp. 380–388.

[28] https://subscription.packtpub.com/book/networking_and_servers/9781788395151/5/ch05lvl1sec30/the-purdue-enterprise-reference-architecture, Erişim Tarihi: 20.06.2020.

[29] https://www.ethercat.org/en/technology.html, Erişim Tarihi: 15.06.2020.

[30] Lee, J. R., EAP Manual. vol. 53, no. 1, pp. 1–9, 2020.

[31] https://infosys.beckhoff.com/english.php?content=../content/1033/ tcsystem /html/tcsystem_usercontrol.htm&id=, Erişim Tarihi: 30.06.2020.

[32] EtherCAT Technology Group, EtherCAT for factory networking. *Pc Control*, 2009.

[33] https://attack.mitre.org/, Erişim Tarihi: 28.06.2020.

[34] https://collaborate.mitre.org/attackics/index.php/Main_Page, Erişim Tarihi: 20.04.2020.

[35] https://www.fireeye.com/current-threats/apt-groups.html, Erişim Tarihi: 15.05.2020).

[36] https://www.us-cert.gov/ics/advisories/ICSA-10-238-01B, Erişim Tarihi: 19.04.2020.

[37] Hemsley, K. E., Fisher, D. R. E., History of Industrial Control System Cyber Incidents. December, p. 37, 2018.

[38] Shrivastava, S., BlackEnergy - Malware for Cyber-Physical Attacks. 2016.

[39] Nelson, N., The Impact of Dragonfly Malware on Industrial Control Systems. *SANS Inst. InfoSec Read. Room*, pp. 1–25, 2016.

[40] https://www.youtube.com/watch?reload=9&v=SyupAcnURtA, Erişim Tarihi: 20.05.2020.

[41] https://github.com/wazuh/wazuh, Erişim Tarihi: 08.05.2020.

[42] https://documentation.wazuh.com/3.12/getting-started/architecture.html, Erişim Tarihi: 10.06.2020.

[43] https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon, Erişim Tarihi: 08.03.2020).

[44] https://collaborate.mitre.org/attackics/index.php/Technique/T875, Erişim Tarihi: 14.04.2020.

[45] https://collaborate.mitre.org/attackics/index.php/Technique/T814, Erişim Tarihi: 25.04.2020.

[46] https://collaborate.mitre.org/attackics/index.php/Technique/T816, Erişim Tarihi: 25.04.2020.

[47] Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., Hahn, A., Guide to Industrial Control Systems (ICS) Security NIST Special Publication 800-82 Revision 2. *NIST Spec. Publ. 800-82 rev 2*, pp. 1–157, 2015.

[48] https://collaborate.mitre.org/attackics/index.php/Technique/T847, Erişim Tarihi: 19.06.2020.

[49] https://collaborate.mitre.org/attackics/index.php/Technique/T818, Erişim Tarihi: 19.06.2020.

[50] https://collaborate.mitre.org/attackics/index.php/Technique/T846, Erişim Tarihi: 25.04.2020.

[51] https://collaborate.mitre.org/attackics/index.php/Technique/T844, Erişim Tarihi: 19.06.2020.

[52] https://collaborate.mitre.org/attackics/index.php/Technique/T873, Erişim Tarihi: 25.04.2020.

[53] https://collaborate.mitre.org/attackics/index.php/Technique/T833, Erişim Tarihi: 25.04.2020.

[54] https://collaborate.mitre.org/attackics/index.php/Technique/T831, Erişim Tarihi: 19.06.2020.

[55] https://collaborate.mitre.org/attackics/index.php/Technique/T843, Erişim Tarihi: 23.07.2020.

[56] https://collaborate.mitre.org/attackics/index.php/Technique/T842, Erişim Tarihi: 23.07.2020.

[57] https://collaborate.mitre.org/attackics/index.php/Technique/T840, Erişim Tarihi: 23.07.2020.

[58] https://documentation.wazuh.com/3.13/user-manual/capabilities/anomalies-detection/how-it-works.html, Erişim Tarihi: 05.06.2020.

EKLER

EK:1 Beckhoff PLC cihazlarına yapılan A1-A5 saldırılarına ait C++ kodu.

```
#include <iostream>
#include <conio.h>
#include <windows.h>

#include<TcAdsDef.h>
#include<TcAdsAPI.h>

using namespace std;

int main()
{
	USHORT	nAdsState;
	USHORT	nDeviceState = 0;
	long	nErr, nPort;
	int	ch,choice;
	void	*pData = NULL;
	char a;
	AmsAddr	Addr;

	do {
		system("cls");
		cout << "---------------------------------------\n";
		cout << "1- AMS ID Aritma_PLC: 5.68.121.88.1.1\n";
		cout << "2- AMS ID Terfi1_PLC: 5.68.121.85.1.1\n";
		cout << "3- AMS ID Terfi2_PLC: 5.60.78.57.1.1\n";
		cout << "4- AMS ID Depo_PLC: 5.60.78.21.1.1\n";
		cout << "5- AMS ID Eng Station: 10.9.16.189.1.1\n";
		cout << "---------------------------------------\n";
		cout << "Please enter a number of AMSID\n\n";
		cin >> choice;
		if (choice == 1) {
			Addr.netId.b[0] = 5;
			Addr.netId.b[1] = 68;
			Addr.netId.b[2] = 121;
			Addr.netId.b[3] = 88;
			Addr.netId.b[4] = 1;
			Addr.netId.b[5] = 1;
		}
		else if (choice == 2) {
			Addr.netId.b[0] = 5;
			Addr.netId.b[1] = 68;
			Addr.netId.b[2] = 121;
			Addr.netId.b[3] = 85;
			Addr.netId.b[4] = 1;
			Addr.netId.b[5] = 1;
		}
```

```
		else if (choice == 3) {
			Addr.netId.b[0] = 5;
			Addr.netId.b[1] = 60;
			Addr.netId.b[2] = 78;
			Addr.netId.b[3] = 57;
			Addr.netId.b[4] = 1;
			Addr.netId.b[5] = 1;
		}
		else if (choice == 4) {
			Addr.netId.b[0] = 5;
			Addr.netId.b[1] = 60;
			Addr.netId.b[2] = 78;
			Addr.netId.b[3] = 21;
			Addr.netId.b[4] = 1;
			Addr.netId.b[5] = 1;
		}
		else if (choice == 5) {
			Addr.netId.b[0] = 10;
			Addr.netId.b[1] = 9;
			Addr.netId.b[2] = 16;
			Addr.netId.b[3] = 189;
			Addr.netId.b[4] = 1;
			Addr.netId.b[5] = 1;
		}

		PAmsAddr	pAddr = &Addr;
		nPort = AdsPortOpen();
		pAddr->port = 10000;

		cout << "\n(R) -> Run\n";
		cout << "(D) -> Shutdown ->> shut down system and restart in run mode \n";
		cout << "(P) -> Power Failure ->>sytem completely stops, hard restart is
required\n";
		cout << "(S) -> Stop\n";
		cout << "(F) -> Reconfig ->> shut down system and restart in config mode\n";
		cout.flush();
		ch = _getch();
		ch = toupper(ch);

		while ((ch == 'R') || (ch == 'D') || (ch == 'P') || (ch == 'S') || (ch == 'F'))
		{
			switch (ch)
			{
			case 'R':
				nAdsState = ADSSTATE_RUN;
				break;
			case 'D':
				nAdsState = ADSSTATE_SHUTDOWN;
				break;
			case 'P':
				nAdsState = ADSSTATE_POWERFAILURE;
				break;
			case 'S':
```

```
                                        nAdsState = ADSSTATE_STOP;
                                        break;
                                case 'F':
                                        nAdsState = ADSSTATE_RECONFIG;
                                        break;
                                }
                                nErr = AdsSyncWriteControlReq(pAddr, nAdsState, nDeviceState, 0,
pData);
                                if (nErr) cerr << "Error: AdsSyncWriteControlReq: " << nErr << '\n';
                                ch = _getch();
                                ch = toupper(ch);
                        }

                        nErr = AdsPortClose();
                        if (nErr) cerr << "Error: AdsPortClose: " << nErr << '\n';
                        cout << "Do you wish to continue? (Y/N)";
                        cin >> a;
                }while (a == 'Y' || a == 'y');
                return 0;
}
```

EK:2 Wazuh HIDS sunucusu kurulum ve yapılandırma komutlar dizisi.

WAZUH HIDS Server Kurulumu

CentOS 7 üzerine wazuh kurulumu komut satırı yetkili modda wazuh.rep dosyasına ilgili URL girilerek indirilecek kaynak belirtilir. “Wazuh manager” indirilir ve servis durumu kontrol edilir:

```
# systemctl stop firewald
# systemctl stop firewalld
# rpm --import https://packages.wazuh.com/key/GPG-KEY-WAZUH
#cat > /etc/yum.repos.d/wazuh.repo <<\EOF [wazuh_repo] gpgcheck=1
gpgkey=https://packages.wazuh.com/key/GPG-KEY-WAZUH enabled=1 name=Wazuh
repository baseurl=https://packages.wazuh.com/3.x/yum/ protect=1 EOF
# yum install wazuh-manager
#  systemctl status wazuh-manager
```

Elde edilen alarmları görüntülemek ve ELK iletişimi için Wazuh API kullanılmıştır. Aşağıdaki komutlarla wazuh-api indirilir ve Elasticsearch kurulumu için elastic.repo dosyasına ilgili yapılandırma komutları yazılmıştır:

```
# yum install wazuh-api
# rpm --import https://packages.elastic.co/GPG-KEY-elasticsearch
```

```
# cat > /etc/yum.repos.d/elastic.repo << EOF
  [elasticsearch-7.x]
  name=Elasticsearch repository for 7.x packages
  baseurl=https://artifacts.elastic.co/packages/7.x/yum
  gpgcheck=1
  gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
  enabled=1
  autorefresh=1
  type=rpm-md
  EOF
```

Wazuh sisteminde oluşan alarmlar "/var/ossec/etc/ossec.conf" dosyasına kaydedilir. Bu yüzden yapılan işlemlerde alarmların oluşup oluşmadığına dair kontroller bu dosya üzerinde yapılabilir. Wazuh Şekil 4.6.'da belirtildiği üzere cluster mimarisinde yapılandırılmıştır. İlgili yapılandırma dosyası "/var/ossec/etc/ossec.conf" dizininde bulunan xml formatındaki dosyadır. Cluster yapı kullanıldığından cluster tag'leri arasındaki "node_type" alanına üzerinde işlem yapılan makine eğer merkez ise "master" dağıtılan wazuh sunuculardakine ise "worker" yazılır. Cluster yapıda iletişim doğrulamadı key üzerinden yapılır. Bu key master ve worker cihazlarda aynı olmalıdır. Key oluşturmak için "openssl rand -hex 16" kullanılabilir. Bu komutun çıktısı key tag'leri arasına yazılmalıdır. Son olarak node IP adresi üzerinde işlem yapılan makinenin IP adresi olarak yazılır. Diğer bilgiler default olarak bırakılmakla beraber isteğe göre değiştirilebilir. Ossec.conf dosyası üzerinde bir değişiklik yapıldığında yapılan değişikliğin aktifleştirilmesi için wazuh manager yeniden başlatılmalıdır:

```
# systemctl status wazuh-manager
# tail -f /var/ossec/logs/alerts/alerts.log
# openssl rand -hex 16
# vim /var/ossec/etc/ossec.conf

#####ossec.conf içine aşağıdaki cluster node ekelenir ##########
  <cluster>
    <name>wazuh</name>
    <node_name>wazuh_merkez</node_name>
    <node_type>master</node_type>
    <key>6990bb5b8cc36ab19d7eb169037d0213</key>
    <port>1516</port>
    <bind_addr>0.0.0.0</bind_addr>
    <nodes>
```

```
      <node>192.168.50.210</node>
    </nodes>
    <hidden>no</hidden>
    <disabled>no</disabled>
  </cluster>
############################ EOF ########################

# systemctl restart wazuh-manager
# /var/ossec/api/scripts/configure_api.sh
```

Oluşturulan alarmlar kibana arayüzünde gösterilmektedir. Bunun için kibana kurulumu yapılmıştır. Kibana üzerinde wazuh agentlarının görüntülenmesi, eklenmesi, yönetimi vs. gibi işlemleri arayüz üzerinden sağlamak için wazuh plugin de kurulmuştur:

```
# yum install kibana-7.5.2
# sudo -u kibana /usr/share/kibana/bin/kibana-plugin install https://packages.wazuh.com/wazuhapp/wazuhapp-3.11.2_7.5.2.zip
```

Kibana kurulumu tamamlandıktan sonra "/etc/kibana/kibana.yml" dizinindeki konfigürasyon dosyasında aşağıdaki gibi elasticsearch makinesinin IP adresi yazılmalıdır. Yapılan değişikliklerin aktifleştirilmesi için kibana yeniden başlatılmalıdır. İletişimde problem oluyorsa firewall kaynaklı olabileceğinden selinux disable yapılabilir ardından tekrar kibana başlatılır:

```
# vim /etc/kibana/kibana.yml

#################kibana.yml içine port / IP doğrulanır. ######
server.port: 5601
server.host: "localhost"
elasticsearch.hosts: ["http://192.168.50.200:9200"]
############################ EOF ########################
# systemctl restart kibana
# systemctl status kibana
# systemctl stop firewalld
# vim /etc/selinux/config

######selinux disabled yapılır ############################
SELINUX=enforcing
#####################EOF ############################
# systemctl restart kibana
```

Kibana web arayüzü erişiminde kimlik doğrulama yapmak için nginx kurulumu yapılmıştır. İlgili sertifika ve kullanıcı kullanımıyla ilgili bilgiler kurulum ve sertifika süreçlerinden sonra "/etc/nginx/conf.d/default.conf" dosyasına aşağıdaki gibi yazılmıştır. Ardından nginx yeniden başlatılmıştır.

```
# yum install epel-release
# yum install nginx
# mkdir -p /etc/pki/tls/certs /etc/pki/tls/private
# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/pki/tls/private/kibana-
access.key -out /etc/pki/tls/certs/kibana-access.pem

# cat > /etc/nginx/conf.d/default.conf <<\EOF
  server {
     listen 80;
     listen [::]:80;
     return 301 https://$host$request_uri;
  }
  server {
     listen 443 default_server;
     listen          [::]:443;
     ssl on;
    ssl_certificate /etc/pki/tls/certs/kibana-access.pem;
    ssl_certificate_key /etc/pki/tls/private/kibana-access.key;
    access_log           /var/log/nginx/nginx.access.log;
    error_log          /var/log/nginx/nginx.error.log;
    location / {
       auth_basic "Restricted";
     auth_basic_user_file /etc/nginx/conf.d/kibana.htpasswd;
     proxy_pass http://localhost:5601/;
   }
  }
 EOF
######################EOF ############################
# yum install httpd-tools
# htpasswd -c /etc/nginx/conf.d/kibana.htpasswd wazuh
# systemctl restart nginx
# systemctl status wazuh-api
```

Wazuh api kullanımı için "/usr/share/kibana/plugins/wazuh/wazuh.yml" dizinindeki konfigürasyon dosyasına wazuh master makinesinin IP adresiyle birlikte kullanıcı adı ve parola bilgileri oluşturulur. Konfigürasyonun aktifleştirilmesi için wazuh API ve wazuh manager yeniden başlatılır. Wazuh API iletişim logları "/var/ossec/logs/api.log" dosyasından kontrol edilebilir.

```
# vim /usr/share/kibana/plugins/wazuh/wazuh.yml

################wazuh.yml içine aşağıdaki blok yazılır ##################
hosts:
  - default:
     url: https://192.168.50.210
     port: 55000
```

```
    user: SAU_TYM
    password: passwd
#######################EOF ############################

# systemctl restart wazuh-api
# systemctl status wazuh-api
# tail -f /var/ossec/logs/api.log
# systemctl restart wazuh-manager
```

Wazuh master/node cihazlarında oluşan alarmların ELK yapısına aktarmak için filebeat kullanılmaktadır. Filebeat kurulumu ve wazuh alarmları için gerekli şablon ve modül dosyası dosyası indirilip izinler verilir:

```
# yum install filebeat-7.5.2
# curl -so /etc/filebeat/filebeat.yml
https://raw.githubusercontent.com/wazuh/wazuh/v3.11.2/extensions/filebeat/7.x/filebeat.yml
# chmod go+r /etc/filebeat/filebeat.yml
# curl -so /etc/filebeat/wazuh-template.json
https://raw.githubusercontent.com/wazuh/wazuh/v3.11.2/extensions/elasticsearch/7.x/wazuh-
template.json
# chmod go+r /etc/filebeat/wazuh-template.json
# curl -s https://packages.wazuh.com/3.x/filebeat/wazuh-filebeat-0.1.tar.gz | sudo tar -xvz -C
/usr/share/filebeat/module
```

"/etc/filebeat/filebeat.yml" dizininde bulunan konfigürasyon dosyasına template dosyasının yolu ve modül isimlendirme gibi yapılandırma ayarları yazılır son olarak filebeat çıktısının gönderileceği elasticsearch makinesinin IP adresi yazılıp kaydedildikten sonra filebeat servisi yeniden başlatılır.

```
# vim /etc/filebeat/filebeat.yml

##############filebeat.yml içine yazılır ######################
filebeat.modules:
  - module: wazuh
    alerts:
      enabled: true
    archives:
      enabled: false

setup.template.json.enabled: true
setup.template.json.path: '/etc/filebeat/wazuh-template.json'
setup.template.json.name: 'wazuh'
setup.template.overwrite: true
setup.ilm.enabled: false

output.elasticsearch.hosts: ['http://192.168.50.200:9200']

#######################EOF ############################

# systemctl restart filebeat
# tail -f /var/ossec/logs/alerts/alerts.json
# tail -f /var/log/messages
```

```
# tail -f /var/log/messages |grep filebeat


# systemctl restart wazuh-manager
```

EK 3: Wazuh Agent Üzerinde Yapılacaklar

Server üzerinde yapılacaklar:

```
# /var/ossec/bin/manage_agents -a IPADDRESS -n AGENT_NAME
# /var/ossec/bin/manage_agents -e AGENT_ID (bu komutun çıktısı registration key olacak bu key ile agent tarafında kayıt işlemi tamamlanacak.)
```

Client üzerinde yapılacaklar:

https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon Sysmon indirilir.

İndirilen dizinde aşağıdaki MITRE kurallarını içeren xml dosyası oluşturulur.

https://github.com/olafhartong/sysmon-modular/blob/master/sysmonconfig.xml

Admin yetkili komut satırından oluşturulan konfigürasyon dosyası ile sysmon kurulumu yapılır.

- Sysmon64.exe -accepteula -i sysmonconfig.xml
- Sysmon64.exe -c sysmonconfig.xml

Powershell Administrator olarak açılıp aşağıdaki komutla ossec-agent kurulur.

- Invoke-WebRequest -Uri https://packages.wazuh.com/3.x/windows/wazuh-agent-3.11.2-1.msi -OutFile wazuh-agent.msi; wazuh-agent.msi /q ADDRESS='192.168.50.210' AUTHD_SERVER='192.168.50.210'

Administrator Powershell ile Wazuh agent başlatılır:

- Restart-Service -Name wazuh

ÖZGEÇMİŞ

Firdevs Sevde TOKER, ilk, orta ve lise eğitimini Sakarya'da tamamladı. Sakarya Üniversitesi Bilgisayar Mühendisliği Bölümü'nü 2016 yılında bitirdi. 2018 yılında Sakarya Üniversitesi Bilgisayar Mühendisliği Bölümü'nde yüksek lisans eğitimine başladı. 2019 yılında Sakarya Üniversitesi'nde araştırma görevlisi olarak çalışmaya başladı. Halen Sakarya Üniversitesi Bilgisayar Mühendisliği Bölümü'nde Araştırma Görevlisi olarak görev yapmaktadır.