Mandiant

SECURITY VALIDATION OVERVIEW

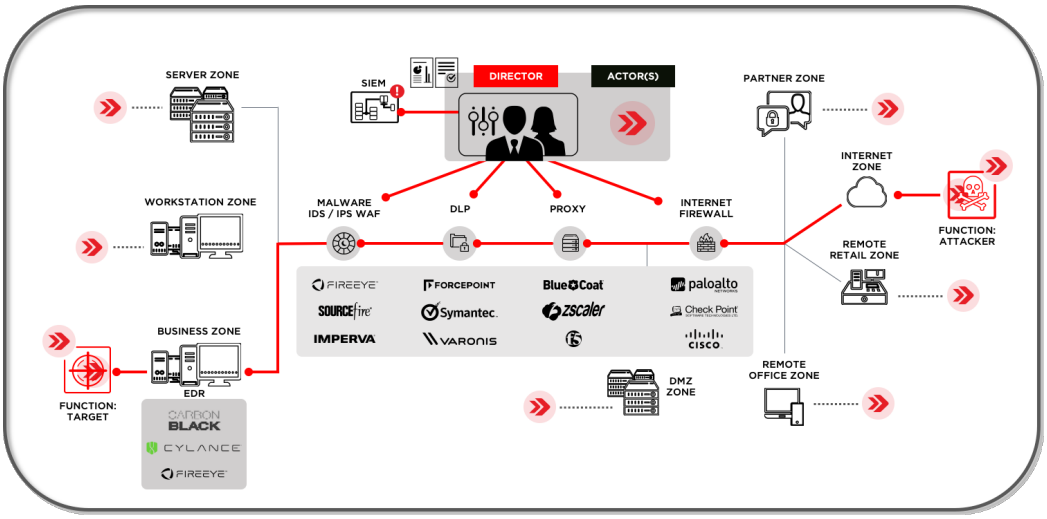
Our Security Validation platform is informed by Mandiant frontline threat intelligence on the latest attacker tactics, techniques, and procedures (TTPs) to continuously validate and measure the effectiveness of your cybersecurity controls.

Mandiant Advantage Security Validation safely processes advanced cyberattack security content within production networks. It's designed so that defenses respond to it as if an attack is taking place across the most critical areas of networks. The software produces evidence that shows how people, processes, and technologies perform when specific malicious behaviors are encountered, such as attacks by a specific threat actor or attack vector.

The core Validation components are:

- The **Director**: The main component of the platform that provides the following functionality:
  - Acts as the Integration point for your SIEM and other components of your security stack
  - Hosts the Content Library (Actions, Sequences, Evaluations, and Files) used for testing your security controls
  - Manages the Actor assignment during testing
  - Aggregates testing results and facilitates report creation
  - Maintains connections with the Mandiant Updater and Content Services, letting you automatically receive updates to both the platform and its content
- **Actors** (also referred to as Flex, Endpoint, and Network Actors): The components that safely perform tests in production environments. Specifically, use Actors to verify the configuration and test the effectiveness of:
  - Network Security Controls
  - Windows, Mac, and Linux endpoint controls
  - Email controls

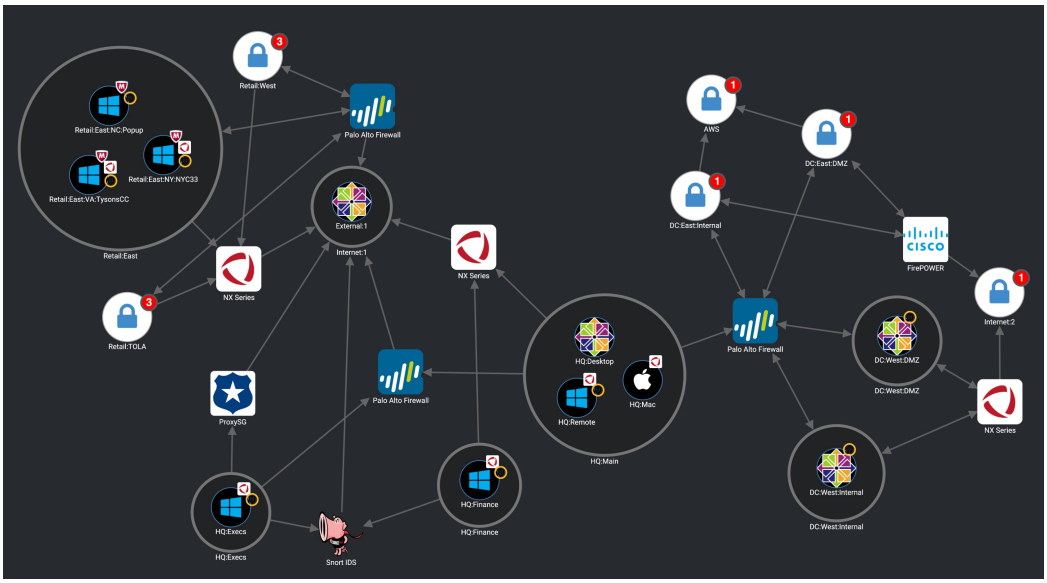
The following image provides an example of a common Validation Platform deployment in a customer environment. You can see where Actors have been deployed, what systems would potentially see the traffic for tests run between Actors, and how the Director is the component that receives the information from the systems in the environment based on an integration with a SIEM. The image also clearly shows that tests are run between Actors and not directly on systems in your environment.



Validation Platform running a test in an example environment

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Once you have your environment configured and have started running tests, you are able to see your overall Validation Platform deployment and the security technologies that blocked and fired events when tests were run.



Validation Platform map

Outside the base Validation Platform deployment, there are additional features that may be included in your subscription or on-prem version of Security Validation. These features include:

- **Protected Theater**: Lets you safely run destructive endpoint tests
- **Email Theater**: Lets you run email-based tests
- **AEDA (Advanced Environmental Drift Analysis)**: Lets you continuously test your environment and provides early alerts for defensive regressions
- **TAAM (Threat Actor Assurance Module)**: Lets you operationalize your commercial threat intelligence platform
- **Cloud Validation Module**: Lets you test your cloud security controls

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.