SIEM USE CASEs configuration and compliance document

Baselining the systems against SOC operational requirements

IS Ops team / 14-feb-2021

Table of Contents

Document Information

Document Title	**Incident Response Policy**
Drafted by	IS Operations team
Draft Date	Jan 5, 2013
Owner	
Classification/ Classification Authority	Internal /
Release Version	1.1
Reference document	SOC implementation plan
Approval Date	
Approved By	
Published Date	

1. Background

The purpose of this document is to illustrate assets owners the underlying procedural requirements and configurations necessary to operate and sustain SOC operations. The understanding of these requirements by owners is critically important in determining the success of SOC operations, In case of any change resulting due to improper configuration or management of these requirements can directly impact the performance of SOC operations team in timely detection and response to security incidents.

2. Scope

The scope of this exercise stretches within the bounds of use-cases requirements mentioned in the SOC implementation plan referenced above (Document Information).

3. Responsibility

3.1. SOC team

The team is responsible for:-

- Maintaining an auditable trail to prove events of interest were followed up on and resolved.
- Active monitoring of controls

3.2. GRC Team

The team is responsible to update, maintain policies for relevancy and to reflect the configuration requirements herein mentioned.

3.3. Internal Audit

The audit is responsible for:-

- Reviewing the internal controls, periodically or as mentioned in annual audit plan or as directed by the regulator, implemented by senior management.
- Internal auditors will evaluate and review the internal controls in place and report for its improvements.

- To ensure that SOPs are followed by concerned department and grey areas, if any, are identified with recommendations how to counter the same.

3.4. Systems / Control owners

The owners are responsible for:-

- Introducing internal Controls through SOPs which are prepared in consultation with respective departmental heads, reviewed and approved by management for implementing the same.
- Configuration and management of audit rules as per policies (e.g Change and configuration management policy).

3.5. Management

The management is responsible for:-

- Establishing a mechanism to update the audit procedures.
- Establishing a periodic review of audit activities and to adjust those audit activities to better support the ’s business goals.

4. Use-Case definition and Attributes

4.1. Section ID: Network

4.1.1. Sub Section ID: Inside Attack

4.1.1.1. Reference ID: 1.2.1.1.

4.1.1.1.1. Goal

Under this use-case the SOC operations team would be detecting a new VPN connection

4.1.1.1.2. Sources

Aggregate firewall

4.1.1.1.3. Requirements

a. Enable syslog on cisco asa 5825. [1]

```
logging host interface_name syslog_ip
```

```
logging trap {severity_level | message_list}
```

b. Filtering syslog messages for VPN session establishment.

4.1.1.1.4. Audit to Event-id Mapping

N/A

4.1.1.1.5. Troubleshooting steps

N/A

4.1.1.1.6. Dependency

N/A

4.1.1.1.7. Limitations

N/A

4.1.1.1.8. Affected Area

- All VPN aggregation firewalls.

4.1.1.1.9. References

[1]http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/monitor_syslog.html#wp1552182

[2] http://www.confighelper.com/2009/07/how-to-check-cisco-asa-vpn-activity-using-syslog.html

4.1.1.2. Reference ID: 1.2.1.2

4.1.1.2.1. Goal

Under this use-case the SOC operations team would be monitoring events for MAC flooding attack

4.1.1.2.2. Sources

AIP module firewall

4.1.1.2.3. Requirements

a. Enable syslog on same as reference id: 1.2.1.1
b. Filtering syslog messages for MAC flooding attempts. [1]

4.1.1.2.4. Audit to Event-id to mapping

Details 1

Product:	AIP module
Maps to	4.1.1.2.3
Event ID:	322001
Description	The adaptive security appliance received a packet from the offending MAC address on the specified interface, but the source MAC address in the packet is statically bound to another interface in the configuration. Either a MAC-spoofing attack or a misconfiguration may be the cause.

Details 2

Product:	AIP module
Maps to	4.1.1.2.3
Event ID:	322002
Description	If the ARP inspection module is enabled, it checks whether a new ARP entry advertised in the packet conforms to the statically configured or dynamically learned IP-MAC address binding before forwarding ARP packets across the adaptive security appliance. If this check fails, the ARP inspection module drops the ARP packet and

	generates this message. This situation may be caused by either ARP spoofing attacks in the network or an invalid configuration (IP-MAC binding).

4.1.1.2.5. Troubleshooting steps

N/A

4.1.1.2.6. Dependency

N/A

4.1.1.2.7. Limitations

N/A

4.1.1.2.8. Affected Area

- All vlans.

4.1.1.2.9. References

[1]http://www.cisco.com/en/US/docs/security/asa/asa83/system/message/logmsgs.html

4.1.1.3. Reference ID: 1.2.1.3

4.1.1.3.1. Goal

Under this use-case the SOC operations team would be monitoring events for scanning attempt made by intruder / attacker

4.1.1.3.2. Sources

AIP module

4.1.1.3.3. Requirements

a. Enable syslog on same as reference id: 1.2.1.1
b. Filtering syslog messages for scanning. [1]

4.1.1.3.4. Audit to Event-id to mapping

Details 1

Product:	AIP module
Maps to	4.1.1.2.3
Event ID:	733101
Description	The adaptive security appliance detected that a specific host (or several hosts in the same 1024-node subnet) is either scanning the network (attacking), or is being scanned (targeted)

4.1.1.3.5. Troubleshooting Steps

N/A

4.1.1.3.6. Dependency

N/A

4.1.1.3.7. Limitations

N/A

4.1.1.3.8. Affected Area

Against Windows critical servers

Against unix critical servers

Against critical network devices

4.1.1.3.9. References

[1]http://www.cisco.com/en/US/docs/security/asa/asa83/system/message/logmsgs.html#wp4771499

4.1.1.4. Reference ID: 1.2.1.4

4.1.1.4.1. Goal

Under this use-case the SOC operations team would be monitoring events for DHCP starvation attack

4.1.1.4.2. Sources

Nexsus 7018, Juniper IDP

4.1.1.4.3. Requirements

a. Configure Nexsus to enable DHCP snooping feature to prevent rogue DHCP and starvation attacks
b. Configure syslog protocol to send DHCP snooping events.[1]

4.1.1.4.4. Audit to Event-id to mapping

N/A

4.1.1.4.5. Troubleshooting Steps

N/A

4.1.1.4.6. Dependency

N/A

4.1.1.4.7. Limitations

1. The SOC team relies on properly configured and secure NEXSUS switch to enable necessary protection (e.g DHCP snooping).

4.1.1.4.8. Affected Area

Active directory.

4.1.1.4.9. References

[1]http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/chap8.html#wp1060946

4.1.1.5. Reference ID: 1.2.1.5

4.1.1.5.1. Goal

Under this use-case the SOC operations team would be monitoring rogue AP's.

4.1.1.5.2. Sources

CISCO MSE

4.1.1.5.3. Requirements

1. Configure Remote Syslog Server to publish MSE logs [1]
    a. Use this option to configure a Remote Syslog Server by specifying the IP address, priority parameter, priority level, and facility.
    b. A Remote Syslog Server has not been configured for this machine.
    c. Configure Remote Syslog Server Configuration parameters? (Y)es/(S)kip/(U)se default
    d. [Skip]: y
    e. Configure Remote Syslog Server IP address
    f. Configure Remote Syslog Server Priority parameter.
    g. select a priority level
    h. Configure Remote Syslog Server's Facility parameter.
    i. Select a logging facility

4.1.1.5.4. Audit to Event-id to mapping

N/A

4.1.1.5.5. Troubleshooting Steps

N/A

4.1.1.5.6. Dependency

N/A

4.1.1.5.7. Limitations

N/A

4.1.1.5.8. Affected Area

All wifi-users / SSIDs

4.1.1.5.9. References

[1]http://www.cisco.com/en/US/docs/wireless/mse/3350/7.0MR1/CAS/configuration/guide/msecg71_appA_Hardening.html#wp1275151

4.1.1.6. Reference ID: 1.2.1.6

4.1.1.6.1. Goal

Under this use-case the SOC operations team would be monitoring when a new VPN site has been cause of worm propagation to other networks.

4.1.1.6.2. Sources

CISCO IDP logs, Symantec End-point

4.1.1.6.3. Requirements

a. Enabling steps

1. Configure the CISCO ASA firewall IDP module to send syslog to Q1 radar appliance.
2. Configure the Symantec end-point server to do the same.

4.1.1.6.4. Audit to event-Id mapping

N/A

4.1.1.6.5. Troubleshooting

N/A

4.1.1.6.6. Dependency

Reference number 1.1.2.1 & Reference number 1.2.1.1

4.1.1.6.7. Limitations

N/A

4.1.1.6.8. Affected Area

ALL Vlans.

4.1.1.6.9. References

N/A

4.1.1.7. Reference ID: 1.2.1.7

4.1.1.7.1. Goal

Under this use-case the SOC operations team would be monitoring If X number of attempts have seen accessing FTP server using default credentials.

4.1.1.7.2. Sources

CISCO IDP logs

4.1.1.7.3. Requirements

a. Enabling steps

1. Configure the CISCO IDP to send brute-force event messages via syslog.
2. Configuring OSSEC agent to alert on ftp brute force attempts. [1]

4.1.1.7.4. Audit to Event-ID mapping

N/A

4.1.1.7.5. Troubleshooting steps

N/A

4.1.1.7.6. Limitations

Access to Nessus server is unavailable.

4.1.1.7.7. Dependencies

N/A

4.1.1.7.8. Affected Area

FTP server farm

4.1.1.7.9. References

[1]www.ossec.net/doc/rules/rules/50_ms_ftpd_rules.xml.html+&cd=1&hl=en&ct=clnk&gl=pk&client=firefox-a

4.1.2. **Sub-section ID: External attacks**

4.1.2.1. Reference ID: 1.2.2.1

4.1.2.1.1. Goal

Under this use-case the SOC operations team would be monitoring for fragmented ICMP traffic entering or leaving the network.

4.1.2.1.2. Sources

CISCO IDP logs

4.1.2.1.3. Requirements

1. Configure the CISCO IDP to send fragmented traffic event messages via syslog.

4.1.2.1.4. Audit to Event-ID mapping

Details 1 [1]

Produc	AIP module

t:	
Maps to	4.1.1.2.3
Signature ID	1100
Message Number	400007
Signature Title	IP Fragment Attack
Signature Type	Attack
Description	Triggers when any IP datagram is received with an offset value less than 5 but greater than 0 indicated in the offset field.

Details 2

Product:	AIP module
Maps to	4.1.1.2.3
Signature ID	1100
Message Number	400009
Signature Title	IP Overlapping Fragments (Teardrop)
Signature Type	Attack

Description	Triggers when two fragments contained within the same IP datagram have offsets that indicate that they share positioning within the datagram. This could mean that fragment A is being completely overwritten by fragment B, or that fragment A is partially being overwritten by fragment B. Some operating systems do not properly handle fragments that overlap in this manner and may throw exceptions or behave in other undesirable ways upon receipt of overlapping fragments, which is how the Teardrop attack works to create a DoS.

4.1.2.1.5. Troubleshooting steps

N/A

4.1.2.1.6. Dependency

N/A

4.1.2.1.7. Limitations

N/A

4.1.2.1.8. Affected Area

All Vlans

4.1.2.1.9. References

[1]http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/protect_tools.html

4.1.2.2. Reference ID: 1.2.2.2

4.1.2.2.1. Goal

Under this use-case the SOC operations team would be monitoring for ping sweep events.

4.1.2.2.2. Sources

CISCO ASA 5585

4.1.2.2.3. Requirements

1. Configure the CISCO IDP to send ping sweep event messages via syslog.

4.1.2.2.4. Audit to Event-ID mapping

N/A

4.1.2.2.5. Troubleshooting

N/A

4.1.2.2.6. Dependency

N/A

4.1.2.2.7. Affected Area

All Vlans

4.1.2.2.8. Limitations

1. Syslog traffic is being blocked or filtered by network and proxies.
2. The recent patch has broken down the functionality of the syslog agent.
3. If the admin exclude his / her account from auditing.

4.1.2.2.9. References

[1]http://www.cisco.com/en/US/docs/security/asa/asa84/system/message/logmsgs.html#wp4769400

4.1.2.3. Reference ID: 1.2.2.3

4.1.2.3.1. Goal

Under this use-case the SOC operations team would be monitoring for operating system fingerprinting event.

4.1.2.3.2. Sources

CISCO IDP logs

4.1.2.3.3. Requirements

1. Configure the CISCO IDP to send events logs related to signature mentioned in section 4.1.2.3.4

4.1.2.3.4. Audit to Event-ID mapping

Details 1 [1]

Product:	AIP module	
Maps to	4.1.2.3	
Signature ID	Signature Pack	Comments
3046/0	S3	This signature looks for a unique combination of TCP packets that the NMAP tool uses to fingerprint a remote operating system.
Signature Title	OS fingerprinting	
Signature Type	Attack	

4.1.2.3.5. Troubleshooting

N/A

4.1.2.3.6. Dependency

N/A

4.1.2.3.7. Limitations

1. Syslog traffic is being blocked or filtered by network and proxies.

2. The recent patch has broken down the functionality of the syslog agent.
3. If the admin exclude his / her account from auditing.

4.1.2.3.8. Affected Area

Unix and windows critical servers

4.1.2.3.9. References

[1]http://www.cisco.com/en/US/docs/security/asa/asa84/system/message/logmsgs.html#wp4769400

4.1.2.4. Reference ID: 1.2.2.4

4.1.2.4.1. Goal

Under this use-case the SOC operations team would be monitoring for XSS attack.

4.1.2.4.2. Sources

CISCO IDP logs

4.1.2.4.3. Requirements

1. Configure the CISCO IDP to have updated set of cross site IPS signatures.[1]

4.1.2.4.4. Auditing to Event-ID Mapping

N/A

4.1.2.4.5. Troubleshooting

N/A

4.1.2.4.6. Dependency

N/A

4.1.2.4.7. Limitations

1. Syslog traffic is being blocked or filtered by network and proxies.
2. The recent patch has broken down the functionality of the syslog agent.
3. If the admin exclude his / her account from auditing.

4.1.2.4.8. Affected Area

All effected critical web-applications

4.1.2.4.9. References

[1] http://tools.cisco.com/security/center/Search.x

4.1.2.5. Reference ID: 1.2.2.5

4.1.2.5.1. Goal

Under this use-case the SOC operations team would be monitoring for SQL injection attacks.

4.1.2.5.2. Sources

CISCO IDP logs

4.1.2.5.3. Requirements

1. Configure the CISCO IDP to send XSS attacks events messages in response to section 4.1.2.5.4

4.1.2.5.4. Auditing to Event-ID Mapping

Details 1 [1]

Product:	AIP module	
Maps to	4.1.2.5	
Signature ID	Signature Pack	Comments

	3732.0	S44	Detects usage of a Microsoft SQL server stored procedure that is used to execute operating system commands
	5337.0	S47	Detects usage of the Microsoft SQL Server *xp_cmdshell* in the arguments of an HTTP request
	5474.0 5474.1	S294	Detects the presence of encoded words that are indicative of SQL injection attacks
	5930.0 through 5930.5	S349	Detects SQL keywords in HTTP arguments
Signature Title	SQL INJECTION		
Signature Type	Attack		

4.1.2.5.5. Troubleshooting steps

N/A

4.1.2.5.6. Dependency

N/A

4.1.2.5.7. Limitations

N/A

4.1.2.5.8. Affected Area

Critical servers

4.1.2.5.9. References

[1] http://www.cisco.com/web/about/security/intelligence/sql_injection.html#11

4.1.3. **Sub-section ID: Visibility**

4.1.3.1. Reference ID: 1.2.3.1

4.1.3.1.1. Goal

The use case will allow the SOC team to monitor when a new port is allowed on either inbound or outbound

4.1.3.1.2. Sources

Cisco ASA Firewall

4.1.3.1.3. Requirements

1. Login into the Cisco ASA firewall through console or SSH
2. Turn on infrastructure device management access logging by running the following command

```
Logging enable

Logging timestamp
logging host admin <SIEM IP>
```

3. Configure an offensive rule in the SIEM appliance when the following type of data is observed in the firewall logs:

```
access-list <name> extended allow <protocol>
<source-network/source IP> <source-netmask>
<destination-network/destination IP> <destinamtion-
netmask> eq <port number>
```

4.1.3.1.4. Auditing to Event-ID Mapping

Details

Product:	Cisco ASA Firewall 5585
Maps to	1.2.3.1
Event ID:	

Event Category	Syslog
Event Type	Syslog log data
Source:	ASA firewall syslog data
Description	This rule is generated when a user open a new port for either direction (inbound/outbound) on the firewall.

4.1.3.1.5. Troubleshooting

1. Make sure UPD 512 port is allowed between Cisco ASA firewall and SIEM

4.1.3.1.6. Dependency

Cisco ASA firewall syslog data

4.1.3.1.7. Limitations

N/A

4.1.3.1.8. Affected Area

Critical firewalls

4.1.3.1.9. References

1. http://www.security-solutions.co.za/cisco-asa-firewall-hardening-cisco-asa-best-practices.html
2. http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a0080862017.shtml

4.1.3.2. Reference ID: 1.2.3.2

4.1.3.2.1. Goal

This use case allows the SOC team to monitor when FTP server is accessed from unauthorized VLAN or network.

4.1.3.2.2. Sources

Cisco ASA Firewall

4.1.3.2.3. Requirements

1. Login into the Cisco ASA firewall through console or SSH
2. Turn on syslog messages on the Cisco ASA firewall through the following commands:

```
    Logging enable

    Logging timestamp
    logging host admin <SIEM IP>
```

3. Configure an offensive rule in the SIEM appliance when the following type of data is observed in the firewall logs:

```
%ASA-4-106100: access-list acl_ID {permitted | denied
| est-allowed} protocol
interface_name/source_address(source_port)(idfw_user,
sg_info) interface_name/dest_address(dest_port)
(idfw_user, sg_info) hit-cnt number ({first hit | number-
second interval})
```

4. Configure an offensive rule based on the source_address field to generate an alert when the server is accessed from a non-trusted source_address (source_adddress!=trusted address)

4.1.3.2.4. Auditing to Event-ID Mapping

Details

Product:	Cisco ASA Firewall 5585
Maps to	1.2.3.4
Event ID:	106100
Event Category	Syslog
Event Type	Syslog log data
Source:	ASA firewall syslog data
Description	This event is generated when the ASA firewall either permit or deny traffic based upon its

access rule.

4.1.3.2.5. Troubleshooting

Make sure UPD 512 port is allowed between Cisco ASA firewall and SIEM

4.1.3.2.6. Dependency

Cisco ASA firewall syslog data

4.1.3.2.7. Limitations

N/A

4.1.3.2.8. Affected Area

FTP servers farm

4.1.3.2.9. References

1. http://www.cisco.com/en/US/docs/security/asa/asa83/system/message/logmsgs.html#wp4769049
2. http://www.cisco.com/en/US/docs/security/asa/asa90/system/message/logsevp.html

4.1.3.3. Reference ID: 1.2.3.3

4.1.3.3.1. Goal

The use case will allow the SOC team to monitor any sensitive data transferred over the ’s network.

4.1.3.3.2. Sources

QFlow

4.1.3.3.3. Requirements

1. On the QRadar SIEM, select the Offences tab and select the Flow option

2. Create a new Flow rule and select the Source Payload option. This option specifies any payload content found in the source payload. Specify all the sensitive keywords we want to detect.
3. Note the QID of the event specified in the QID field.
4. Once the flow policy is configured look for the events associated with those QIDs.

4.1.3.3.4. Auditing to Event-ID Mapping

Details

Product:	QFlow Appliance
Maps to	1.2.3.5
Event ID:	
Event Category	Flow Rule
Event Type	Source Payload
Source:	QFlow Flow Rule
Description	This event is generated when a source payload in a packet contain the keyword we specified in the rule.

4.1.3.3.5. Troubleshooting

1. Make sure the QFlow appliance is getting all the traffic. This is done through either installing the QFlow appliance inline or through port mirroring.
2. Run TCPDUMP on the QFlow appliance to ensure the traffic is received there successfully
3. Make sure QFlow successfully forwards the data to the QRadar SIEM appliance.

4.1.3.3.6. Dependency

Network traffic, sensitive keywords classifications

4.1.3.3.7. Limitations

1. QFlow Appliance needs to be installed inline
2. All sensitive keywords must be defined prior to implement this rule

4.1.3.3.8. Affected Area

Critical servers

4.1.3.3.9. References

QRadar User Guide Chapter 5 – Investigating Flows

4.1.3.4. Reference ID: 1.2.3.4

4.1.3.4.1. Goal

This use case allows the SOC team to monitor and detect tunneled traffic.

4.1.3.4.2. Sources

QFlow

4.1.3.4.3. Requirements

1. On the QRadar SIEM, select the Offences tab and select the Flow option
2. Create a new Flow rule and select the Protocol option and choose the protocol for which we want to configure the rule. For example, if we want to detect FTP data tunneled over HTTP, select HTTP in this step.
3. Choose the Custom Rule option to create a custom rule for the flow.
4. Select the Payload option and generate an offense when payload is not equal to protocol.

4.1.3.4.4. Auditing to Event-ID Mapping

Details 1

Product:	QFlow Appliance
Maps to	1.2.3.6
Event ID:	
Event Category	Flow Rule
Event Type	Protocol
Source:	QFlow Flow Rule
Description	This event is generated when payload of a packet doesn’t correspond to the protocol specified in the Protocol field.

4.1.3.4.5. Troubleshooting

1. Make sure the QFlow appliance is getting all the traffic. This is done through either installing the QFlow appliance inline or through port mirroring.
2. Run TCPDUMP on the QFlow appliance to ensure the traffic is received there successfully
3. Make sure QFlow successfully forwards the data to the QRadar SIEM appliance.

4.1.3.4.6. Dependency

Network traffic

4.1.3.4.7. Limitations

QFlow Appliance needs to be installed inline or configured through port mirroring

4.1.3.4.8. Affected Area

Across all vlans

4.1.3.4.9. References

QRadar User Guide Chapter 5 – Investigating Flows

4.1.3.5. Reference ID: 1.2.3.5

4.1.3.5.1. Goal

This use case allow the SOC team to monitor when a new user is created on the Juniper / Cisco ASA firewall

4.1.3.5.2. Sources

Cisco ASA Firewall AND Juniper

4.1.3.5.3. Requirements

1. Login into the Cisco ASA firewall through console or SSH
2. Turn on infrastructure device management access logging by running the following command

```
Logging enable

Logging timestamp
logging host admin <SIEM IP>
```

3. Configure an offensive rule in the SIEM appliance when the following type of data is observed in the firewall logs:

```
%ASA-5-502101: New user added to local dbase:
Uname: user Priv: privilege_level Encpass: string
```

4.1.3.5.4. Auditing to Event-ID Mapping

Details

Product:	Cisco ASA Firewall 5585
Maps to	1.2.3.7
Event ID:	502101
Event Category	Syslog
Event	Syslog log data

Type	
Source:	ASA firewall syslog data
Description	This rule is generated when a new user account is created on the ASA firewall

4.1.3.5.5. Troubleshooting

Make sure UPD 512 port is allowed between Cisco ASA firewall and SIEM

4.1.3.5.6. Dependency

Cisco ASA firewall syslog data

4.1.3.5.7. Affected Area

Critical servers

4.1.3.5.8. Limitations

N/A

4.1.3.5.9. References

1. http://www.cisco.com/en/US/docs/security/asa/asa83/system/message/logmsgs.html#wp4773963

4.1.3.6. Reference ID: 1.2.3.6

4.1.3.6.1. Goal

This use case will allow the SOC team to monitor when data is uploaded to the Internet in RAR archive chunks.

4.1.3.6.2. Sources

QFlow

4.1.3.6.3. Requirements

1. On the QRadar SIEM, select the Offences tab and select the Flow option

2. Create a new Flow rule and select the Source Payload option. This option specifies any payload content found in the source payload. Specify all the sensitive keywords we want to detect.
3. Select the Custom Rule option and configure a custom rule when the Source Payload contain “RAR!...” payload
4. Select the Source Byte greater than 20 MB.
5. Note the QID of the event specified in the QID field.
6. Once the flow policy is configured look for the events associated with those QIDs.

4.1.3.6.4. Auditing to Event-ID Mapping

Details

Product:	QFlow Appliance
Maps to	1.2.3.8
Event ID:	
Event Category	Flow Rule
Event Type	Source Payload, Source Byte
Source:	QFlow Flow Rule
Description	This event is generated when the source payload contain the specified application data

4.1.3.6.5. Troubleshooting

1. Make sure the QFlow appliance is getting all the traffic. This is done through either installing the QFlow appliance inline or through port mirroring.
2. Run TCPDUMP on the QFlow appliance to ensure the traffic is received there successfully1Make sure QFlow successfully forwards the data to the QRadar SIEM appliance.

4.1.3.6.6. Dependency

N/A

4.1.3.6.7. Limitations

1. QFlow Appliance needs to be installed inline or configured through port mirror
2. The rule is going to trigger only when the source byte is greater than 20 MB. We assumed the email attachment size is 20 MB that is why the user is going to use the Internet upload option. If the source bytes are less than 20 MB (in other words if the uploaded data is less than 20 MB), the rule will not be triggered.

4.1.3.6.8. Affected Area

All vlans

4.1.3.6.9. References

QRadar User Guide Chapter 5 – Investigating Flows

4.1.3.7. Reference ID: 1.2.3.7

4.1.3.7.1. Goal

This use case will allow the SOC team to monitor when an online messenger is used to chat or transfer files.

4.1.3.7.2. Sources

QFlow

4.1.3.7.3. Requirements

1. On the QRadar SIEM, select the Offences tab and select the Flow option
2. Create a new Flow rule and select the Source Payload option. This option specifies any payload content found in the source payload. Specify all the sensitive keywords we want to detect.
3. Select the Custom Rule option and configure a custom rule when the Source Payload contain "IMP (instant message applications)..." payload

4.1.3.7.4. Auditing to Event-ID Mapping

N/A

4.1.3.7.5. Troubleshooting

1. Make sure the QFlow appliance is getting all the traffic. This is done through either installing the QFlow appliance inline or through port mirroring.
2. Run TCPDUMP on the QFlow appliance to ensure the traffic is received there successfully1Make sure QFlow successfully forwards the data to the QRadar SIEM appliance.

4.1.3.7.6. Dependency

N/A

4.1.3.7.7. Limitations

N/A

4.1.3.7.8. Affected Area

All vlans

4.1.3.7.9. References

[1] http://www.ndm.net/siem/pdf/q1labs/The-Value-of-QRadar-QFlow-and-QRadar-VFlow-for-Security-Intelligence.pdf

4.1.3.8. Reference ID: 1.2.3.8

4.1.3.8.1. Goal

This use case will allow the SOC team to monitor when malicious traffic hit the executive network

4.1.3.8.2. Sources

Cisco ASA 5585 Firewall AIP Module

4.1.3.8.3. Requirements

1. Login into the Cisco ASA firewall through console or SSH
2. Turn on infrastructure device management access logging by running the following command
3. Configure Cisco Intrusion Prevention Systems (forensics) DSM in the QRadar.
4. Configure an offensive rule based on the destination_address field to generate an alert when destination_address contain one of the IP address assigned to the executive subnet.
5. Step by step procedure of how to turn on packet inspection is given at http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00807335ca.shtml

4.1.3.8.4. Auditing to Event-ID Mapping

Details 1

Product:	Cisco ASA Firewall 5585
Maps to	1.2.3.4
Event ID:	106100
Event Category	Syslog
Event Type	Syslog log data
Source:	ASA firewall syslog data
Description	This event is generated when the ASA firewall either permit or deny traffic based upon its access rule.

4.1.3.8.5. Troubleshooting

Using the CISCO OIT (Output Interpreter Tool), issue the following “show” commands to troubleshoot. The following show commands are helpful in troubleshooting the problem:

a) Show module
b) Show run
c) Show access-list

Further troubleshooting details are available at References section.[3]

4.1.3.8.6. Dependency

Cisco ASA firewall syslog data

4.1.3.8.7. Limitations

N/A

4.1.3.8.8. Affected Area

All such secure vlans

4.1.3.8.9. References

1. http://www.cisco.com/en/US/docs/security/asa/asa83/system/message/logmsgs.html#wp4769049
2. http://www.cisco.com/en/US/docs/security/asa/asa90/system/message/logsevp.html
3. http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00807335ca.shtml

4.1.3.9. Reference ID: 1.2.3.9

4.1.3.9.1. Goal

This use case will enable SOC team to monitor the event when SIP phones receive telnet traffic.

4.1.3.9.2. Sources

Cisco ASA Firewall

4.1.3.9.3. Requirements

1. Login into the Cisco ASA firewall through console or SSH
2. Turn on syslog messages on the Cisco ASA firewall through the following commands:

```
Logging enable
Logging timestamp
logging host admin <SIEM IP>
```

3. Configure an offensive rule in the SIEM appliance when the following type of data is observed in the firewall logs:

```
%ASA-4-106100: access-list acl_ID {permitted | denied
| est-allowed} protocol
interface_name/source_address(source_port)(idfw_user,
sg_info) interface_name/dest_address(23) (idfw_user,
sg_info) hit-cnt number ({first hit | number-second
interval})
```

4. Configure an offensive rule based on the dest_address and dest_port fields to generate an alert when dest_address is one of the SIP phone IP addresses and destination port is 23 which is the default telnet port.

4.1.3.9.4. Auditing to Event-ID Mapping

Details 1

Product:	Cisco ASA Firewall 5585
Maps to	1.2.3.8
Event ID:	106100
Event Category	Syslog
Event Type	Syslog log data
Source:	ASA firewall syslog data
Description	This event is generated when the ASA firewall either permit or deny traffic based upon its access rule.

4.1.3.9.5. Troubleshooting

Make sure UPD 512 port is allowed between Cisco ASA firewall and SIEM

4.1.3.9.6. Dependency

Cisco ASA firewall syslog data

4.1.3.9.7. Limitations

N/A

4.1.3.9.8. Affected Area

All sip devices/ phones / servers

4.1.3.9.9. References

1. http://www.cisco.com/en/US/docs/security/asa/asa83/system/message/logmsgs.html#wp4769049
2. http://www.cisco.com/en/US/docs/security/asa/asa90/system/message/logsevp.html

4.1.3.10. Reference ID: 1.2.3.10

4.1.3.10.1. Goal

This use case will enable the SOC team when attempt is made to access adult contents from the ’s protected network.

4.1.3.10.2. Sources

Microsoft TMG Proxy

4.1.3.10.3. Requirements

1. Configure URL Filtering in the right pane of the ISA management console
2. Click on the Category Query and Select the Liability category. Pornography and adult contents are sub category of Liability
3. Check the Liability category and press OK
4. Install QRadar Adaptive Log Exporter (ALE) agent on the ISA proxy server

5. Open the ALE interface and select the ISA Server. In the RootLogDirectory field, enter C:\Windows\System32\LogFiles and press OK. ALE will gather the TMG Logs from the specified directory.
6. Create an offensive rule to fire when logs in the TMG proxy logs contain Category=Liability and Sub Category=Pornography

4.1.3.10.4. Auditing to Event-ID Mapping

Details 1

Product:	Cisco ASA Firewall 5585
Maps to	1.2.3.7
Event ID:	-
Event Category	Windows Logs
Event Type	QRadar Adaptive Log Exporter Logs
Source:	Microsoft TMG Proxy Server
Description	This event is generated when the Microsoft TMG Proxy block a pornographic URL request

4.1.3.10.5. Troubleshooting

1. Make sure the ALE agent is able to communicate with the QRadar SIEM and logs are successfully received at the QRadar SIEM console.
2. Verify that TMG is logging the events when URL is blocked based on some category.

4.1.3.10.6. Dependency

1. Logs are enabled and TMG Proxy
2. ALE transfer logs from the TMG Proxy to the QRadar SIEM

4.1.3.10.7. Limitations

N/A

4.1.3.10.8. Affected Area

All vlans effected

4.1.3.10.9. References

1. http://www.isaserver.org/tutorials/TMG-Back-Basics-Part8.html

4.1.3.11. Reference ID: 1.2.3.11

4.1.3.11.1. Goal

This use case will enable SOC team to monitor when someone perform port scan against the SIP ports 5060 and 5061.

4.1.3.11.2. Sources

Cisco ASA Firewall

4.1.3.11.3. Requirements

1. Login into the Cisco ASA firewall through console or SSH
2. Turn on syslog messages on the Cisco ASA firewall through the following commands:

```
Logging enable

Logging timestamp
logging host admin <SIEM IP>
```

3. Configure an offensive rule in the SIEM appliance when the following type of data is observed in the firewall logs:

```
%ASA-4-106100: access-list acl_ID {permitted | denied
| est-allowed} protocol
interface_name/source_address(source_port)(idfw_user,
sg_info) interface_name/dest_address(5060|5061)
(idfw_user, sg_info) hit-cnt number ({first hit | number-
second interval})
```

4. Configure an offensive rule based on the number of such events. A threshold of 5 can be set to fire the offensive rule when five connection attempts are detected in 1 second of time.

4.1.3.11.4. Auditing to Event-ID Mapping

Details 1

Product:	Cisco ASA Firewall 5585
Maps to	1.2.3.9
Event ID:	106100
Event Category	Syslog
Event Type	Syslog log data
Source:	ASA firewall syslog data
Description	This event is generated when the ASA firewall either permit or deny traffic based upon its access rule.

4.1.3.11.5. Troubleshooting

Make sure UPD 512 port is allowed between Cisco ASA firewall and SIEM

4.1.3.11.6. Dependency

Cisco ASA firewall syslog data

4.1.3.11.7. Limitations

N/A

4.1.3.11.8. Affected Area

All sip devices/ phones / servers

4.1.3.11.9. References

1. http://www.cisco.com/en/US/docs/security/asa/asa83/system/message/logmsgs.html#wp4769049
2. http://www.cisco.com/en/US/docs/security/asa/asa90/system/message/logsevp.html

4.1.4. **Sub-section ID: Policy violations**

4.1.4.1. Reference ID: 1.2.4.1

4.1.4.1.1. Goal

Under this use-case the SOC operations team would be monitoring for detecting bit-torrent traffic over network

4.1.4.1.2. Sources

Qflows device,CISCO IDP (ASA)

4.1.4.1.3. Requirements

1. Configure the cisco ASA device to send logs related to bit-torrent events.

4.1.4.1.4. Auditing to Event-ID Mapping

Details 1 [1]

Product:	AIP module
Maps to	4.1.3.1.3
Event ID:	11030/0
Description	BitTorrent is a P2P file sharing program designed to quickly disseminate files in a distributed fashion. This network is relying on the presence of trackers to synchronize the file status

4.1.4.1.5. Troubleshooting

Make sure UPD 512 port is allowed between **Cisco ASA firewall** and SIEM

4.1.4.1.6. Dependency

N/A

4.1.4.1.7. Limitations

1. CISCO asa events are cleared before being send to Qradar appliance (SIEM server)

4.1.4.1.8. Affected Area

All vlans

4.1.4.1.9. References

[1]http://tools.cisco.com/security/center/viewIpsSignature.x?signatureId=11030&signatureSubId=0

4.1.4.2. Reference ID: 1.2.4.2

4.1.4.2.1. Goal

Under this use-case the SOC operations team would be monitoring for firewall admin saves config file on an unauthorized machine.

4.1.4.2.2. Sources

CISCO IDP (ASA) and juniper

4.1.4.2.3. Requirements

CISCO ASA is configured to view events related to configuration action. To configure set the ASA to send logs related to message ID 111008 and 111010. The syslog number 111008 and 111010 will log the command that is entered by user.

4.1.4.2.4. Auditing to Event-ID Mapping

Details 1 [1]

Product:	ASA
Maps to	4.1.4.2
Event ID:	111008
Description	BitTorrent is a P2P file sharing program designed to quickly disseminate files in a distributed fashion. This network is relying on the presence of trackers to synchronize the file status

Details 2 [1]

Product:	ASA
Maps to	4.1.4.2
Event ID:	111010
Description	BitTorrent is a P2P file sharing program designed to quickly disseminate files in a distributed fashion. This network is relying on the presence of trackers to synchronize the file status

4.1.4.2.5. Troubleshooting

Make sure UPD 512 port is allowed between **Cisco ASA firewall** and SIEM

4.1.4.2.6. Dependency

N/A

4.1.4.2.7. Limitations

N/A

4.1.4.2.8. Affected Area

All such network devices

4.1.4.2.9. References

[1]www.cisco.com/en/US/docs/security/asa/asa84/system/message/logmsgs.html#wp4769410

4.1.5. **Sub-section ID: Operations**

4.1.5.1. Reference ID: 1.2.5.1

4.1.5.1.1. Goal

Under this use-case the SOC operations team would be monitoring for If X number of changes have been made on a firewall over x period of time by x user.

4.1.5.1.2. Sources

CISCO IDP (ASA)

4.1.5.1.3. Requirements

CISCO ASA is configured to view events related to configuration action. Events would be matched as follows:-

1. Time differences between most recent changes to firewall are alerted when exceeded beyond set limit.

Changes made in x time – Changes made in y time.

4.1.5.1.4. Auditing to Event-ID Mapping

Details 1 [1]

Product:	AIP module
Maps to	4.1.5.1
Event ID:	111008

Description	BitTorrent is a P2P file sharing program designed to quickly disseminate files in a distributed fashion. This network is relying on the presence of trackers to synchronize the file status

Details 2 [1]

Product:	AIP module
Maps to	4.1.5.1
Event ID:	111010
Description	BitTorrent is a P2P file sharing program designed to quickly disseminate files in a distributed fashion. This network is relying on the presence of trackers to synchronize the file status

4.1.5.1.5. Troubleshooting

N/A

4.1.5.1.6. Dependency

N/A

4.1.5.1.7. Limitations

N/A

4.1.5.1.8. Affected Area

All such network devices

4.1.5.1.9. References

[1]www.cisco.com/en/US/docs/security/asa/asa84/system/message/logmsgs.html#wp4769410

4.1.6. **Sub-section ID: Legal**

4.1.6.1. Reference ID: 1.2.6.1

4.1.6.1.1. Goal

Under this use-case the SOC operations team would be monitoring for If a disgruntled employee launches an attack to outside agency using network.

4.1.6.1.2. Sources

CISCO IDP (ASA)

4.1.6.1.3. Requirements

1. Login into the Cisco ASA firewall through console or SSH
2. Turn on infrastructure device management access logging by running the following command

```
Logging enable

Logging timestamp
logging host admin <SIEM IP>
```

3. Configure an offensive rule in the SIEM appliance when the following type of data is observed in the firewall logs:

```
access-list <name> extended allow <protocol>
<source-network/source IP> <source-netmask>
<destination-network/destination IP> <destinamtion-
netmask> eq <port number>
```

4.1.6.1.4. Auditing to Event-ID Mapping

Details 1 [1]

Product:	AIP module
Maps to	4.1.5.1
Event ID:	111008
Descri	BitTorrent is a P2P file sharing program

ption	designed to quickly disseminate files in a distributed fashion. This network is relying on the presence of trackers to synchronize the file status

Details 2 [1]

Product:	AIP module
Maps to	4.1.5.1
Event ID:	111010
Description	BitTorrent is a P2P file sharing program designed to quickly disseminate files in a distributed fashion. This network is relying on the presence of trackers to synchronize the file status

4.1.6.1.5. Troubleshooting

N/A

4.1.6.1.6. Dependency

N/A

4.1.6.1.7. Limitations

N/A

4.1.6.1.8. Affected Area

All such network devices

4.1.6.1.9. References

[1]www.cisco.com/en/US/docs/security/asa/asa84/system/message/logmsgs.html#wp4769410