Saldırı Tespit Sistemleri ve Olay Yönetimi
Snort, Wazuh ve TheHive

Firdevs Sevde TOKER

İÇERİK

- Saldırı Tespit Sistemleri
- Uç Nokta Saldırı Tespit Sistemleri
- Ağ Tabanlı Saldırı Tespit Sistemleri
- Olay Yönetimi

Saldırı Tespit Sistemleri (Intrusion Detection Systems -IDS)

- Sistemin CIA metriklerini ihlal eden durumların analiz edilerek **istenmeyen/olumsuz durum kararının** verilmesini sağlayan sistemlerdir.
- Sistemin izlenebilirliği, Alarm üretimi, Log toplama-anlamlandırma
- Cihaz yapılandırmalarındaki hata/sorunların tespit edilmesi
- Regülasyon uyumluluk kontrolleri

SALDIRI TESPİT SİSTEMLERİ (Intrusion Detection Systems -IDS)

Ortamına Göre IDS Türleri

- Ağ tabanlı (NIDS)
- Uç Nokta Tabanlı (HIDS)
- Protokol Tabanlı Saldırı Algılama Sistemi (PIDS)
- Uygulama Protokolü Tabanlı Saldırı Algılama Sistemi (APIDS)
- Hibrit
- …

Tespit Yöntemine Göre IDS Türleri

- İmza Tabanlı
- Anomali Tabanlı
- İtibar tabanlı tespit
- Durumsal protokol analizi
- …

İmza Tabanlı IDS

- Olası tehditleri saptamak için zararlı aktiviteyi arayarak daha önceden tespit edilmiş saldırı imzaları ile karşılaştırır.

Avantajlar

- İmza tanımlarının bilinen saldırı durumlarına göre modellenmesi
- Anlaşılabilir ve hızlı kullanım

Dezvantajlar

- Zero-day zafiyetlerinden oluşacak saldırılar tespit edilemez.
- İmza veritabanının sürekli güncel tutulması gerekliliği

Anomali Tabanlı IDS

- Ortam durumunu daha önceden belirlenmiş normal durum ile karşılaştırarak normal seviyeden ciddi seviyedeki sapmaları tespit etmeye çalışır.

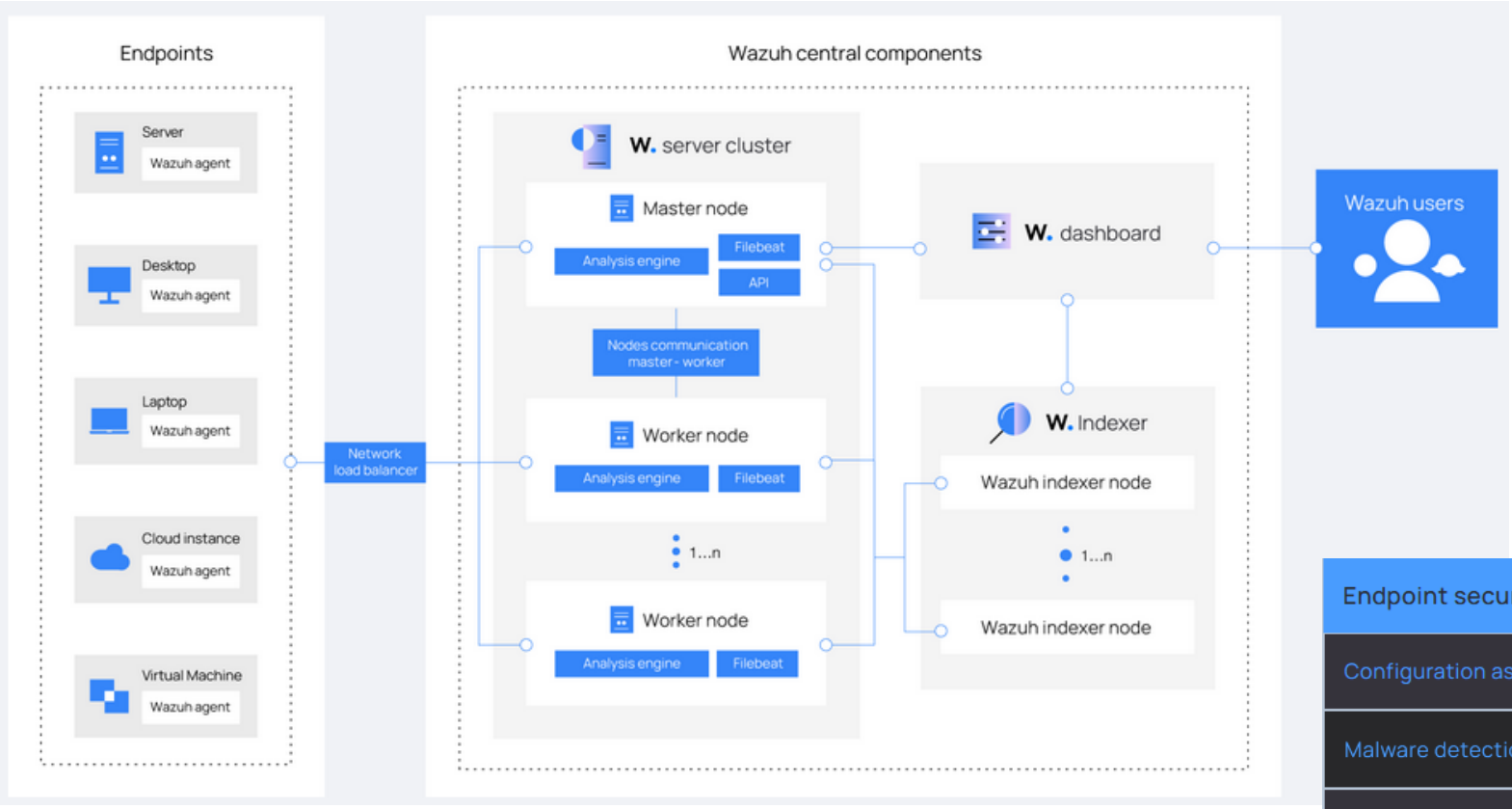
Avantajlar

- Zero-day zafiyetlerinden oluşacak saldırıları tespit etmede daha iyidir.

Dezavantajlar

- **False-positive** oranı yüksek olabilir.
- Sistem işleyişine göre «**baseline**» çıkarımı için uzun bir süre/veri gerekliliği
- Zamanla hangi saldırılara yönelik tespit oluşturacağının belirsizliği

WAZUH

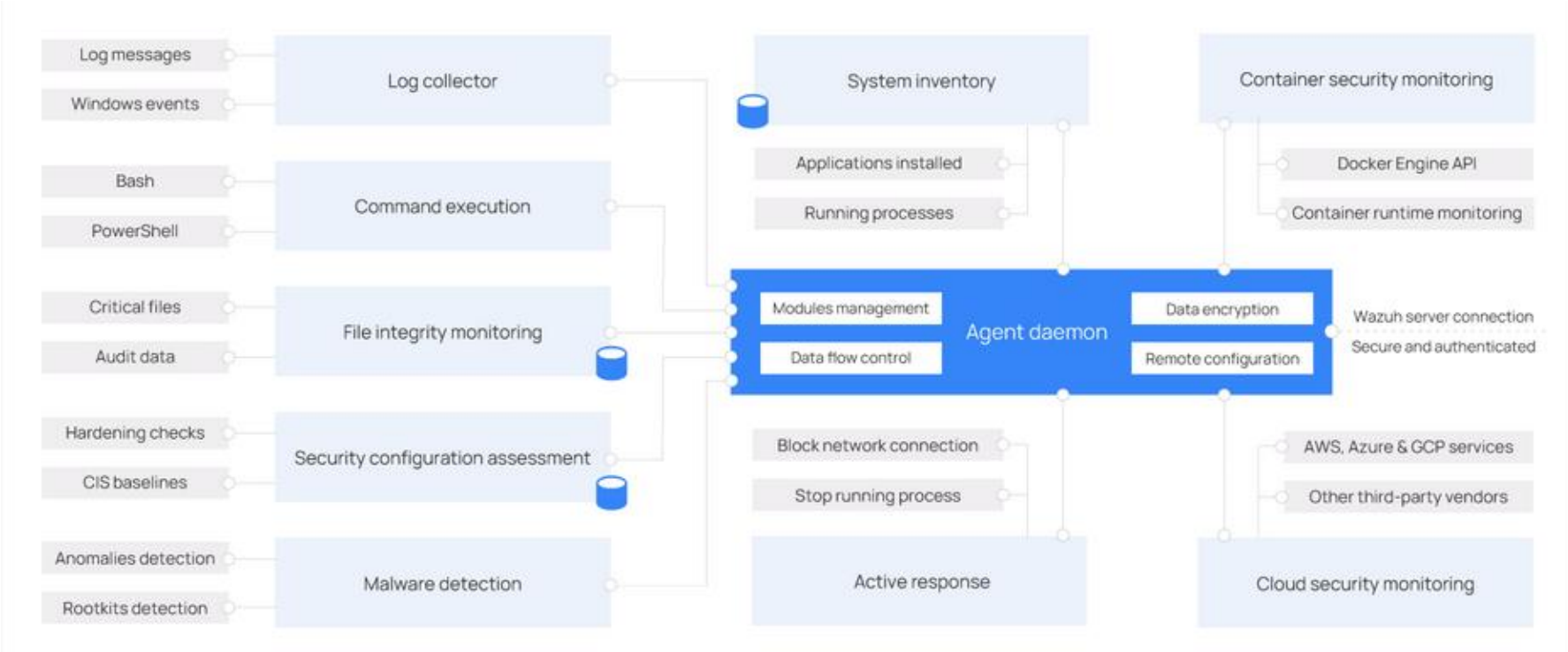


Endpoint security	Threat intelligence	Security operations	Cloud security
Configuration assessment	Threat hunting	Incident response	Container security
Malware detection	Log data analysis	Regulatory compliance	Posture management
File integrity monitoring	Vulnerability detection	IT hygiene	Workload protection

https://documentation.wazuh.com/current/getting-started/architecture.html

WAZUH – Ossec Agent

Desteklenen Agent Ortamları



https://documentation.wazuh.com/current/quickstart.html

https://documentation.wazuh.com/current/getting-started/components/wazuh-

Wazuh Decoder

```
<decoder name="ossec">
  ...
</decoder>
```

```
Apr 14 19:28:21 gorilla sshd[31274]: Connection closed by 192.168.1.33
```

Output

```
Type one log per line

Apr 14 19:28:21 gorilla sshd[31274]: Connection closed by 192.168.1.33

**Phase 1: Completed pre-decoding.
        full event: 'Apr 14 19:28:21 gorilla sshd[31274]: Connection closed by 192.168.1.33'
        timestamp: 'Apr 14 19:28:21'
        hostname: 'gorilla'
        program_name: 'sshd'

**Phase 2: Completed decoding.
        name: 'sshd'
        parent: 'sshd'
        srcip: '192.168.1.33'
```

Wazuh Kural Yapısı

```
<rule id="100001" maxsize="300" level="3">
  <if_sid>100200</if_sid>
  <match>Queue flood!</match>
  <description>Flooded events queue.</description>
</rule>
```

```
<rule id="100001" level="3">
  <if_sid>100500</if_sid>
  <regex>\d+.\d+.\d+.\d+</regex>
  <description>Matches any valid IP</description>
</rule>
```

```
<rule id="3151" level="10" frequency="8" timeframe="120">
  <if_matched_sid>3102</if_matched_sid>
  <same_source_ip />
  <description>sendmail: Sender domain has bogus MX record. </description>
  <description>It should not be sending e-mail.</description>
  <mitre>
    <id>T1114</id>
    <id>T1499</id>
  </mitre>
  <group>multiple_spam,pci_dss_11.4,gdpr_IV_35.7.d,nist_800_53_SI.4,tsc_CC6.1,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,</group>
</rule>
```

Sysmon (**Sys**tem **Mon**itoring)

- System
- Application
- Security

Default Logs

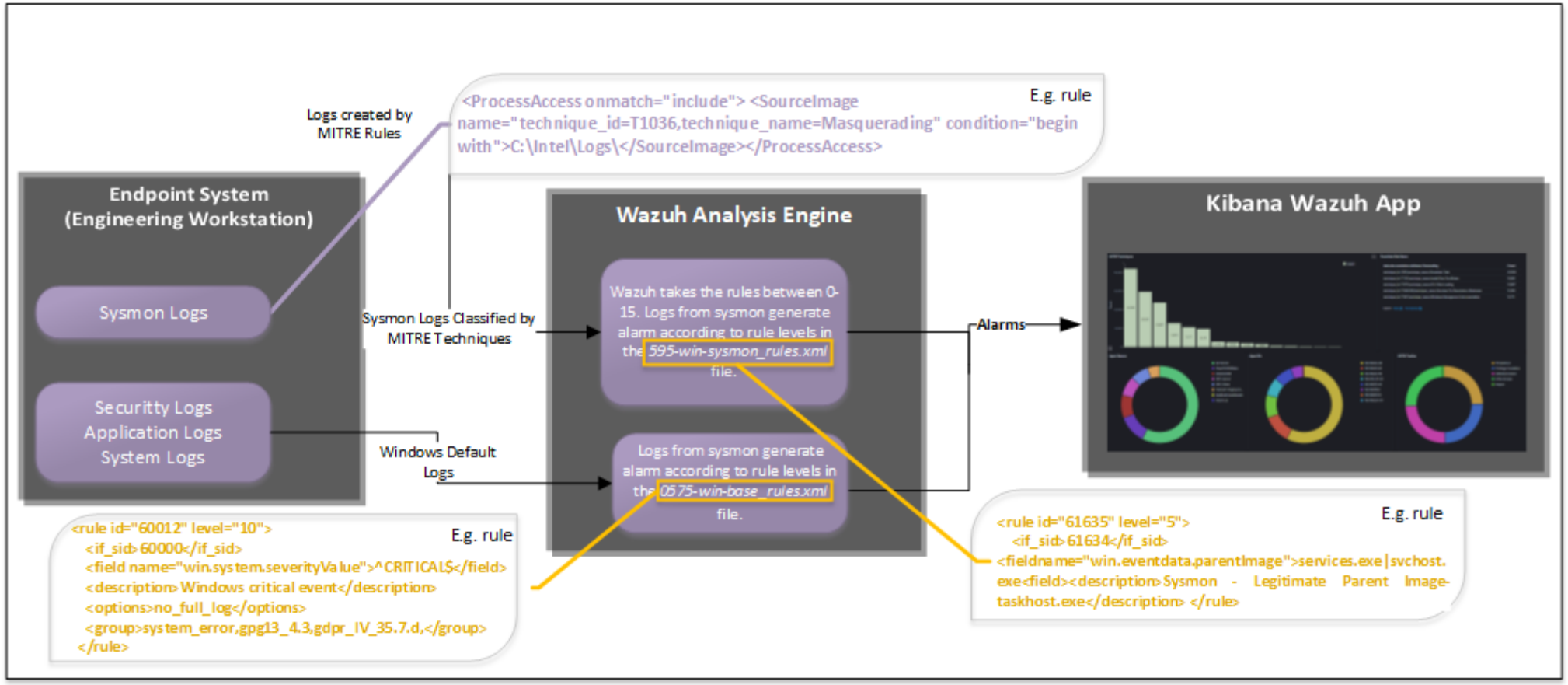
- WMI Events
- Registry Change
- …

Sysmon

ID	Tag
1 ProcessCreate	Proses oluşturulması
2 FileCreateTime	Dosya oluşturulma zamanı
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

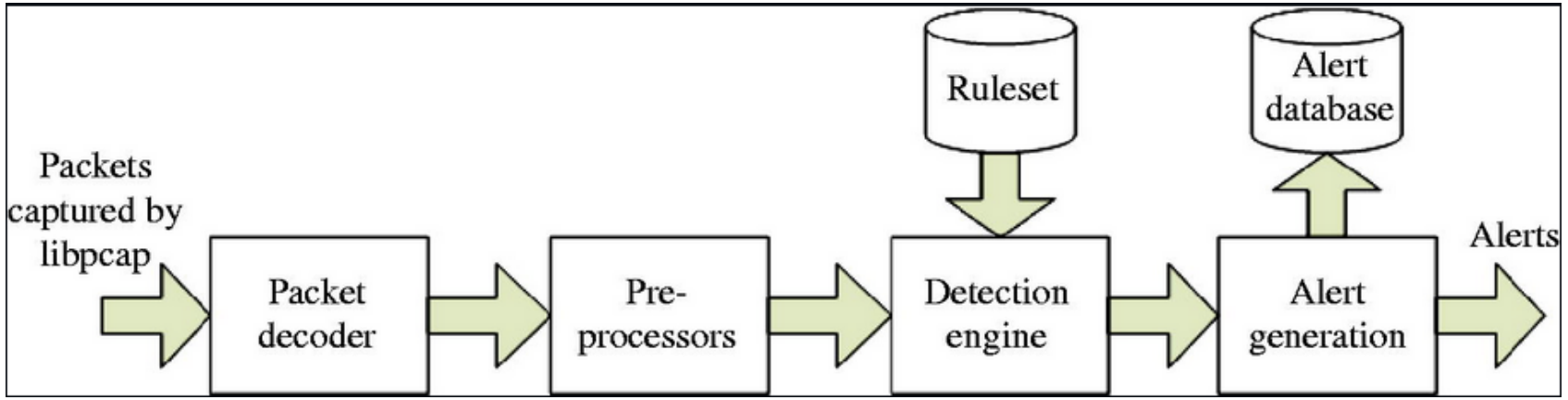
https://wazuh.com/resources/blog/detecting-process-injection-with-wazuh/sysmonconfig.xml

WAZUH Workflow



F. S. Toker, K. Ovaz Akpinar and İ. ÖZÇELİK, "MITRE ICS Attack Simulation and Detection on EtherCAT Based Drinking Water System," 2021 9th International Symposium on Digital Forensics and Security (ISDFS), Elazig, Turkey, 2021, pp. 1-6, doi: 10.1109/ISDFS52919.2021.9486331.

NIDS - Snort



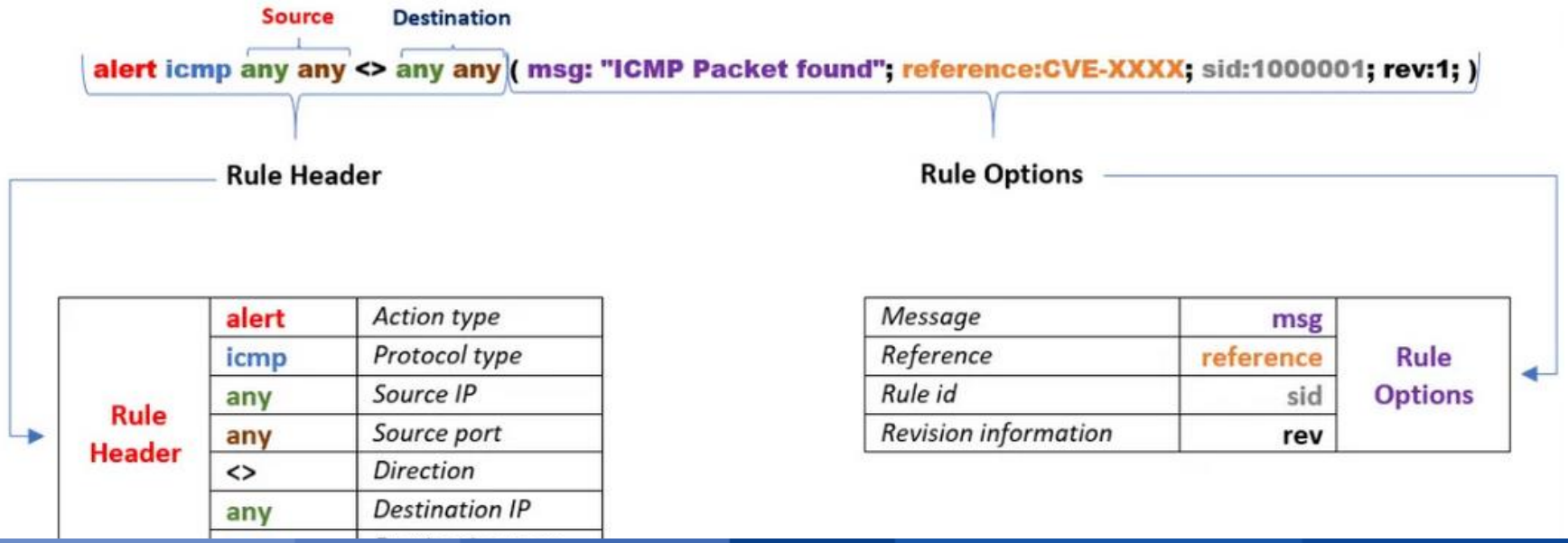
- Snort gerçek zamanlı trafik analizi ve loglama yapabilen Open-Source bir IDS/IPS güvenlik aracıdır.
- Kural tabanlı bir çalışma yapısı vardır.
- Varsayılan kurulumda ddos.rules, oracle.rules gibi birçok uygulama ve saldırı tekniğine özgü kurallar bulunmaktadır.
- Snort IDS aracıyla OT sistemlerde, TCP/UDP üzerinden haberleşen endüstriyel protokollerle ilgili custom kural yazma imkanı sağlamaktadır.

Resim:

Snort Kural Yapısı

Action	Protocol	Source IP	Source Port	Direction	Destination IP	Destination Port	Options
Alert Drop Reject	TCP UDP ICMP	ANY	ANY	<>	ANY	ANY	Msg Reference Sid Rev
Rule Header							Rule Options

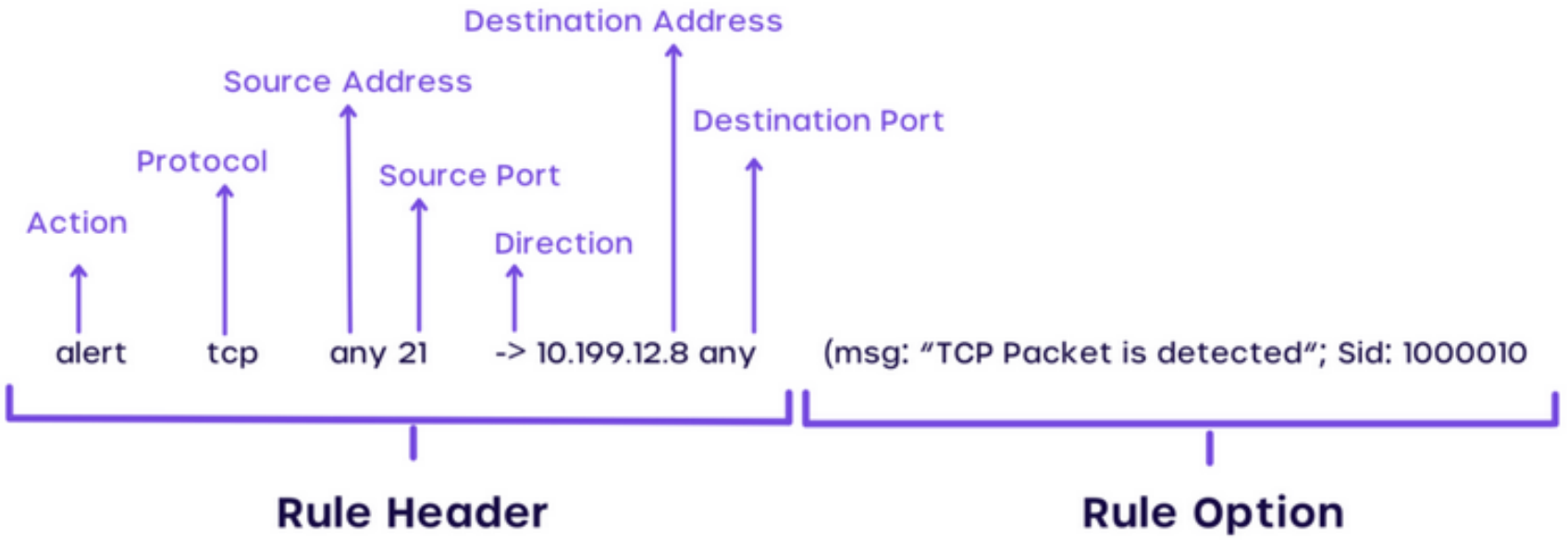
- The following rule will generate an alert for each ICMP packet processed by Snort;



https://medium.com/@kaanogut/snort-505ad08c7db9

Örnek Snort Kuralı

alert tcp any any -> 192.168.1.0/24 80 (msg:"HTTP Traffic Detected"; flow:established; sid:100001;)



https://cyvatar.ai/write-configure-snort-rules

Olay Yönetimi, TheHive

TheHive aracı SOC süreçlerinin önemli adımlarından biri olan case-management sistemidir. Sistem içerisinde «Siber Olay» meydana geldiğinde TheHive aracı ile aşağıdaki süreçler işletilebilir:

- Alarmlardan servis talebi oluşturulması
- Olayları SOC ekibinin farklı üyelerine atanması
- Olay çözülene kadar vakaların takibinin yapılması

Case Management – TheHive

- Alert Management
- Case Management
- Multi Tenant Environments
- Advanced User Management
- Metrics and Dashboards
- MISP Integration
- MITRE ATT&CK Integration
- Case Reporting

https://thehive-project.org

Olay Yönetimi, TheHive - SOAR

- Alert management
- Case management
- Multi-tenant environments
- Advanced user management
- Notifications framework
- Metrics and dashboards
- Comprehensive APIs
- MISP integration
- MITRE ATT&CK integration
- Case reporting
- Knowledge base
- Timelines

Analyzer /Responder – Cortex

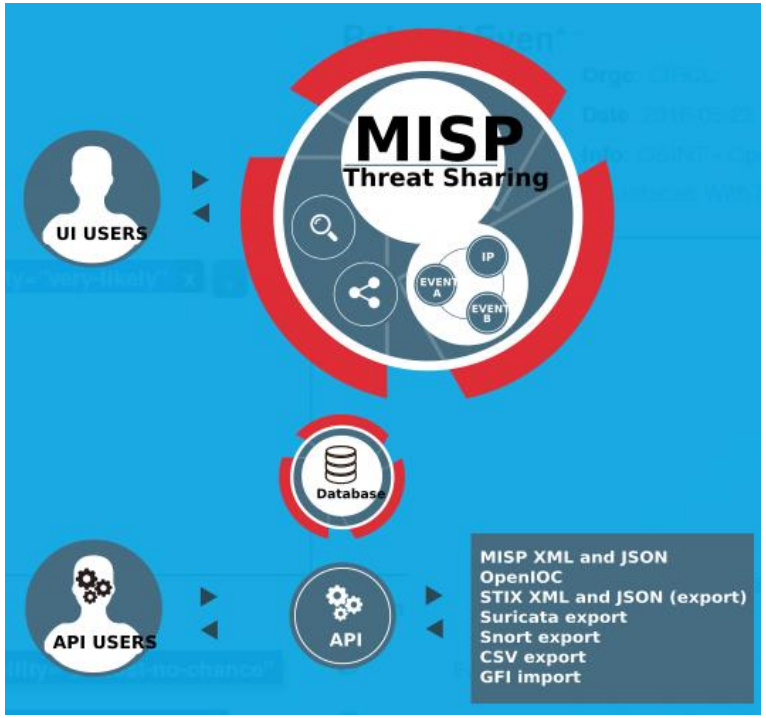
- Tek bir araç üzerinden observables (thehive findings) geniş ölçekte analiz edilebilirliği sağlar.

- Tehditlere active response için otomatize süreçler ve esnek konfigürasyon yeteneği sağlar.

https://github.com/thehive-project/Cortex/

CTI– MISP

- IoCs
- Metadata Tagging
- Multiple feeds activation
- Multiple data format support
- Visualization



https://www.misp-project.org/

SAKARYA ÜNİVERSİTESİ