Mandiant

SECURITY VALIDATION QUICK-START WORKBOOK

To help you with your Validation Platform deployment, we've created this workbook. It will help you identify your requirements and who you need to work with within your company during deployment. If you are using the SaaS version of Security Validation, some of the Director information will not be pertinent.

Modules Purchased

Module	Purchased (y/n)
AEDA	
Cloud Theater (Mandiant-hosted Actor)	
Email Theater	
Premium Content	
Protected Theater	
TAAM	

Interested Parties

Role	Access to Security Validation (y/n)	Contact information
Sponsor		
Manager		
Primary Admin		
Secondary Admin		
Super User		
Receives Reports		

Required Installation Information

All Directors

Description	Value
Director host information	**Hostname:**
	IP address:
Designated interface for Director to listen for connections	**Interface:**
License file	**Location of license file:**

Description	Value
Postgres database password	Changing/Setting the password is part of the software install, but a separate step for virtual appliances
Contact for Opening required Ports	

Software Directors

Description	Value
Director host information	**Hostname:**
Privileged user account	**Username:**
Designated services group	**Group:**
Check Point integration?	**Specify:** Yes or No
Online repository	**Repository:**

All Actors

Requirement	Data
Designated interface for Director to listen for connections (management Interface)*	**Interface:** Note: If you only have 1 Actor, you can use DHCP.
Test interface (optional)	**Interface:**
	IP address:
	netmask:
	gateway:
	DNS:
Monitoring interface (optional)	**Interface:**
	IP address:
	netmask:
	gateway:
	DNS:
Contacts for Opening required Ports	

NOTE: * You must configure the networking outside of the Validation Platform for Actors on RHEL 8 /CentOS 8

Linux Software Actors

Requirement	Data
Privileged user account	**Username:**
Designated services group	**Group:**
Online repository location (optional)	**Repository:**

Network Zones

Zone Name	Defended by which Security Tools	Actor Type (endpoint/network/both)
DMZ		
Internet		
Desktop		
Server		

Certificates

If self-signed certificates aren't supported, identify the components that need custom certificates and who you need to contact to get those certs. You can use the Director to generate the Certificate Signing Request and apply the certificate to the Director. If you need custom certifications for Actors, there are instructions in the Admin and install guides on how to apply them.

NOTE: Custom certificates can be required in various situations, such as when your Actor is in AWS.

Security Validation Component	Location of Component (Zone)	POC Email	POC Department
Director			

Security Validation Component	Location of Component (Zone)	POC Email	POC Department
Actor			
Actor			
Actor			

Network & Endpoint Technologies

To help you identify what technologies you are expecting to see when you run security technology and who you need to contact for more information, populate the following tables.

SIEMs

SIEM	Version	Integration point (Correlation Engine/ Indexer/Search head)	Brief Architecture Description

SIEM	Required Connections	POC Email	POC Department

Proxy

Proxy	Version	Integrate with Director	Authentication Schema

Proxy continued

Proxy	Required Connections	POC Email	POC Department

Endpoint Security Technologies

Type	Manufacturer	Version	Events to SIEM (y/n)	Director Integration (y/n)
AV				
DLP				
EDR				
HIDS/HIPS				

EndPoint Security Technologies continued

Type	Manufacturer	Required Connections	POC Email	POC Department
AV				
DLP				
EDR				
HIDS/HIPS				

Network Security Technologies

Type	Manufacturer	Version	Events to SIEM (y/n)	Director Integration (y/n)
Firewall				
IDS/IPS				
WAF				

Type	Manufacturer	Version	Events to SIEM (y/n)	Director Integration (y/n)
Malware				
Other				
Other				
Other				
Other				

Network Security Technologies continued

Type	Manufacturer	Required Connections	POC Email	POC Department
Firewall				
IDS/IPS				
WAF				
Malware				
Other				
Other				
Other				
Other				