Incident Response Team Hero Scenarios

<Author: Jerald Dawkins; Contributor: Logan DeWitt>

Transform data into decisions with Argo & Security Co-Pilot

Organizations often amass many tools and services to address complex security challenges, thinking this will provide insight into their ever-evolving cyber threat landscape. However, these tools & services are often still segregated from one another, with various departments operating independently to address multiple security concerns. Argo integrates with the organization’s existing tools & services to provide end-to-end visibility to security teams, which allows organizations to overcome data and team silos. By leveraging Security Co-Pilot to augment these datasets, security teams can parse out potential decisions and reduce the lag time to develop an effective and efficient work plan.

Scenarios

Sub-Scenario 1: Incident Response team analyzing anomalous behavior on an asset

**Target Persona/user role:** Incident Response (IR) team.

**Situation:** The IR team is investigating anomalous behavior identified on a particular asset and needs a list of existing vulnerabilities associated with that device. The team needs to determine what approach to take to ensure they address the most pressing risks first based on the unique landscape of the organization and the value of the target asset.

**Decisions Enabled:** *A*. Correlate vulnerabilities that are currently being exploited or are part of trending attack patterns that are associated to target asset. *B*. Assess the likelihood of exploitation *C*. Determine remediation priorities and develop a work plan.

**Current Practice:** Effective vulnerability remediation demands synchronized efforts from multiple stakeholders who can provide additional insight or validation. When people, processes, and data are disconnected, it results in lot of ‘swivel-chairing’ which increases lag time in assessing and mitigating potential risks to an organization. IR teams unable to give either the incident their full attention when trying to gather and correlate information from multiple security tools, reviewing risk, vulnerability, and/or pen test reports and correlating with online repository vulnerability information to determine the current risk to an asset or organization.

**objective:** By consolidating historical information and correlating current information, the IR team members can better understand the existing landscape which enables them to better assess the potential threat to the asset and overall organization.

**Sample prompt and expected response:**

**SCRIPT:**

* **IR**: Please provide me with extensive details for my most recent Microsoft Sentinel incident.
* **Copilot**: Provides details of recent incident(s) and a list to export of,
  + CVE Title & Identifier
  + Incident ID
  + Generated Date
  + Details
  + Related Endpoint name
  + Severity Score
* **IR**: Please use ArgoSecure to get asset details and vulnerability information for the endpoint listed and tell me if the asset has the vulnerability from that incident associated with it.
* **Copilot**: Reports how many vulnerabilities are associated with the target device, and correlates the recent incident details including,
  + CVE ID
  + CVE Name
  + CVSS Score
    - Risk Level details
  + Vulnerability type
  + Remediation suggestions
* **IR:** Use ArgoSecure to get a list of all assets and endpoints and provide me with the information related to the asset involved with this incident to determine if the device is being managed for backups.
* **Copilot:** Presents an analysis of device details, cross-referenced with the organization’s services to indicate that the target device appears to not be covered by backup services.
* **IR**: Please use Defender Threat Intelligence to tell me more about the CVE in question along with IOCs so we can investigate the rest of the network for other instances of this exploit being leveraged. If there are no known IOCs associated with the CVE, please provide recommended respond actions.
* **CoPilot**: Indicates there are no known IOCs associated with the vulnerability and provides response actions to take in the absence of specific IOCs,
  + Patch Management
  + Network Monitoring
  + Log Analysis
  + Endpoint Protection
  + User Education