INTRO TO SECURITY VALIDATION'S MONITORS AND ADVANCED ENVIRONMENTAL DRIFT ANALYSIS (AEDA)

Mandiant Advantage Security Validation (MA-SV) Monitors are scheduled jobs to repeatedly run security content with explicitly defined results that, if not met, generate a notification. Monitors are the primary components of the Validation Platform Advanced Environmental Drift Analysis (AEDA) module. By executing security content on a frequent, repeatable basis, you can continuously validate that network defenses are operating as intended and have not been adversely affected by system changes, accidents, or intentionally malicious behavior.

Why AEDA?

Security is not a static effort. Securing your environment is a continuous process of deployment, configuration, and tuning of security technologies and products to stay ahead of bad actors. Security controls are updated, reconfigured, and moved from time to time. Testing and instrumentation must remain as fluid as your efforts to secure your environment.

Additionally, you will want to prevent regression of your security controls. The key to having a secure infrastructure is to establish a baseline and incrementally build on that baseline. AEDA will help you verify that security controls are working as expected, test configuration changes and updates, and confirm fixes to existing issues.

AEDA works best as a "purple team" effort. Whereas the blue team generally identifies the controls that should be in place, how they should respond, and what you should see, the red team identifies issues, tracks fixes, tracks performance, and ensures that key use cases are covered. AEDA and Monitors build a bridge between red and blue teams to create an ongoing mechanism for ensuring that security controls are configured and working properly per your policies.