Mandiant

NETWORK COMMUNICATIONS ARCHITECTURE

Security Validation's Director's primary functions are to be the management console that orchestrates the registration of Actors, to assign Actors roles as Attacker or Target, to coordinate bi-directional communications and the execution of malicious attacks and behaviors, and to aggregate the evidence to report a full defensive stack analysis. The Director is the point of integration into the existing security stack components and hosts the Attack Library, which is repository containing malicious Actions that can be combined into Evaluations and Sequences.

Core Capabilities:

- Manages Actors and the assignments of Attacker and Target.
- Integrates with security components: Firewall, IDS, DLP, Proxy, Endpoint, SIEM, etc.
- Orchestrates communications and execution of attack actions/behaviors.

Security Validation Actors

- Security Validation Actors can be deployed in a variety of formats to support a variety of environments and requirements: as a virtual appliance, a fully contained VM that is deployable; as software deployed on a Linux instance; as Microsoft® Windows® executables testing Windows controls; and as Apple ® Macintosh® executables testing Mac controls. An Actor is assigned an IP address and will look like any other device on the network to the security stack controls or network scanning tools.
- Security Validation Actors receive assignments and direction from the Director, leverage a key exchange for authentication, and then process the attack action patterns while traversing the production security stack. As the pattern processes, each security technology will either not respond, prevent, detect, generate events, or perform as configured when interacting with an attack behavior or sequence. The Validation Platform captures this evidence and delivers it back as a measurement of effectiveness.
- Network and Endpoint Actors are two of the more commonly used Actor types.

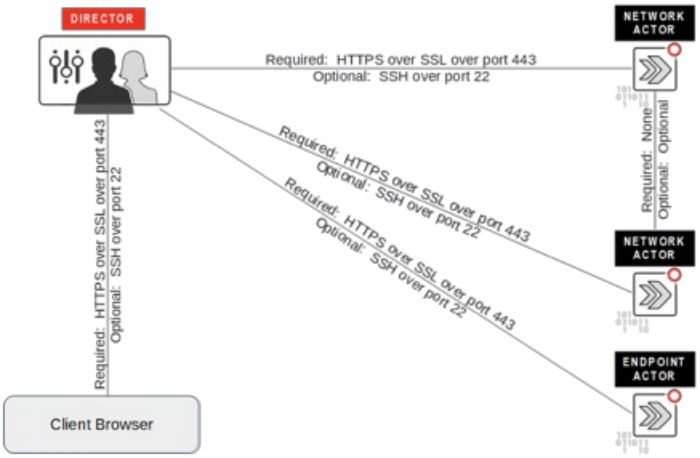
Network Actors

Network controls are controls inspecting network traffic (e.g. IDS, IPS, NGFW, etc.). To safely test production IT environments, Network Actors act as both the source and destination of a test, sending traffic between each other to see how the network control responds. These tests include segmentation and policy validation, malicious file transfer, C2, data exfiltration, etc. The Validation Platform is the only platform that safely leverages real malware and real attack bytes to provide 100% reliability of test results. Security Validation Network Actors are deployed within a customer's business zones and are available as a virtual machine, physical appliance or installable software.

Endpoint Actors

Endpoint controls are implemented to protect the host. Endpoint Actors are installed directly onto systems in the production IT environment. There is no need to install Endpoint Actors on every endpoint, simply a sampling of systems that represent deployed endpoint and user configurations. Endpoint Actors process tests within the context of a user to validate access to resources, attempt privilege escalation, exfiltrate data, and perform other behaviors across the Cyber Kill Chain. Tests can leverage all aspects of the endpoint's operating system, including the CLI and even PowerShell for Windows endpoints. Endpoint Actors can be installed onto Windows, Mac, and Linux endpoints.

Network Communication Architecture Diagram



Network Communications Architecture Description

Browser Client to Director

- **Network Interfaces:** Only a single network interface on the Director is required. This interface requires a static, routable IP address to ensure the Actor registration process functions as designed.
- **Communication Protocols:** The Security Validation Director's user interface is delivered using Web technology via HTTP over SSL on port 443 of the Director. TLS version 1.2 is used. It is recommended that port 22 be made available from a system on your network to the Director in case troubleshooting is required.

Director to Actor

- **Network Interfaces:** Two network interfaces are required for proper Actorfunction. These interfaces require static, routable IP addresses to ensure the Actor registration process functions as designed, and that tests can be processed on the Actor's second interface.
- **Communication Protocols:** The Security Validation Director communicates with the Actor via HTTP over SSL on port 443. TLS 1.2 is used. It is recommended that port 22 be made available from the Director to the Actor in case troubleshooting needs to occur. The Actor registration process generates a secure token using AES256, and that token is used to authenticate any communication from the Director to the Actor.
- **Communication Methods:** Director to Actor communication can be configured to be unidirectional. This is configured in the product as an Actor is registered to the Director with the "Comm Mode" option. Valid options include:
    - Push mode, where the Director may initiate communications to the Actor, is the default option and should be used in any network where only one-way communication is allowed from the Directorto Actor.
    - Pull mode, where the Actor initiates communications with the Director, should be used when Director cannot reach out to the Actor directly.

Actor to Actor

Network Interfaces: The Actors will communicate on their second interfaces for the execution of tests. These interfaces will require routable IP addresses to function properly. Optionally, a third interface can be added to any Actor that will consistently be executing Monitors and can be white-listed into your monitoring systems/services and Security Operations Center to ensure that your ability to detect environmental drift does not create unnecessary alert traffic.

Communication Protocols, Communication Methods: Actor-to-Actor communication is variable based on the types of tests being processed on the defenses in your environment. Any network communication on any TCP or UDP port can be processed between two Network Actors to ensure that your testing is complete and thorough.