

SIEM – VAR OLAN VERİLERİN ANLAMI

MEHMET KILIÇ
HACKTRICKCONF

İÇERİK

- SIEM Nedir? Ne Değildir?
- SIEM Ürünleri
- SIEM Yetenekleri
- HP ArcSight
- IBM QRadar
- Etkin Log Korelasyonu

“ SIEM is defined as a complex set of technologies brought together to provide a holistic view into a technical infrastructure. Depending on who you talk to, there are about five different popular opinions on what the letters stand for ”

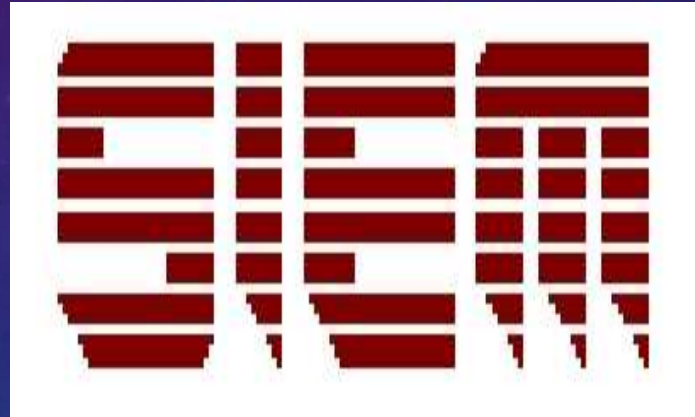
Security Information and Event Management

SIEM ÜRÜNLERİ



SIEM YETENEKLERİ

- Event/Log Toplama
- Normalizasyon
- Korelasyon
- Aggregation
- Raporlama
- Alarm
- Log Yönetimi (Regülasyonlar)



SIEM ÖZELLİKLERİ



İŞLEYİŞ/SÜREÇ



HP ARCSIGHT COMMAND CENTER



The screenshot displays the HP ArcSight Command Center interface. At the top, there's a navigation bar with 'Dashboards', 'Events', 'Reports', 'Cases', 'Applications', and 'Administration'. The 'Events' tab is active. Below the navigation bar, there's a search bar with a 'Go!' button. A 'Field Summary' panel on the left shows a bar chart of event counts over time, with a legend indicating '1 bar = 5 second'. The main area shows a table of events with columns: Time (Event Time), Device, Node, deviceVendor, deviceProduct, and deviceVersion. A modal window titled 'deviceVendor (5)' is open, showing a bar chart of event counts by device vendor, with a legend indicating '1 bar = 5 second'.

Field Value	Count	%
ArcSight	1,536	47.392%
Microsoft	1,057	32.613%
Unix	468	14.439%
Tumbleweed	162	4.998%
McAfee	18	0.555%

HP ARCSIGHT CONSOLE

The screenshot displays the HP ArcSight console interface. The main window is titled "Viewer" and shows a list of events. The "Inspector/Editor" window is open on the right, showing the configuration for a rule named "Rule: Account Added to Privileged...".

Viewer Window:

- Connector Connection and Cache Status: Untitled Active Channel
- Active Channel: Untitled Active Channel
- Total Events: 22,140
- Start Time: 4 May 2016 17:49:24 EEST
- End Time: 4 May 2016 19:49:24 EEST
- Filter: Device Vendor != "ArcSight"
- Inline Filters: No Filter
- Verified Rules: No Rule
- Severity: Very High: 0, High: 1,557, Medium: 2,382, Low: 15,801, Very Low: 2,400
- Radar: A bar chart showing event frequency over time.
- Table of Events:

Manager Receipt Time	End Time	Name	Attacker Address	Target Address	Priority	Device Vendor
4 May 2016 19:49:24 EEST	4 May 2016 19:49:06 EEST	An account was logged off.			3	Microsoft
4 May 2016 19:49:24 EEST	4 May 2016 19:49:06 EEST	An account was logged off.			3	Microsoft
4 May 2016 19:49:19 EEST	4 May 2016 19:49:00 EEST	A privileged service was called.			5	Microsoft
4 May 2016 19:49:19 EEST	4 May 2016 19:49:00 EEST	A privileged service was called.			5	Microsoft
4 May 2016 19:49:19 EEST	4 May 2016 19:49:00 EEST	A privileged service was called.			5	Microsoft
4 May 2016 19:49:19 EEST	4 May 2016 19:49:06 EEST	ID4FE20EDF: uid=0 from=<root>			7	Unix
4 May 2016 19:49:19 EEST	4 May 2016 19:49:06 EEST	ID4FE20EDF: uid=0 from=<root>			7	Unix
4 May 2016 19:49:19 EEST	4 May 2016 19:49:06 EEST	postfix cleanup message ID			2	Tumbleweed
4 May 2016 19:49:19 EEST	4 May 2016 19:49:06 EEST	postfix cleanup message ID			2	Tumbleweed
4 May 2016 19:49:19 EEST	4 May 2016 19:49:06 EEST	queue active			2	Tumbleweed
4 May 2016 19:49:19 EEST	4 May 2016 19:49:06 EEST	queue active			2	Tumbleweed
4 May 2016 19:49:19 EEST	4 May 2016 19:49:06 EEST	(02307-14) ESMTTP: [127.0.0.1]:10024...			7	Unix
4 May 2016 19:49:19 EEST	4 May 2016 19:49:06 EEST	(02307-14) ESMTTP: [127.0.0.1]:10024...			7	Unix
4 May 2016 19:49:19 EEST	4 May 2016 19:49:06 EEST	(02307-14) Chedding: RK69Q5b18C90...			7	Unix
4 May 2016 19:49:19 EEST	4 May 2016 19:49:06 EEST	(02307-14) Chedding: RK69Q5b18C90...			7	Unix
4 May 2016 19:49:19 EEST	4 May 2016 19:49:06 EEST	query	192.168.2.12	192.168.2.12	3	Unix
4 May 2016 19:49:19 EEST	4 May 2016 19:49:06 EEST	createfetch			3	Unix
4 May 2016 19:49:19 EEST	4 May 2016 19:49:06 EEST	createfetch			3	Unix
4 May 2016 19:49:19 EEST	4 May 2016 19:49:06 EEST	query	192.168.2.12	192.168.2.12	4	Unix
4 May 2016 19:49:19 EEST	4 May 2016 19:49:06 EEST	query	192.168.2.12	192.168.2.12	4	Unix
4 May 2016 19:49:19 EEST	4 May 2016 19:49:06 EEST	query	192.168.2.12	192.168.2.12	4	Unix

Inspector/Editor Window:

- Rule: Account Added to Privileged...
- Attributes: Conditions, Aggregation, Actions, Local Variables, Notes
- Event conditions:

 - AND
 - Type = Base
 - Device Vendor = Microsoft
 - Device Product = Microsoft Windows
 - Category Device Group = /Operating System
 - OR
 - Device Event Class ID = Microsoft-Windows-Security-Auditing-
 - Device Event Class ID = Microsoft-Windows-Security-Auditing-
 - Device Custom String6 = "CR1\\Domain Admins"

Common Conditions:

Name	Op	Condition
Event		
Aggregated Event C...		
Application Protocol		
Bytes In		
Bytes Out		
Correlated Event Count		
Customer		
Domain		

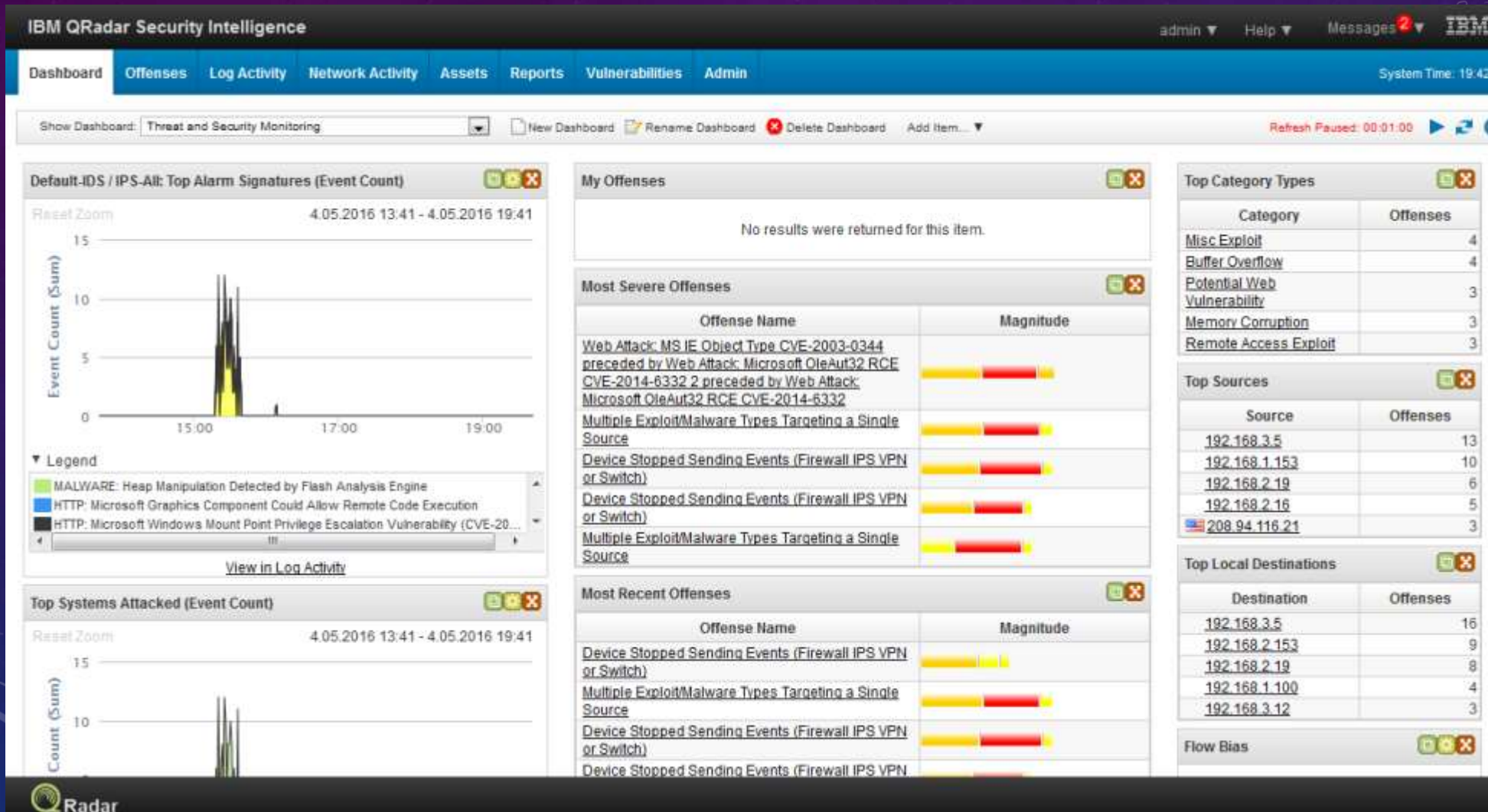
Search for: [Search bar]

Buttons: Test, OK, Cancel, Apply, Help

ARCSIGHT LOG ENTEGRASYONU

- ArcSight SmartConnector
- Alınmak İstenen Log Kaynağı ?
- ArcSight'ın Doğrudan Desteği Bulunuyor mu?
- ArcSight FlexConnector

IBM QRADAR



IBM QRADAR LOG AKTIVİTESİ

IBM QRadar Security Intelligence

admin ▾ Help ▾ Messages ² ▾ IBM

Dashboard Offenses **Log Activity** Network Activity Assets Reports Vulnerabilities Admin

System Time: 20:03

Search... ▾ Quick Searches ▾ Add Filter Save Criteria Save Results Cancel False Positive Rules ▾ Actions ▾

Quick Filter ▾ Search

Viewing real time events View: Select An Option: ▾ Display: Default (Normalized) ▾

Using Search: Ignore system log

Current Filters:

Event Name is not Information Message (Clear Filter) Event Name is not Health Metric (Clear Filter) Log Source is not SIM Generic Log DSM-7 :: qradar (Clear Filter)

Log Source is not SIM Audit-2 :: qradar (Clear Filter)

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	D
Success Audit: The Windows Filtering Platform has allowed a connection		5	4 May 2016 20:04:21	Access Permitted	192.168.3.10	56569	19
Success Audit: An account was logged off		4	4 May 2016 20:04:21	Host Logout	192.168.3.10	0	19
Success Audit: Network Share Object Checked for Access		2	4 May 2016 20:04:21	Information	192.168.3.10	56568	19
Success Audit: Successful logon with administrative or special privileges		4	4 May 2016 20:04:21	Admin Login Successful	192.168.3.10	0	19
Success Audit: The Windows Filtering Platform has allowed a connection		2	4 May 2016 20:04:21	Access Permitted	192.168.3.10	56568	19
Success Audit: An account was successfully logged on		4	4 May 2016 20:04:21	User Login Success	192.168.3.10	56568	19
Success Audit: A network share object was accessed		1	4 May 2016 20:04:21	Information	192.168.3.10	56568	19
Success Audit: The Windows Filtering Platform has permitted a bind to a local ...		1	4 May 2016 20:04:31	Access Permitted	192.168.3.10	0	19
Success Audit: An operation was performed on an object		8	4 May 2016 20:04:21	Information	192.168.3.10	0	19
Failure Audit: A privileged service was called	192.168.3.14@win8	3	4 May 2016 20:04:10	Misc Authorization	192.168.3.14	0	19
Success Audit: The Windows Filtering Platform has permitted a bind to a local ...		1	4 May 2016 20:04:21	Access Permitted	192.168.3.10	0	19
Success Audit: The Windows Filtering Platform has permitted a bind to a local ...		1	4 May 2016 20:04:21	Access Permitted	0.0.0.0	0	19
Success Audit: The Windows Filtering Platform has allowed a connection		1	4 May 2016 20:04:10	Access Permitted	192.168.3.10	56566	19
HTTP: Firefuzzer SQL Injection Scanning II	IntruShield @ GMT	1	4 May 2016 20:04:20	Host Port Scan	192.168.1.153	59654	19
HTTP: Firefuzzer SQL Injection Scanning II	IntruShield @ GMT	1	4 May 2016 20:04:20	Host Port Scan	192.168.1.153	59654	19
HTTP: SQL Injection - detection DB2	IntruShield @ GMT	1	4 May 2016 20:04:16	SQL Injection	192.168.1.153	59651	19

IBM QRADAR OFFENSES

IBM QRadar Security Intelligence admin ▼ Help ▼ Messages ² ▼ IBM

Dashboard Offenses Log Activity Network Activity Assets Reports Vulnerabilities Admin System Time: 20:05

Offenses

Search... Save Criteria Actions ▼ Print Last Refresh: 00:00:05

All Offenses View Offenses: Select An Option: ▼

Current Search Parameters:
 Exclude Hidden Offenses (Clear Filter) Exclude Closed Offenses (Clear Filter)

	Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destina
	37	Web Attack: MS IE Object Type CVE-2003-0344 preceded by Web Attack: Microsoft O...	Source IP	208.94.116.21	3	208.94.116.21	Local (2)
	23	Multiple Exploit/Malware Types Targeting a Single Source	Destination IP	192.168.1.100	3	192.168.1.153	192.168
	19	Multiple Exploit/Malware Types Targeting a Single Source	Destination IP	192.168.2.153	3	192.168.1.153	192.168
	27	Device Stopped Sending Events (Firewall IPS VPN or Switch)	Rule	Buffer Overflow Attempt	3	Multiple (3)	Local (4)
	25	Device Stopped Sending Events (Firewall IPS VPN or Switch)	Rule	SQL Injection Detected	3	192.168.1.153	192.168
	26	Device Stopped Sending Events (Firewall IPS VPN or Switch)	Rule	Misc Exploit Detected	3	192.168.1.153	192.168
	28	Device Stopped Sending Events (Firewall IPS VPN or Switch)	Rule	Remote Access Exploit D...	3	Multiple (2)	Local (3)
	22	HTTP: Cross Site Scripting Cheat Sheet	Rule	Cross Site Scripting Dete...	3	192.168.1.153	192.168
	30	HTTP: Microsoft SharePoint ws asmx Denial of Service Vulnerability	Event Name	HTTP: Microsoft SharePoi...	3	192.168.1.153	192.168
	24	Device Stopped Sending Events (Firewall IPS VPN or Switch)	Rule	Web Attack Tespit Edlidi	3	192.168.1.153	Local (2)
	31	HTTP: Apache httpd mod_deflate Resource Exhaustion Denial Of Service	Event Name	HTTP: Apache httpd mod_...	3	192.168.1.153	192.168
	18	Web Attack: Microsoft OleAut32 RCE CVE-2014-6332 2 preceded by Web Attack: Mic...	Source IP	208.94.116.21	3	208.94.116.21	192.168
	29	Actual action: Cleaned by deletion preceded by Virus Detected	Rule	Malicious File Detected	3	Multiple (2)	WIN-SYI
	14	Multiple Login Failures for the Same User containing Privilege Escalation Failed	Username	cri	2	192.168.2.19	192.168
	16	Multiple Login Failures for the Same User containing Root Login Failed	Username	root	2	192.168.1.164	192.168
	15	Exploit Followed by Suspicious Host Activity - Chained	Source IP	192.168.3.5	2	192.168.3.5	WIN-SYI
	36	Audit Log Cleared	Rule	Audit log was cleared.	2	Multiple (2)	Local (2)
	33	Audit Log Cleared	Rule	Audit log was cleared.	2	192.168.3.5	WIN-SYI

IBM QRADAR LOG ENTEGRASYONU

- Log Sources

Add a log source

Log Source Name	<input type="text"/>
Log Source Description	<input type="text"/>
Log Source Type	3Com 8800 Series Switch
Protocol Configuration	Syslog
Log Source Identifier	<input type="text"/>
Enabled	<input checked="" type="checkbox"/>
Credibility	5
Target Event Collector	eventcollector0 :: qradar
Coalescing Events	<input checked="" type="checkbox"/>
Incoming Payload Encoding	UTF-8
Store Event Payload	<input checked="" type="checkbox"/>

Please select any groups you would like this log source to be a member of:

☒ IPS
☒ Linux
☒ SEP
☒ Windows

Save Cancel

ETKİN LOG KORELASYONU

The screenshot displays the ArcSight Rule Editor interface. The top tabs include Attributes, Conditions, Aggregation, Actions, Local Variables, and Notes. The main workspace shows a rule configuration with the following structure:

- Event conditions**
 - Matching Event**
 - AND**
 - `AttackEvent.Attacker Address = ResponseEvent.Target Address`
 - `AttackEvent.Target Address = ResponseEvent.Attacker Address`
 - AttackEvent**
 - AND**
 - NOT**
 - `InActiveList("/All Active Lists/ArcSight System/Attackers/Trusted List")`
 - OR**
 - `Category Significance StartsWith /Compromise`
 - `Category Significance = /Hostile`
 - AND**
 - `Category Outcome != /Failure`
 - `Category Outcome Is NOT NULL`
 - OR**
 - AND**
 - `Category Behavior = /Communicate/Query`
 - `Category Technique = /Exploit/Vulnerability`
 - AND**
 - `Category Behavior StartsWith /Execute`

At the bottom, there is a **Common Conditions Editor** table:

Name	Op	Condition	As	⊗
Event				
Aggregated Event C...				

Below the table is a search bar labeled "Search for:" and a green "Test" button.

The screenshot shows the **Rule Wizard: Rule Test Stack Editor** window. It asks, "Which tests do you wish to perform on incoming events?".

Test Group: All

Export as Building Block: [Button]

Type to filter:

- when the local network is one of the following networks
- when the destination network is one of the following networks
- when the IP protocol is one of the following protocols
- when the Event Payload contains this string
- when the source port is one of the following ports
- when the destination port is one of the following ports
- when the local port is one of the following ports
- when the remote port is one of the following ports
- when the source IP is one of the following IP addresses
- when the destination IP is one of the following IP addresses
- when the local IP is one of the following IP addresses

Rule (Click on an underlined value to edit it)
Invalid tests are highlighted and must be fixed before rule can be saved.

Apply Excessive Firewall Denies from Single Source on events which are detected by the Local system

and NOT when an event matches any of the following BB:HostDefinition: Servers

and when any of these BB:CategoryDefinition: Firewall or ACL Denies with the same source IP more than 50 times, across exactly 1 destination IP within 15 minutes

Please select any groups you would like this rule to be a member of:

- ☒ Anomaly
- ☐ Asset Reconciliation Exclusion
- ☐ Authentication
- ☐ Botnet
- ☒ Category Definitions

Notes (Enter your notes about this rule)

Navigation buttons: << Back, Next >>, Finish, Cancel

SIEM VE TEHDİT İSTİHBARATI

- Command and Controller Tespiti
- Malicious Connections
- Email Pattern



TEŞEKKÜRLER

???