Integrations Overview

Lumeta Spectre amplifies the value of your security stack by correlating the comprehensive and authoritative data about your network with integrated data connectors. The following table shows the Integrations available with Spectre along with their overview and how to verify their configurations. Integrations are available at Settings=>Integrations menu item.

Integrations	Description	Configuration Input	How to test if feed is accessible	Tables Populated	Dashboards /Reports
Open Source Feeds:					
Emerging Threats	http://rules.emergingthreats.net/blockrules/compromised-ips.txt provides you with a list of IPs that have been compromised. Spectre ingests this list and compares it to your discovered devices.	Polling Interval	Go to the emerging threats URL and verify that you can view the results	threat_feed_ip (_source: openthreat)	Breach Detection => Zombie Devices
Tor	Enabling Tor feed helps you find if any of your organization's trusted network assets are behaving as TOR relays or exit addresses. URLs that Spectre gets the TOR relays and exit addresses from are: https://onionoo.torproject.org/summary?type=relay https://check.torproject.org/exit-addresses	Polling Interval	Go to the TOR URLs and verify that you can view the results	tor	Breach Detection => Tor Nodes and Tor Flow Charting
ISC	https://isc.sans.edu/services.html provides Spectre with a list of ports that have been compromised. Spectre ingests this list and compares it against the open ports of your discovered devices.	Polling Interval	Go to ISC URL and verify that you can view the results	portlookup	Breach Detection => Nefarious Ports Summary
Subscription Feeds:					
Emerging Threats Pro	With a valid customer key, http://rules.emergingthreatspro.com provides Spectre with a list of IPs that have been compromised. Spectre ingests this list and compares it with your discovered devices.	Polling Interval Customer Key	Go to Emerging Threats Pro URL and verify that you can view the results	threat_feed_ip (_source: emergingthreat)	Breach Detection => Zombie Devices
iDefense	Verisign iDefense is a closed-source threat intelligence feed available to all Spectre customers. This feed correlates iDefense IPs against your network's IPs to produce actionable lists of zombie devices and threat flows in your network.	Polling Interval Customer Key	Go to https://api.intelgraph.verisign.com/rest/threatindicator/v0 and login with your username /password and verify that you can view the results	threat_feed_ip (_source: idefense)	Breach Detection => Threat Flow Charting
Other Solutions:					

Gigamon	Spectre uses NetFlow data to identify threat conversations between your network and external adversaries. This NetFlow data comes to Spectre as a result of its integration with a Gigamon solution.	Enable Netflow Packet Capture Service	Once you enable netflow, make sure nfcapd files are created under /var /spool /netflow directory. Gigamon (GigaSMART engine) can create only one type of record – either IPFIX, v9 or v5. We have tested Spectre with v9 only. As per our Development team, IPFIX is not supported.	Not tables under /var /spool /netflow directory, you will see nfcapd files	Breach Detection => Threat Flow Charting
Carbon Black	The integration of Carbon Black Endpoint Detection and Response capabilities to Spectre enables you to know whether hosts on your enterprise network are either unmanaged by Carbon Black, unmanaged by Spectre, or managed by both.	Polling Interval Customer Key Server Name	• Verify that you can login to your Carbon Black Server with your username and password • Verify that you have port 443 open • Verify that you have IPs in your network with CB sensor installed	managed_hosts_v (_source: bit9) bit9_managed_hosts_regex	Endpoint Management

McAfee	Lumeta Spectre fetches McAfee ePO-managed data, compares it to Spectre-discovered data within the same network space, and then pushes the findings back to the ePO server. This ensures on a continual basis that ePO has the complete set of networks and devices to manage.	Polling Interval Server Name Username Password	• Verify that you can login to your McAfee ePO Server with your username and password • Verify that you have port 443 open • Verify that you have IPs in your network licensed for McAfee	managed_hosts_v (_source: epo) epo_managed_hosts	ePO Management
Infoblox	This integration reconciles data between Spectre and Infoblox (an IP address management solution) and enables you to export an IP list with which to update the IP assets managed on Infoblox.	Polling Interval Server Name Username Password	• Verify that you can login to your Infoblox Server with your username and password • Verify that you have port 443 open • Verify that you have IPs in your network licensed for Infoblox	managed_hosts_v (_source: infoblox) infoblox_managed_hosts	IP Address Management

Cisco PxGrid	The Cisco pxGrid integration enables you to exchange context with Cisco products to retrieve endpoint, identity group, security group, and session data from a Cisco ISE server. To make use of this integration, your network must be running the Cisco pxGrid agent and be monitored by Lumeta Spectre.	Server Name Username Keystore File Keystore Password Truststore File Truststore Password	• Verify that you can login to your Cisco PxGrid Server with your username and password. • Verify that your Cisco pxGrid agent is running. • Verify that Spectre can discover your Cisco pxGrid agent. • Verify that you have port 443 open	cisco_ise_endpointprofile cisco_ise_identity_group cisco_ise_securitygroup cisco_ise_session	Search=>Devices=> Pxgrip IP Sessions
Qualys	Spectre helps your Qualys Enterprise server work better by comparing Qualys-subscribed and Qualys-scanned IPs with Spectre-indexed hosts in the same network space. Qualys receives a list of endpoint data information from Spectre at every polling interval, enabling Qualys to add the endpoints to its network space, thereby eliminating any gaps in coverage and ensuring the comprehensive provision of vulnerability management to Qualys customers.	Polling Interval Server Name Username Password Auto-Subscribe	• Verify that you can login to your Qualys Server with your username and password • Verify that you have port 443 open • Verify that you have IPs in your network licensed for Qualys	qualys_scanned_ips_raw qualys_subscribed_ips qualys_subscribed_ips_v	Vulnerability Management
McAfee DXL	Spectre targets on extending McAfee integration to such that events will be published to DXL message bus.	Server Name Host Name Broker Chain certs Unique Broker Id Broker Port	• Verify that System and device events (notification) are published in log file(/var/log/dxl) and DL Task Manager	No tables created	No Reports /Dashboards

RedSeal	RedSeal integration will only include ingesting RedSeal managed hosts into Spectre	Polling Interval Server Name Username Password	• Verify that you can login to your RedSeal Server with your username and password • Verify that you have IPs in your RedSeal Management Dashboard	redseal_managed_hosts	RedSeal Management

Integration Feeds (Data Pulled)	Integration Feeds (Data Pulled and Pushed)
• Emerging Threats • ISC • TOR • Emerging Threats Pro • iDefense • Carbon Black • Cisco pxGrid • Gigamon NetFlow • RedSeal	• Qualys • Infoblox • McAfee ePO • McAfee DXL

Lumeta Spectre Extension to McAfee ePO

The Lumeta Spectre extension to McAfee ePO server is fully certified by McAfee. Both "fetch" and "push" extensions make use of a polling interval you configure.

1. Login to McAfee Server
2. Browse to Software => Extensions and click on Install Extensions
3. Install the Lumeta extension: LumetaRemoteCommandPush.zip (ask SA to provide you with this file)

Granting Permissions to Use the Lumeta Spectre Extension

An ePO user without Admin privileges can be granted permissions to use the Lumeta Spectre extension as follows:

1. On the McAfee ePO server, click **Hamburger** icon > **Permission Sets.**
   Notice the new permission set created for this installed extension called "LumetaRemoteCommandPush."

1. Select **My Organization** and click **Save**.
2. Select Lumeta Spectre Remote Command and click **Edit**.
3. Select "**Activate permission to run remote command for Lumeta Spectre extension** " and click **Save**.
4. Click **Hamburger** icon > **Users.**

1. Select the user that will be using the Spectre extension and click **Actions** > **Edit**.
2. Select the **LumetaRemoteCommandPush** permission set and save the user.

Now this particular user can configure the Lumeta Spectre extension in McAfee without admin permissions, and can get and post data to, from, and into ePO.

How data is pulled and pushed for McAfee ePO

- Pull the list of Hosts/devices managed by ePO
- Determine the list of devices not managed by ePO (potentially considered rogue)

- Push devices that are not managed by ePO into ePO server and add them to Rogue Detection Systems.
- McAfee Server => Dashboards => RSD Summary displays Rogue Systems.

For further Information:

Lumeta Spectre Extension to McAfee ePO => **https://support.lumeta.com/confluence/display/SPEC/Lumeta+Spectre+Extension+to+McAfee+ePO**

Qualys and Vulnerability Management

1. This integration will run at scheduled feed interval.
2. Each time this integration is run, it will check for asset group LUMETA_ESI_DISCOVERED and update this asset group with latest data (As oppose to IPSonar where each time a report is generated, a new asset group is created)
3. Currently, we overwrite asset group with updated ips each time we run a feed
4. Please make sure that the user configured on Settings=>Integrations=>Qualys Integration page has Manager access on Qualys server.
5. Spectre gets two lists from Qualys: IPs subscribed by Qualys and IPs scanned or managed by Qualys (this list is generated from LUMETA_ESI_DISCOVERED Asset group)
6. User-enabled Qualys Integration
    a. Subscribed IPs are ingested from Qualys server into qualys_subscribed_ips table.
    b. ALL IPs currently scanned by Qualys are ingested into qualys_scanned_ips_raw table.
7. When autosubscribe is ON:
    a. Push back to Qualys subscribed list "IPs Unmanaged by Qualys"
    b. Create a list of IPs that are in Qualys subscribed List but not in Qualys managed list.
8. When autosubscribe is OFF:
    a. Find a list of IPs common between Qualys managed list and ESI discovered list.
    b. Create a list of IPs currently in subscribed list which is not in above list.
9. Create an asset group: LUMETA_ESI_DISCOVERED
10. Push the above list in Asset Group.

Qualys & Vulnerability Management => https://support.lumeta.com/confluence/display/SPEC/Qualys+Integration