1.3. User Roles and Responsibilities

In the Spectra360 Security Operations Center (SOC) platform, a well-defined structure of user roles ensures efficient security monitoring, threat detection, and incident response. Each role carries specific responsibilities, contributing to the platform's overall effectiveness.

1.3.1. SOC Manager

Responsibilities:

- Oversee daily SOC operations, ensuring seamless coordination among team members.
- Develop and implement security policies and procedures to maintain a robust security posture.
- Manage resource allocation, set priorities, and ensure that security objectives align with organizational goals.
- Act as the primary liaison between the SOC team and executive management, providing regular updates on security status and incidents.

1.3.2. Tier 1 Analyst – Triage Specialist

Responsibilities:

- Monitor security alerts and alarms to identify potential security incidents.
- Assess and prioritize alerts based on severity and potential impact.
- Determine the validity of alerts, distinguishing between false positives and genuine threats.
- Escalate confirmed incidents to Tier 2 analysts for further investigation.

1.3.3. Tier 2 Analyst – Incident Responder

Responsibilities:

- Conduct in-depth analysis of escalated security incidents to determine their scope and impact.
- Utilize threat intelligence to enrich incident data and understand adversary tactics.
- Develop and implement containment and remediation strategies to address security incidents.
- Document incident findings and actions taken for post-incident review.

1.3.4. Tier 3 Analyst – Threat Hunter

Responsibilities:

- Proactively search for threats within the organization's networks and systems that may evade standard detection mechanisms.
- Conduct vulnerability assessments and penetration testing to identify potential security weaknesses.
- Analyze advanced threats and develop detection techniques to enhance security monitoring.
- Provide guidance and recommendations to improve security controls and monitoring capabilities.

1.3.5. Security Engineer

Responsibilities:

- Design, implement, and maintain security infrastructure and tools to support SOC operations.
- Configure and manage security monitoring solutions, ensuring optimal performance.
- Collaborate with analysts to fine-tune detection rules and reduce false positives.
- Stay updated on emerging security technologies and recommend enhancements to existing tools.

1.3.6. Compliance Auditor

Responsibilities:

- Ensure that the organization's security practices adhere to relevant regulatory requirements and industry standards.
- Conduct regular audits of security controls and processes to verify compliance.
- Prepare and present compliance reports to management and regulatory bodies as needed.

1.3.7. Dark Web Analyst

Responsibilities:

- Monitor dark web forums, marketplaces, and other sources for information related to potential threats against the organization.
- Analyze findings to assess the credibility and relevance of identified threats.
- Collaborate with incident responders to address risks associated with dark web activities.
- Maintain awareness of dark web trends and methodologies to enhance monitoring efforts.

Revision #2
Created 9 February 2025 20:02:20 by Admin
Updated 10 February 2025 10:51:21 by Admin