Mandiant

SECURITY VALIDATION USE CASES

The Validation Platform can provide many benefits to an organization. For example, identify limitations in current cybersecurity stack, evaluate proposed cybersecurity tools for an organization, automate assessment actions, train cybersecurity operators, etc. As you plan your deployment, you will want to identify your top priorities and use cases. This will help you determine where the initial deployment of Actors needs to occur, and what features and functionality you need to configure first.

If you do not already know what your primary focus is going to be, we are providing some example business and use cases.

Summary Business Cases (SBC)

- Generate baseline security control effectiveness metrics for endpoint and network security tools.
- Demonstrate ability to automate and scale enterprise security validation for constant improvement across technology, people and process
- Deliver reporting that will enable the security team to communicate security effectiveness across functional teams as well as to the executive team and board of directors
- Provide guidance for improvement of security control implementation and continuously Detect Environmental Drift to ensure those improvements are maintained over time
- Demonstrate effectiveness of installed Security Technologies against a known threat actor or attack vector

Technical Use Cases (TUC)

- Produce data to demonstrate the efficacy of the following network security controls
  - Firewall
  - IDS/IPS
  - Proxy
  - DLP
- Produce data to demonstrate the efficacy of the following endpoint security controls
  - EDR platform
  - Endpoint DLP
- Produce data to demonstrate working event detection and flow from security controls, specific to Mandiant behavior execution, in the following products:
  - SIEM
- Managed Security Provider validation