Cybersecurity Transformation with Microsoft Sentinel Adoption

Meeting Summary

Date: [Insert Date]
Participants:

- Commander Cook
- Joe Murray (Deputy Executive Director for Cyber Security, CBP)
- Emmett [Last Name] (USCIS, Contract Lead for R&D)
- Dwayne [Last Name]
- Michael [Last Name]
- Rhett [Last Name]
- Others (up to 40 attendees)

Main Topics Discussed

1. Transition to Microsoft Sentinel

a. Data Feeds Integration

- **Recent Addition:** Tanium data feed turned on; Sentinel is now ingesting Tanium tables.
- **Pilot Program:** Implementing Sentinel as a replacement for Thunderdome, consolidating all logs into Sentinel as the central SIEM platform.

b. Replacement of Existing Systems

- **Thunderdome Replacement:** All Thunderdome logs are being pushed into Sentinel, making Sentinel the "one-stop shop" for security monitoring.

2. Comparison of Elastic and Sentinel

a. Alert Volume and Management

- **Elastic Performance:**
  - Average of ~4 alerts based on 2,000 devices.
- **Sentinel Performance:**
  - Increased to ~2,000 alerts per week.
  - Significant increase in workload for Watch Analysts.
  - Implementation of numerous automations to manage and clean up alerts.

b. Rules Configuration

- **Elastic:** Limited to ~4 alerts based on historical data.
- **Sentinel:**
  - Increased from ~20 to over 200 custom analytic rules tailored to specific organizational needs.
  - Utilizes Defender for Endpoint, Defender for Cloud Apps, and Defender for Identity for granular monitoring.

3. Automation and Effectiveness

a. Red Team Detection

- Deployment of Defender tools has successfully detected and stopped red team exercises on three occasions.
- **Outcome:** Enhanced security posture, making it difficult for unauthorized activities to go unnoticed.

b. Working Groups and Focus Areas

- **Current Working Group:** Focused on Defender for Identity across 110 Domain Controllers (DCs).
- **Objective:** Identify Advanced Persistent Threats (APTs) and develop analytic rules to detect and mitigate them.

4. Threat Intelligence and Data Collection

a. Threat Intelligence Feeds

- Efforts to incorporate additional threat intelligence feeds.
- **Challenges:** Integration within DoD environments due to strict governance and compliance requirements.

b. Password Spray Attack Detection

- **Incident Timeline:** Detected six months ago; ongoing attack identified through Sentinel.
- **Detection Method:** Utilized Power BI and modified KQL queries for Gov Cloud.
- **Findings:** 100% failure rates in Azure PowerShell due to conditional access policies, indicating ongoing password spray attacks.

5. Q&A Session

a. Coast Guard's Decision to Adopt Microsoft Stack

- **Primary Factors:**
  - **Cost Effectiveness:** Significant cost savings compared to previous solutions.
  - **DoD Mandates:** Requirement to adopt T5 licenses and enhanced insights into environments.

- **Migration Strategy:** Moving remaining Elastic components into Sentinel to consolidate systems and reduce costs.

b. Challenges in Transitioning from Elastic

- **Increased Alert Volume:** Shift from ~4 to ~2,000 weekly alerts necessitates enhanced triage processes.
- **Analytic Rule Development:** Need to create and fine-tune over 200 custom rules.
- **Community Support:** Large Sentinel community provides extensive resources and KQL query libraries, aiding faster implementation.

c. CBP's Perspective on Adoption

- **Scale and Complexity:** CBP handles ~50 TB/day with spikes over 100 TB, involving thousands of network assets and multiple cloud environments.
- **Cost-Benefit Analysis:** Transition requires rigorous evaluation to ensure cost savings and meet CBP's specific requirements.

6. Data Ingestion and Log Management

a. Ingestion Strategy

- **Sentinel Retention:** All data retained in Sentinel for 90 days.
- **Long-Term Storage:** Post 90 days, data is moved to Azure Data Explorer (ADX) for long-term retention.
- **Cost Management:** Utilization of Event Hubs as a pass-through to minimize storage costs.

b. Log Prioritization

- **Normalization:** Leveraging Defender products to normalize data, reducing the need for one-to-one event ID ingestion.

- **Selective Event ID Pulling:** Deploying Azure Monitoring Agent (AMA) to ingest specific high-value event IDs, enhancing analytic capabilities without incurring high costs.

7. Endpoint Detection and Response (EDR) Transition

a. Current EDR Tools

- **Defender Deployment:** All workstations and Azure Virtual Desktops have Microsoft Defender installed.
- **Trellix Coexistence:** Temporary coexistence with Trellix on standard workstations and servers until full transition to Defender.

b. Effectiveness Comparison

- **Trellix:** Limited detection capabilities; Red Team was able to bypass security measures effectively.
- **Defender:** Significantly improved detection and response times; effectively halts Red Team activities promptly.

c. Transition Plan

- **Current Status:** Mapping Trellix functionalities to Defender; aim to fully transition within the next few months.
- **Compliance:** Ensuring Defender feeds integrate correctly with DoD compliance systems.

8. Automation Efforts

a. Incident Management Automations

- **Automatic Closures:** Automating the closure of known non-threatening alerts (e.g., eDiscovery cases).

- **Severity Adjustments:** Raising the severity of certain alerts based on organizational policies.
- **Instant User Notifications:** Implementing real-time notifications for policy violations to enhance user awareness and prompt corrective actions.

b. Future Automation Plans

- **Advanced Automations:** Exploring Jupyter Notebooks for machine learning and generative AI capabilities.
- **Customization:** Developing workflows to close, reopen, or escalate alerts based on completion of automated tasks.

9. Dashboard and Reporting

a. Unified SOC Experience

- **Integration:** Consolidating Defender for Identity, Defender for Endpoint, Defender for Office, Defender for Cloud Apps, and Sentinel into a unified portal.
- **Capabilities:** Enhanced threat hunting, querying, and incident management across the entire security estate.

b. Executive Dashboards

- **Current State:** Basic incident counts and statuses.
- **Development Plans:** Creating comprehensive Power BI dashboards for auditing, device monitoring, and policy compliance tailored to leadership requirements.

10. Data Loss Prevention (DLP) and Classification

a. DLP Policies

- **Scope:** Implemented across OneDrive, SharePoint, and Outlook to prevent unauthorized data exfiltration.
- **Specific Rules:**
    - **Internal Use Only:** Restrictions on sending sensitive documents externally.
    - **Password Protection:** Detection and prevention of password sharing across various Microsoft platforms.

b. Data Classification

- **Current Status:** Partial implementation; ongoing efforts to expand classification policies.
- **Future Plans:** Incorporating DoD-mandated classification levels and enhancing data labeling for better protection and tracking.

11. Future Plans and Roadmap

a. Priority Actions

- **Complete Migration from Elastic:** Transition remaining Elastic data sources to Sentinel to eliminate legacy costs.
- **Deploy Azure Monitoring Agent (AMA):** Enable specific event ID ingestion for enhanced analytic rule effectiveness.

b. Long-Term Goals

- **Expand Automations:** Incorporate machine learning and AI-driven incident responses by summer 2025.
- **Enhance Dashboards:** Develop executive-level dashboards for comprehensive visibility into the security environment.
- **Policy Refinements:** Continuously update and refine security policies to address emerging threats and compliance requirements.

Action Items

1. **Documentation:**
    - **Task:** Document all analytic rules and data feeds prior to migration.
    - **Responsible:** Security Operations Team
    - **Deadline:** [Insert Deadline]
2. **Azure Monitoring Agent Deployment:**
    - **Task:** Deploy AMA across all devices to ingest specific high-value event IDs.
    - **Responsible:** IT Deployment Team
    - **Deadline:** [Insert Deadline]
3. **Analytic Rule Development:**
    - **Task:** Develop and fine-tune analytic rules to align with the MITRE ATT&CK framework.
    - **Responsible:** Cybersecurity Analysts
    - **Deadline:** Ongoing
4. **Unified SOC Implementation:**
    - **Task:** Finalize the integration of all Defender products into the unified SOC portal.
    - **Responsible:** SOC Integration Team
    - **Deadline:** [Insert Deadline]
5. **Executive Dashboard Creation:**
    - **Task:** Design and implement Power BI dashboards for leadership visibility.
    - **Responsible:** Business Intelligence Team
    - **Deadline:** [Insert Deadline]

6. **Data Loss Prevention Enhancements:**
    - **Task:** Implement additional DLP rules and expand data classification policies.
    - **Responsible:** Compliance and Security Teams
    - **Deadline:** [Insert Deadline]

Follow-Up Points

1. **CBP's SIEM Transition:**
    - **Action:** CBP to conduct a rigorous cost-benefit analysis before transitioning to Sentinel.
    - **Responsible:** CBP Cybersecurity Division
    - **Status:** Pending
2. **Vendor Collaboration:**
    - **Action:** Continue collaboration with Navy Cyber and Marine Corps for shared resources and playbooks.
    - **Responsible:** Commander Cook and Team
    - **Status:** Ongoing
3. **Defender vs. Trellix Deployment:**
    - **Action:** Complete the transition to Defender by discontinuing Trellix within the next few months.
    - **Responsible:** Endpoint Management Team
    - **Status:** In Progress
4. **Incident Response Automation:**
    - **Action:** Develop and deploy advanced automations using Jupyter Notebooks and generative AI.

    - **Responsible:** Automation and AI Team
    - **Deadline:** Summer 2025

5. **User Training and Awareness:**

    - **Action:** Provide training sessions based on automated remediation emails to prevent inadvertent policy violations.
    - **Responsible:** Training and Development Team
    - **Status:** Planned

6. **Data Labeling and Classification Expansion:**

    - **Action:** Implement comprehensive data classification policies as per DoD and internal requirements.
    - **Responsible:** Data Governance Team
    - **Deadline:** [Insert Deadline]

Additional Notes

- **Community Support:** Leveraging the large Microsoft Sentinel community for resources, KQL queries, and best practices.
- **Cost Management:** Emphasis on cost-effective data ingestion and storage strategies to handle large volumes without escalating costs.
- **Policy Enforcement:** Continuous improvement of security policies to align with DoD mandates and organizational needs.
- **User Behavior Monitoring:** Enhanced monitoring and immediate feedback mechanisms to educate users and prevent risky behaviors.

This summary encapsulates the key discussions, decisions, and action items from the meeting. For detailed information or specific inquiries, please refer to the meeting transcript or contact the respective team leads.