

Korrelasyon Yazılması

- Ossimde korrelasyon kuralı oluřturmak için Web arayüzünden **Configuration >> Threat Intelligence >> Directives** sekmesi açılarak **New Directive** butonuna basılır.
- Korrelasyonun için isim yazılır ve Intent, Stragegy, Method ve Priority değeri belirlenir.

NAME FOR THE DIRECTIVE

MY – Scan and SSH Brute Force Attack

TAXONOMY

Intent:

Delivery & Attack

Strategy:

Bruteforce Authentication

Method:

SSH

PRIORITY

0

1

2

3

4

5

CANCEL

NEXT

- Korrelasyonu tetikleyecek olan ilk kuralın ismi yazılır.

NAME FOR THE RULE

AV – Scan and SSH Brute Force Attack

CANCEL

NEXT

- Event tipi seçilir.

Choose between **Event Types Selection** or **Taxonomy**

☒ **Event Types** ☐ **Taxonomy**

SELECT A PLUGIN

ALIENVAULT HIDS-RECON

Detector – recon

· Search a plugin name or ID:

7014

CANCEL

BACK

- İlgili alt event seçilir

Choose between Event Sub-Types Selection or Taxonomy

☒ Event Sub-Types ☐ Taxonomy

PLUGIN SIGNATURES	
1 items selected	Remove all
5706 - AlienVault HIDS: SSH insecure connection attempt (scan).	3911 - AlienVault HIDS: Multiple connection attempts from same so...
	5731 - AlienVault HIDS: SSH Scanning.
	11252 - AlienVault HIDS: Multiple connection attempts from same s...
	11307 - AlienVault HIDS: Multiple connection attempts from same s...
	11452 - AlienVault HIDS: Multiple FTP connection attempts from sa...
	11511 - AlienVault HIDS: Multiple connection attempts from same s...
	31151 - AlienVault HIDS: Multiple web server 400 error codes from ...
	31161 - AlienVault HIDS: Multiple web server 501 error code (Not I...
	31163 - AlienVault HIDS: Multiple web server 503 error code (Servi...
	40601 - AlienVault HIDS: Network scan from same source ip.
	51006 - AlienVault HIDS: Client exited before authentication.

Empty selection means ANY signature

CANCEL BACK NEXT

- Kaynak ve hedef adresler belirlenir.

Empty selection means ANY asset

NETWORK	
SOURCE HOST/NETWORK	DESTINATION HOST/NETWORK
<p>Asset: <input type="text"/> FILTER ADD IP</p> <p>All Assets</p> <p>Assets</p> <p>Asset Groups</p> <p>Networks</p> <p>HOME NET IHOME NET</p>	<p>Asset: <input type="text"/> FILTER ADD IP</p> <p>All Assets</p> <p>Assets</p> <p>Asset Groups</p> <p>Networks</p> <p>HOME NET IHOME NET</p>
SOURCE PORT(S)	DESTINATION PORT(S)
<p>Use comma to specify several ports</p> <p>Can be negated using '!'</p> <p>Reputation options</p>	<p>Use comma to specify several ports</p> <p>Can be negated using '!'</p> <p>Reputation options</p>

CANCEL BACK NEXT

- Reliability değeri seçilir.

NOT! : AlienVaultta risk hesaplaması $priority * reliability * asset_value / 25$ olarak hesaplanır. Sonuç 1 'den büyükse alarm üretilir.

- Risk kategorileri :
 - 0,1,2 = Low
 - 3,4 = Precaution
 - 5,6 = Elevated
 - 7,8 = High

- 9,10 = Very High

RELIABILITY

· $Risk = (priority * reliability * asset_value) / 25.$

= 0

= 1

= 2

= 3

= 4

= 5

= 6

= 7

= 8

= 9

= 10

CANCEL BACK

- Finish butonuna tıklanarak ilk kuralın oluşturulması tamamlanır.

RULE DEFINED

Would you like to specify any other condition for this rule (Protocol, Sensor, Special fields...)?

BACK FINISH NEXT

- İlk kural oluştuktan sonra oluşması beklenen ikinci kuralı tanımlamak için Action sekmesindeki + butonuna tıklanır.

New Directive Test Directives Restart Server Search a directive name: SEARCH

▼ User Contributed [1 directive]

▼ MY – Scan and SSH Brute Force Attack
Delivery & Attack, Bruteforce Authentication, SSH – Priority 3

▼ RULES

NAME	RELIABILITY	TIMEOUT	OCCURRENCE	FROM	TO	DATA SOURCE	EVENT TYPE	[...]	ACTION
AV – Scan and SSH Brute Force Attack	5	None	1	✦ ANY	✦ ANY	✦ AlienVault HIDS–recon (7014)	✦ SIDs: 5706	► More	+

► DIRECTIVE INFO

- İkinci kuralın adı girilir.

NAME FOR THE RULE

SSH Brute Force Attack

CANCEL NEXT

- Event tipi seçilir.

Choose between **Event Types Selection** or **Taxonomy**

☒ **Event Types** ☐ **Taxonomy**

SELECT A PLUGIN

ALIENVAULT HIDS-AUTHENTICATION_FAILED

Detector – authentication_failed

• **Search** a plugin name or ID:

CANCEL

BACK

- İlgili alt event seçilir

Choose between Event Sub-Types Selection or Taxonomy

☒ Event Sub-Types ☐ Taxonomy

PLUGIN SIGNATURES		
1 items selected	Remove all	Add all
5716 - AlienVault HIDS: SSHD authentication failed.	—	2501 - AlienVault HIDS: User authentication failure. +
		2502 - AlienVault HIDS: User missed the password more than one ti... +
		3332 - AlienVault HIDS: Postfix SASL authentication failure. +
		3601 - AlienVault HIDS: Imapd user login failed. +
		3902 - AlienVault HIDS: Courier (imap/pop3) authentication failed. +
		4321 - AlienVault HIDS: Failed login attempt at the PIX firewall. +
		4324 - AlienVault HIDS: Password mismatch while running 'enable' ... +
		4334 - AlienVault HIDS: AAA (VPN) authentication failed. +
		4336 - AlienVault HIDS: AAA (VPN) user locked out. +
		4724 - AlienVault HIDS: Failed login to the router. +
		4811 - AlienVault HIDS: Firewall authentication failure. +

· Empty selection means ANY signature

CANCEL

BACK

SELECTED FROM LIST

PLUGIN SID FROM RULE OF LEVEL 1

!PLUGIN SID FROM RULE OF LEVEL 1

- Kaynak ve hedef adresler seçilir. Bir önceki kuraldaki kaynak ve hedef ile eşleşmesi isteniyorsa “From a parent rule” kısmından aşağıdaki görüntüdeki gibi seçim yapılır.

NETWORK	
· Empty selection means ANY asset	
SOURCE HOST/NETWORK	DESTINATION HOST/NETWORK
From a parent rule: <input type="text" value="Source IP from level 1"/>	From a parent rule: <input type="text" value="Destination IP from level 1"/>
SOURCE PORT(S)	DESTINATION PORT(S)
· Use comma to specify several ports · Can be negated using '!' From a parent rule: <input type="text"/>	· Use comma to specify several ports · Can be negated using '!' From a parent rule: <input type="text"/>
► Reputation options	► Reputation options
CANCEL	BACK NEXT

- Reliability değeri seçilir.

RELIABILITY

$\cdot Risk = (priority * reliability * asset_value) / 25.$

= 0	+ 0
= 1	+ 1
= 2	+ 2
= 3	+ 3
= 4	+ 4
= 5	+ 5
= 6	+ 6
= 7	+ 7
= 8	+ 8
= 9	+ 9
= 10	+ 10

CANCEL

BACK

- Kuralın oluşturulması tamamlanır.

RULE DEFINED

Would you like to specify any other condition for this rule (Protocol, Sensor, Special fields...)?

BACK

FINISH

NEXT

- İlk kural oluştuktan sonra ikinci kuralın oluşması için beklenilecek süre belirlenir.

▼ ✓ 📄 🗑️ ✎ **MY – Scan and SSH Brute Force Attack**
Delivery & Attack, Bruteforce Authentication, SSH – Priority 3

▼ **RULES**

NAME	RELIABILITY	TIMEOUT	OCCURRENCE
▼ AV – Scan and SSH Brute Force Attack	5	None	1
SSH Brute Force Attack	+10	60	1

▶ **DIRECTIVE INFO**

- İlk kural oluştuktan sonra ikinci kuralın kaç kez oluşması gerektiği belirlenir.

▼ ✓ 📄 🗑️ ✎ **MY – Scan and SSH Brute Force Attack**
Delivery & Attack, Bruteforce Authentication, SSH – Priority 3

▼ **RULES**

NAME	RELIABILITY	TIMEOUT	OCCURRENCE
▼ AV – Scan and SSH Brute Force Attack	5	None	1
SSH Brute Force Attack	+10	60	2

▶ **DIRECTIVE INFO**

- İşlemler tamamlandıktan sonra “Restart Server” butonuna basılır. (restart etmeden önce “test directives” butonuna basarak oluşturduğunuz korelasyon kurallarında hata olup olmadığını test edebilirsiniz.)

New Directive Test Directives Restart Server Search a directive name: brute SEARCH CLEAR

▼ User Contributed [1 directive]

▼ MY – Scan and SSH Brute Force Attack
Delivery & Attack, Bruteforce Authentication, SSH – Priority 3

▼ RULES

NAME	RELIABILITY	TIMEOUT	OCCURRENCE	FROM	TO	DATA SOURCE	EVENT TYPE	[...]	ACTION
▼ AV – Scan and SSH Brute Force Attack	5	None	1	+	ANY	+	ANY	+	AlienVault HIDS-recon (7014)
SSH Brute Force Attack	+10	60	2	+	1:SRC_IP	+	1:DST_IP	+	AlienVault HIDS-authentication_failed (7010)

► DIRECTIVE INFO

Kuralın Test Edilmesi

- **Analysis >> Alarms** bölümünden oluşan alarmlar takip edilir.
- İlk kuralın tetiklenmesi sağlanır. (nmap ile tarama yapılarak oluşturulabilir)
- İlk tarama sonrası alarmın oluştuğu ve risk seviyesinin 1 olduğu gözlemlenir.

SHOW 20 ENTRIES ACTIONS

DATE	STATUS	INTENT & STRATEGY	METHOD	RISK	OTX	SOURCE	DESTINATION
7 secs		Bruteforce Authentication	SSH	1	N/A	Host-192-168-1-6	Host-192-168-1-10

- 1 dakika içerisinde 2 adet başarısız ssh erişimi aktivitesi yapılarak korelasyonun çalışması ve risk değerinin 2 'ye yükselmesi gözlemlenir.

DATE	STATUS	INTENT & STRATEGY	METHOD	RISK	OTX	SOURCE	DESTINATION
2017-01-08 17:13:59	open	Bruteforce Authentication	SSH	2	N/A	Host-192-168-1-6:62007	Host-192-168-1-10

- Ayrıca yapılan bu işlemlerin tamamına **Analysis >> SIEM** bölümünden ulaşılabilir.

SIGNATURE	DATE GMT+3:00	SENSOR	OTX	SOURCE	DESTINATION	RISK
AlienVault HIDS: SSHD authentication failed.	2017-01-08 17:13:59	VirtualUSMAllInOne	N/A	Host-192-168-1-6:62007	Host-192-168-1-10	1
directive_event: MY - Scan and SSH Brute Force Attack	2017-01-08 17:13:59	N/A	N/A	Host-192-168-1-6:62007	Host-192-168-1-10	2
AlienVault HIDS: SSHD authentication failed.	2017-01-08 17:13:57	VirtualUSMAllInOne	N/A	Host-192-168-1-6:62007	Host-192-168-1-10	1
AlienVault HIDS: SSH insecure connection attempt (scan).	2017-01-08 17:13:29	VirtualUSMAllInOne	N/A	Host-192-168-1-6	Host-192-168-1-10	0
directive_event: MY - Scan and SSH Brute Force Attack	2017-01-08 17:13:29	N/A	N/A	Host-192-168-1-6	Host-192-168-1-10	1