SIEM – VAR OLAN VERİLERİN ANLAMI

MEHMET KILIÇ

HACKTRICKCONF

İÇERİK

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

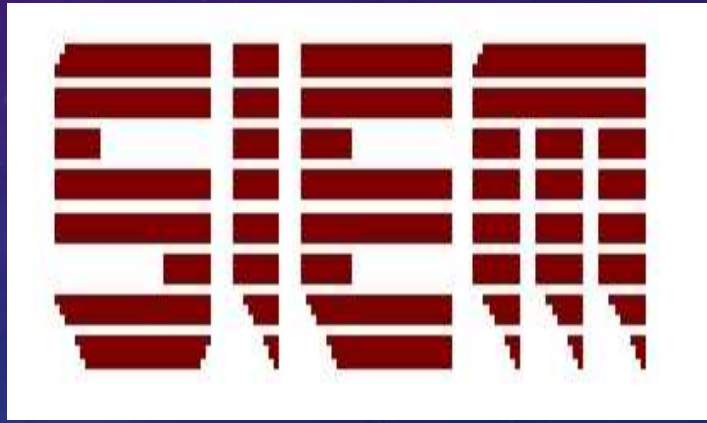
“SIEM is defined as a complex set of technologies brought together to provide a holistic view into a technical infrastructure. Depending on who you talk to, there are about five different popular opinions on what the letters stand for”

Security Information and Event Management

SIEM ÜRÜNLERİ

SIEM YETENEKLERİ

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

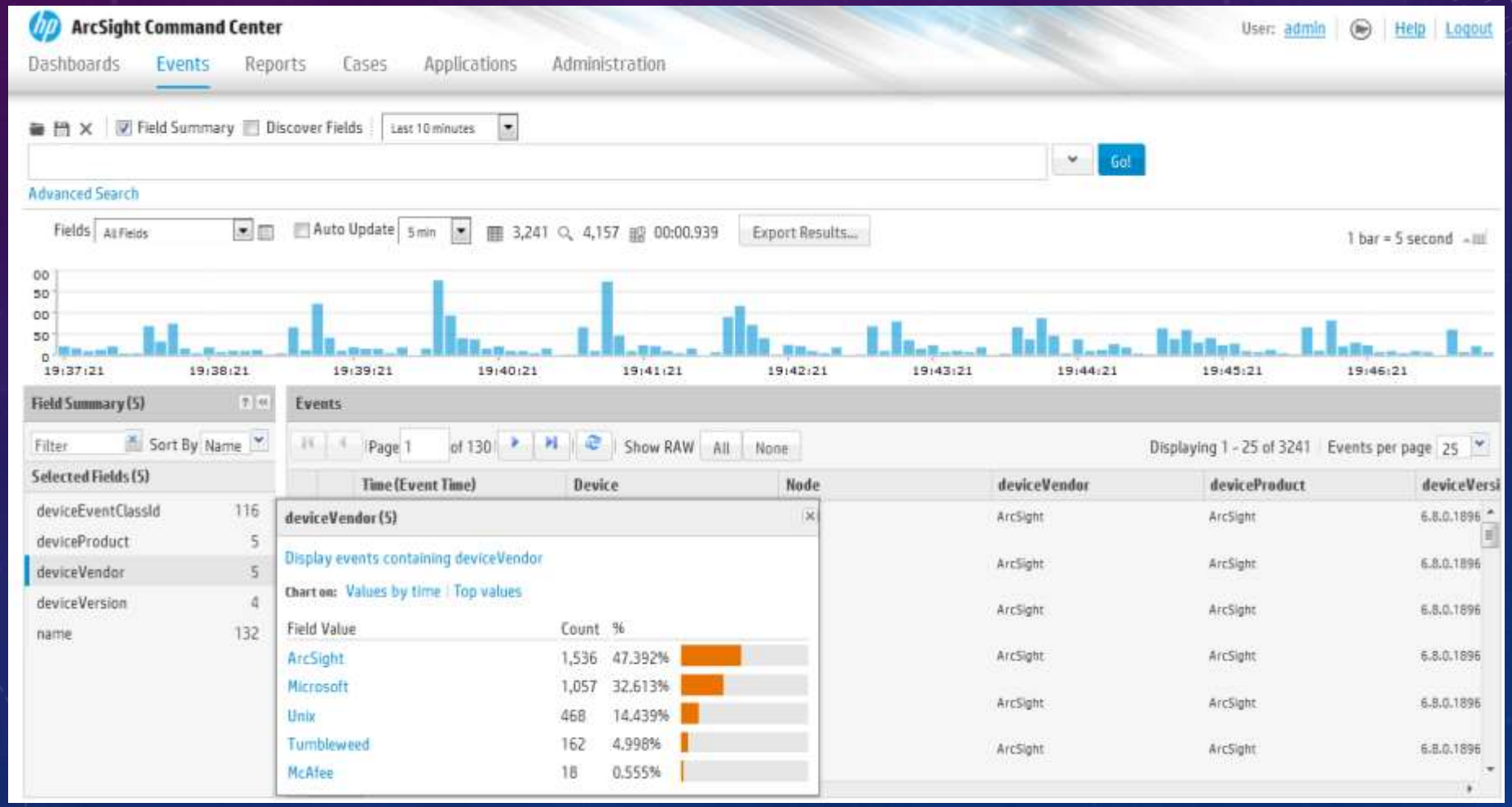


SIEM ÖZELLİKLERİ

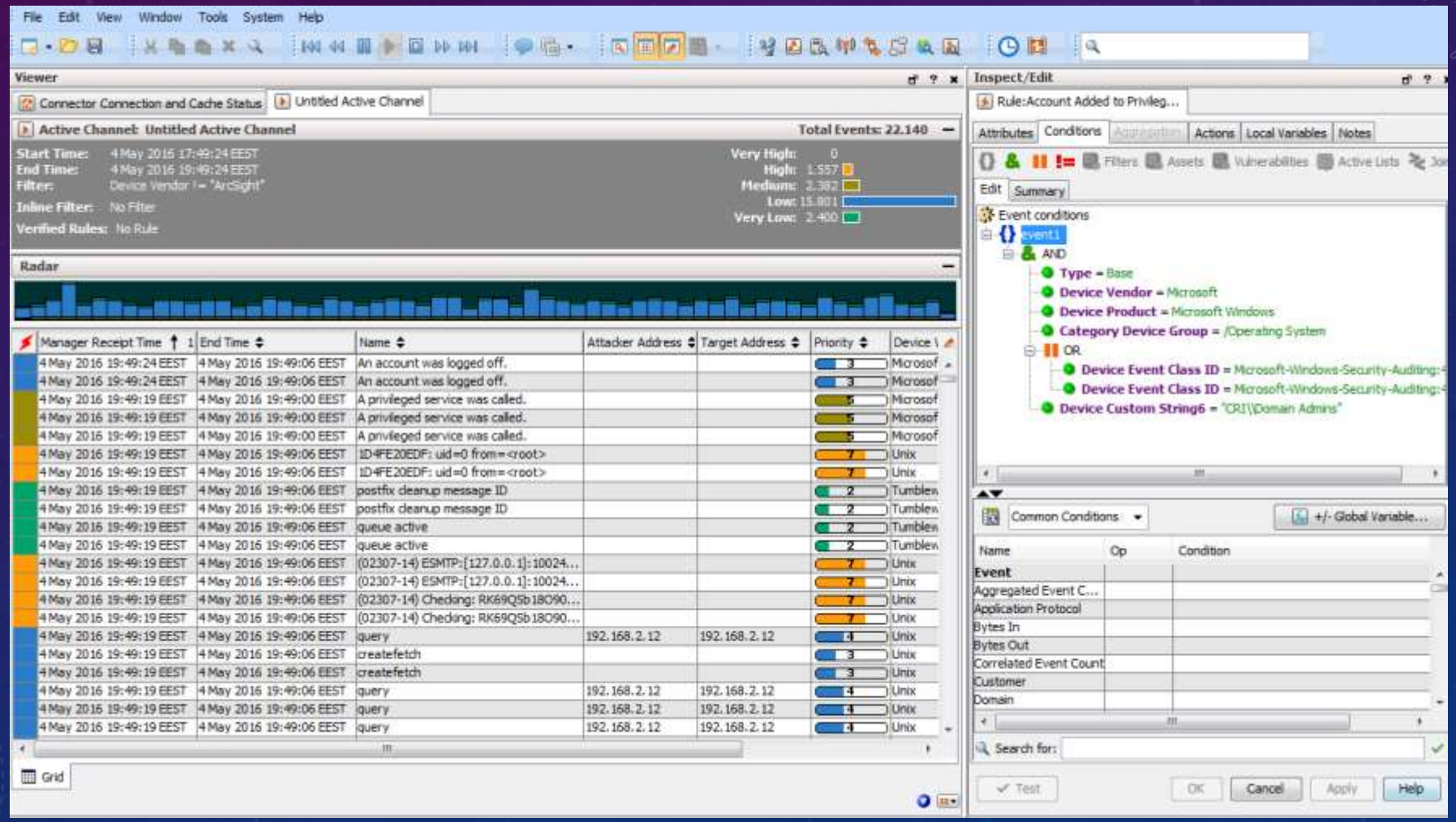
İŞLEYİŞ/SÜREÇ

HP ARCSIGHT COMMAND CENTER

HP ARCSIGHT COMMAND CENTER



HP ARCSIGHT CONSOLE



ARCSIGHT LOG ENTEGRASYONU

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

IBM QRADAR

IBM QRadar Security Intelligence

admin ▼ Help ▼ Messages 2 ▼ IBM

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

System Time: 19:42

Show Dashboard: Threat and Security Monitoring | New Dashboard | Rename Dashboard | Delete Dashboard | Add Item... ▼

Refresh Paused: 00:01:00

Default-IDS / IPS-All: Top Alarm Signatures (Event Count)

Reset Zoom 4.05.2016 13:41 - 4.05.2016 19:41

Event Count (Sum): 15, 10, 5, 0

15:00 17:00 19:00

▼ Legend

- MALWARE: Heap Manipulation Detected by Flash Analysis Engine
- HTTP: Microsoft Graphics Component Could Allow Remote Code Execution
- HTTP: Microsoft Windows Mount Point Privilege Escalation Vulnerability (CVE-20...

View in Log Activity

Top Systems Attacked (Event Count)

Reset Zoom 4.05.2016 13:41 - 4.05.2016 19:41

Count (Sum): 15, 10

My Offenses

No results were returned for this item.

Most Severe Offenses

Offense Name	Magnitude
Web Attack: MS IE Object Type CVE-2003-0344 preceded by Web Attack: Microsoft OleAut32 RCE CVE-2014-6332 2 preceded by Web Attack: Microsoft OleAut32 RCE CVE-2014-6332	
Multiple Exploit/Malware Types Targeting a Single Source	
Device Stopped Sending Events (Firewall IPS VPN or Switch)	
Device Stopped Sending Events (Firewall IPS VPN or Switch)	
Multiple Exploit/Malware Types Targeting a Single Source	

Most Recent Offenses

Offense Name	Magnitude
Device Stopped Sending Events (Firewall IPS VPN or Switch)	
Multiple Exploit/Malware Types Targeting a Single Source	
Device Stopped Sending Events (Firewall IPS VPN or Switch)	
Device Stopped Sending Events (Firewall IPS VPN	

Top Category Types

Category	Offenses
Misc Exploit	4
Buffer Overflow	4
Potential Web Vulnerability	3
Memory Corruption	3
Remote Access Exploit	3

Top Sources

Source	Offenses
192.168.3.5	13
192.168.1.153	10
192.168.2.19	6
192.168.2.16	5
208.94.116.21	3

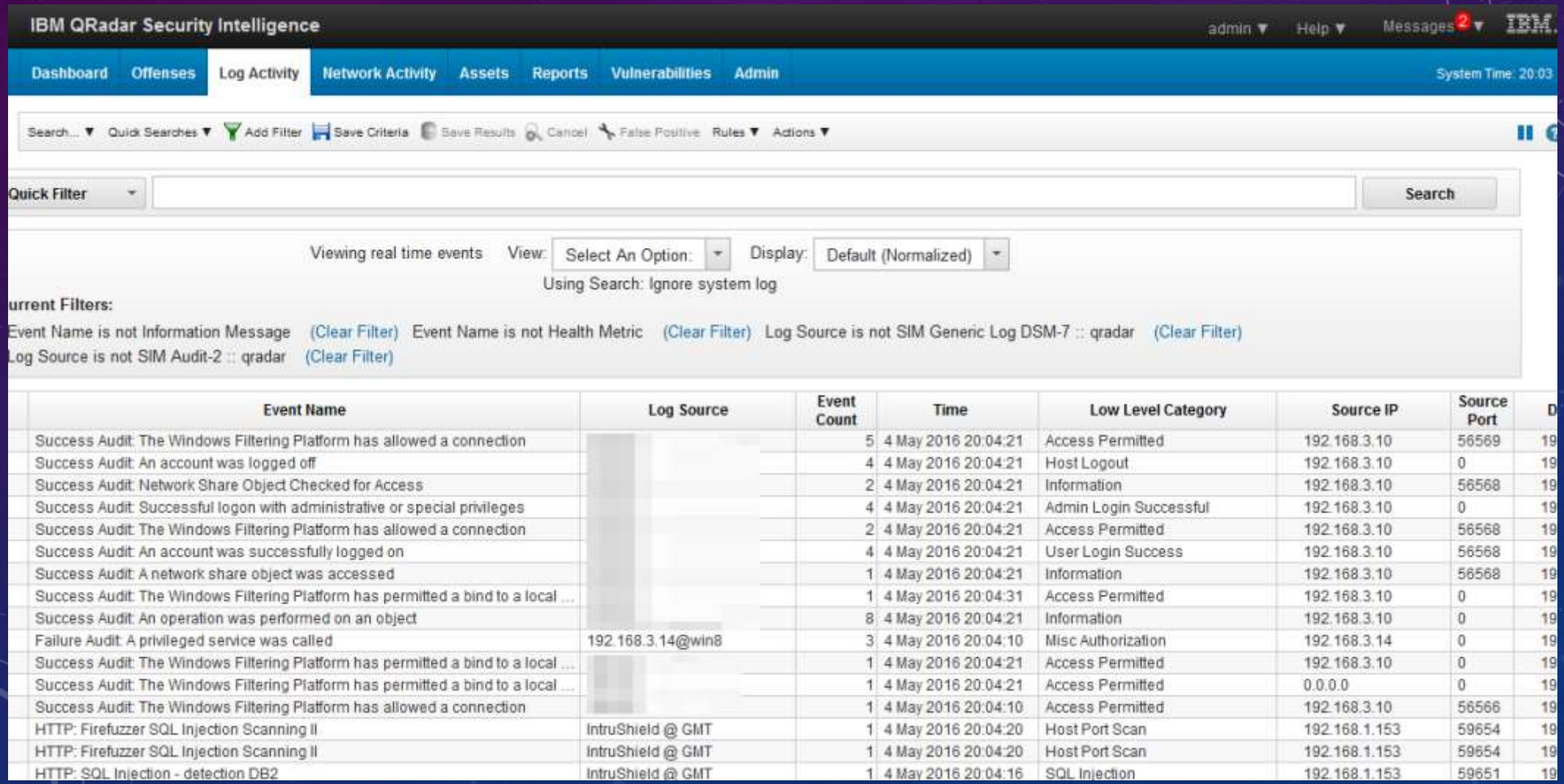
Top Local Destinations

Destination	Offenses
192.168.3.5	16
192.168.2.153	9
192.168.2.19	8
192.168.1.100	4
192.168.3.12	3

Flow Bias

QRadar

IBM QRADAR LOG AKTİVİTESİ



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

My Offenses

All Offenses

By Category

By Source IP

By Destination IP

By Network

Rules

Search... ▼ Save Criteria Actions ▼ Print

Last Refresh: 00:00:05

All Offenses View Offenses: Select An Option:

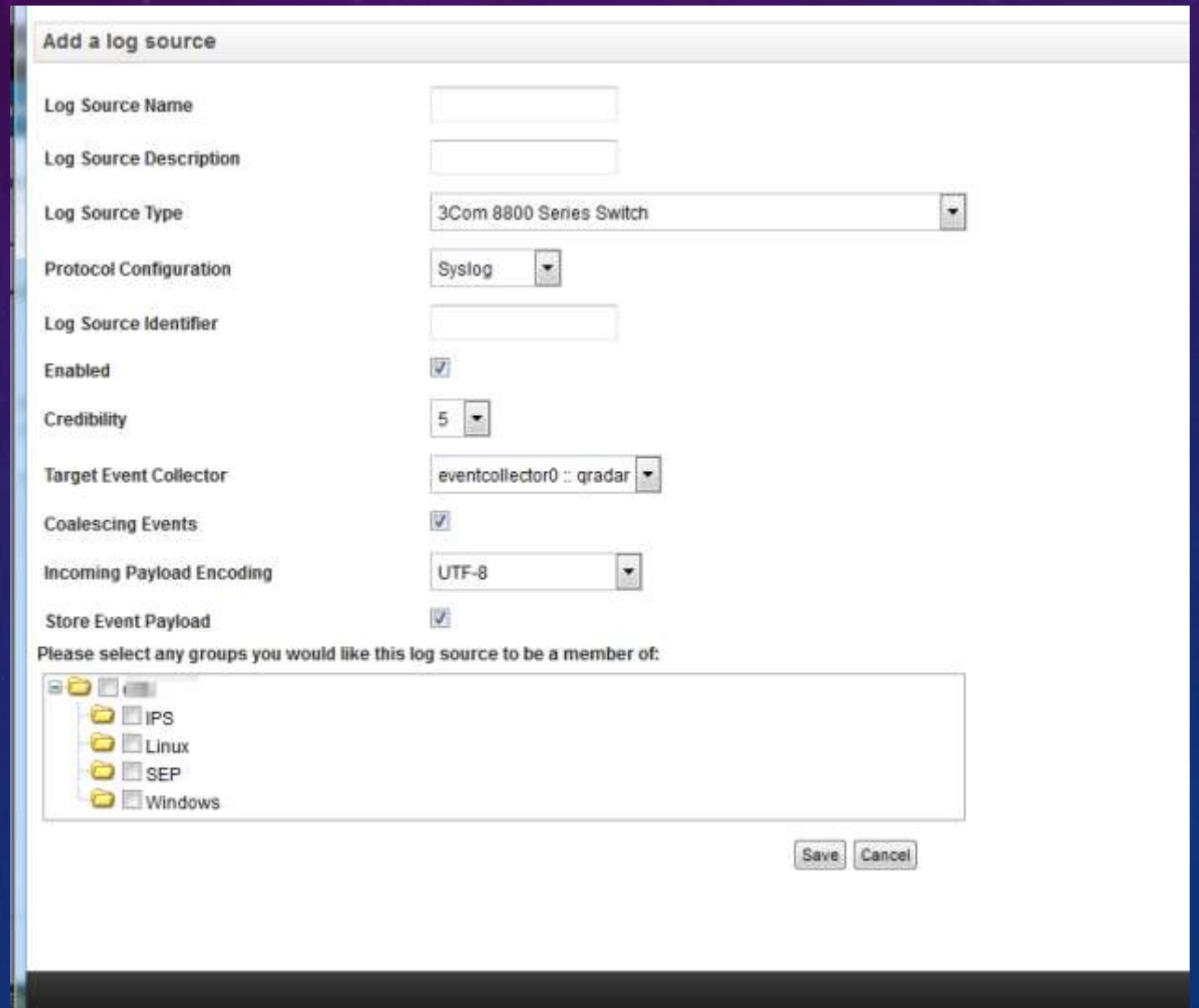
urrent Search Parameters:

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

IBM QRADAR LOG ENTEGRASYONU

- Log Sources



ETKİN LOG KORELASYONU

Attributes | Conditions | Aggregation | Actions | Local Variables | Notes

Filters | Assets | Vulnerabilities | Active Lists | Joins

Edit | Summary

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

Common Conditions Editor

Name	Op	Condition
Event		
Aggregated Event C...		

Search for:

Test

Rule Wizard

Rule Wizard: Rule Test Stack Editor

Which tests do you wish to perform on incoming events?

Test Group All — Export as Building Block

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)

<< Back | Next >> | Finish | Cancel

SIEM VE TEHDİT İSTİHBARATI

- Command and Controller Tespiti
- Malicious Connections
- Email Pattern

TEŞEKKÜRLER

???