ORION Shared Security Operations Centre (ON-SSOC) Frequently Asked Questions (FAQs)

ON-SSOC Onboarding Process and Expectations

Question: What are the prerequisites or modes of deployment?

Answer:

Prerequisites for Deployment:

1. You need an active Sentinel Workspace in your Azure subscription. This workspace should be linked to your Log Analytics Workspace, which collects log data from your IT systems.
2. Ensure your Sentinel workspace and related Resource Group in Azure have unique names, like "InstitutionName-RG" and "InstitutionName-Sentinel", to smoothen Lighthouse integration. Avoid generic names such as “Sentinel”, “Sentinel-Workspace”, “ResourceGroup1”, “ResourceGroupA”, etc.
3. Basic logs like Azure AD Sign and Audit Logs, Office 365 Logs, and Azure Activity Logs must be ingested in your workspace to enable the ON-SSOC team to query the logs and monitor the rules. Additional logs are welcome.

Mode of Deployment

1. ORION will create a separate Sentinel workspace for your institution.
2. Your Sentinel workspace will be linked to ORION's workspace via Azure Lighthouse. Lighthouse will have read-only access (only log data is read and queried, no edits or admin-level actions can be made on your Sentinel workspace).
3. ORION will establish analytic rules on your workspace to query your ingested data through Azure Lighthouse.

Engagement Expectations:

1. ORION will actively collaborate with your team during onboarding, Lighthouse access setup, testing, and rule creation.
2. Ongoing weekly/bi-weekly/monthly engagement is needed to review escalated incidents, fine-tune requirements, and enhance incident detection accuracy (True Positives).
3. Regular Technical Working Groups will be held with the subscribing institutions to discuss new features and gather service requirements.

Types of Security Incidents Monitored by ON-SSOC Team

Question: What are the key types of security incidents monitored by the ON-SSOC team?

Answer:

Identity and Access Management Use Cases:

- Unusual account sign-in activity not adhering to usual MFA enforcements.
- Account activity using third-party VPNs.
- Creation and deletion of privileged accounts in a short timeframe.
- Brute force attempts on the Azure portal.
- SharePoint file operations indicating potential data exfiltration.

Perimeter Control Use Cases:

- Network activity from Indicators of Compromise (IoCs) related to various threat actors.
- Detection of potential Command and Control traffic based on outbound traffic patterns.

AV & Malware Protection Use Cases:

- Identification of potential activity related to known malware based on IoCs or Tactics, Techniques, and Procedures (TTPs).

Managing Log Ingestion in Your Sentinel Workspace

Question: How can my IT/Security team manage log ingestion from our Sentinel workspace?

Answer:

ORION has developed log management scripts based on insights from other institutions' experiences during the Pilot and ongoing service in Sentinel. These scripts are designed to optimize log volumes in Azure to reduce your monthly bills while preserving high-fidelity data for SOC monitoring. If you plan to onboard to Sentinel and the ON-SSOC service, ORION's team can provide you with these methods and scripts for efficient log management.

Automated Responses in ON-SSOC

Question: Does ON-SSOC support automated responses?

Answer:

Currently, ON-SSOC does not offer automated response features. This decision aligns with feedback received from participating institutions regarding ORION's role in the service. However, we remain open to considering changes to this feature based on additional feedback and requirements from participating institutions.

Handling Zero-Day Threats in ON-SSOC

Question: Can the ON-SSOC team address zero-day threats? If so, how?

Answer:

The ORION team monitors advisories and bulletins from Federal and Provincial bodies, including CCCS, CanSSOC, and Ontario Government - MPBSD, to assess the need for creating new analytic rules in response to zero-day threats. Additionally, the team stays updated by reviewing Microsoft forums, SigmaRule repositories, and other relevant communities for new rules related to zero-day threats.