Mandiant

INTEGRATION QUERIES OVERVIEW

Integrations include queries that allow the Validation Platform to identify the events coming from security controls. Many of our integrations make the query configurable. This requires the owner of the control and the owner of the Validation Platform to communicate which modifications and tuning are appropriate given the tests being run and the controls being validated.

As an example, Splunk's query should only include indexes that store logs relevant to the Actions being run, which means you include indexes for firewalls but not web servers.

By default, a Job will query an integration for 15 minutes with a frequency of once every 30 seconds. You can configure both of these times in the Integrations' Advanced Settings section.

As the criteria for the queries age out of that window, they are removed from the query. When the query ages out, the security control no longer queries and the integration service moves into a sleep state waiting for more Actions to be run.

Some integrations have queries that you define based on your integration's settings. The most common query type is an overall query, but there might also be queries related to specific Action types or specific for the integration. The following tables show which queries are available for each integration, grouped by integration type.

When setting up Actors that will be used to run Host CLI Actions, always assign its Alternate Hostname. Integrations that support Host CLI-specific queries use the information in this field, as well as the simple hostname, when the %HOST_CLI_ACTOR_HOSTNAMES% variable is used.

SIEMs and Event Aggregators

SIEMs and Event Aggregators	Available Queries				
Technology Name	**General**	**Malicious DNS Action**	**Email Action**	**Host CLI**	**Special**
Alert Logic					
Alienvault USM / OSSIM	✔				✔
ArcSight ESM					✔
Azure Sentinel	✔	✔	✔	✔	
Chronicle Backstory					
Cisco Firepower	✔			✔	✔
Elasticsearch	✔	✔	✔	✔	
Exabeam Data Lake	✔	✔	✔	✔	

SIEMs and Event Aggregators	Available Queries				
Technology Name	**General**	**Malicious DNS Action**	**Email Action**	**Host CLI**	**Special**
Google BigQuery	✔	✔	✔		
Graylog					
Helix	✔	✔	✔	✔	
Juniper Secure Analytics (JSA)	✔	✔	✔	✔	✔
Logrhythm Elasticsearch	✔				
Logrhythm SQL	✔	✔	✔	✔	
Logzilla	✔	✔	✔	✔	
Trellix Enterprise Security Manager	✔	✔	✔	✔	
QRadar	✔	✔	✔	✔	✔
Splunk	✔	✔	✔	✔	✔
Splunk ES	✔	✔	✔	✔	✔
Sumo Logic	✔			✔	
Threat Stack					

Network Technologies

Network Technologies	Available Queries				
Technology Name	**General**	**Malicious DNS Action**	**Email Action**	**Host CLI**	**Special**
Check Point (also supports their NGFW)	✔				
RSA Netwitness	✔				

Network Technologies	Available Queries				
Technology Name	**General**	**Malicious DNS Action**	**Email Action**	**Host CLI**	**Special**
Security Onion - ELK	✔				
Security Onion - ELSA	✔	✔			
Cisco Firepower FMC	✔			✔	✔
CloudTrail					
CloudWatch	✔	✔	✔	✔	
Darktrace					
Exabeam Advanced Analytics					
Trellix (supports CMS, Email, NX)					
GuardDuty					
Trellix Network DLP	✔				
Palo Alto Network Firewalls & Panorama	✔				
Securonix SNYPR					
Threat Stack					
Tipping Point SMS					
VMware AppDefense					

Endpoint Technologies

Endpoint Technologies	Available Queries				
Technology Name	**General**	**Malicious DNS Action**	**Email Action**	**Host CLI**	**Special**
Carbon Black Cloud (Also works with Defense, PSC, and ThreatHunter)	✔				
Carbon Black CB Protection					
Carbon Black CB Response	✔				
Cisco AMP					
Crowdstrike	✔				
Cybereason	✔				✔
Cylance PROTECT					
Microsoft Defender ATP					
EndGame					
Trellix Endpoint Security (HX)					
Trellix Endpoint Security	✔				
Trellix Network DLP	✔				
Netskope					
SentinelOne	✔				
Sophos Central					
Symantec DLP					

Endpoint Technologies	Available Queries				
Technology Name	**General**	**Malicious DNS Action**	**Email Action**	**Host CLI**	**Special**
Symantec EP					
Threat Stack					
VMware AppDefense					