The Triaging Process

What Is Alert Triaging?

Alert triaging, performed by a Security Operations Center (SOC) analyst, is the process of evaluating and prioritizing security alerts generated by various monitoring and detection systems to determine their level of threat and potential impact on an organization's systems and data. It involves systematically reviewing and categorizing alerts to effectively allocate resources and respond to security incidents.

Escalation is an important aspect of alert triaging in a SOC environment. The escalation process typically involves notifying supervisors, incident response teams, or designated individuals within the organization who have the authority to make decisions and coordinate the response effort. The SOC analyst provides detailed information about the alert, including its severity, potential impact, and any relevant findings from the initial investigation. This allows the decision-makers to assess the situation and determine the appropriate course of action, such as involving specialized teams, initiating broader incident response procedures, or engaging external resources if necessary.

Escalation ensures that critical alerts receive prompt attention and facilitates effective coordination among different stakeholders, enabling a timely and efficient response to potential security incidents. It helps to leverage the expertise and decision-making capabilities of individuals who are responsible for managing and mitigating higher-level threats or incidents within the organization.

What Is The Ideal Triaging Process?

1. Initial Alert Review:
   - Thoroughly review the initial alert, including metadata, timestamp, source IP, destination IP, affected systems, and triggering rule/signature.
   - Analyze associated logs (network traffic, system, application) to understand the alert's context.
2. Alert Classification:
   - Classify the alert based on severity, impact, and urgency using the organization's predefined classification system.
3. Alert Correlation:
   - Cross-reference the alert with related alerts, events, or incidents to identify patterns, similarities, or potential indicators of compromise (IOCs).
   - Query the SIEM or log management system to gather relevant log data.
   - Leverage threat intelligence feeds to check for known attack patterns or malware signatures.
4. Enrichment of Alert Data:
   - Gather additional information to enrich the alert data and gain context:
     - Collect network packet captures, memory dumps, or file samples associated with the alert.
     - Utilize external threat intelligence sources, open-source tools, or sandboxes to analyze suspicious files, URLs, or IP addresses.
     - Conduct reconnaissance of affected systems for anomalies (network connections, processes, file modifications).
5. Risk Assessment:
   - Evaluate the potential risk and impact to critical assets, data, or infrastructure:
     - Consider the value of affected systems, sensitivity of data, compliance requirements, and regulatory implications.
     - Determine likelihood of a successful attack or potential lateral movement.
6. Contextual Analysis:

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

- The analyst considers the context surrounding the alert, including the affected assets, their criticality, and the sensitivity of the data they handle.
- They evaluate the security controls in place, such as firewalls, intrusion detection/prevention systems, and endpoint protection solutions, to determine if the alert indicates a potential control failure or evasion technique.
- The analyst assesses the relevant compliance requirements, industry regulations, and contractual obligations to understand the implications of the alert on the organization's legal and regulatory compliance posture.

7. Incident Response Planning:

- Initiate an incident response plan if the alert is significant:
  - Document alert details, affected systems, observed behaviors, potential IOCs, and enrichment data.
  - Assign incident response team members with defined roles and responsibilities.
  - Coordinate with other teams (network operations, system administrators, vendors) as necessary.

8. Consultation with IT Operations:

- Assess the need for additional context or missing information by consulting with IT operations or relevant departments:
  - Engage in discussions or meetings to gather insights on the affected systems, recent changes, or ongoing maintenance activities.
  - Collaborate to understand any known issues, misconfigurations, or network changes that could potentially generate false-positive alerts.
  - Gain a holistic understanding of the environment and any non-malicious activities that might have triggered the alert.
  - Document the insights and information obtained during the consultation.

9. Response Execution:

- Based on the alert review, risk assessment, and consultation, determine the appropriate response actions.
- If the additional context resolves the alert or identifies it as a non-malicious event, take necessary actions without escalation.
- If the alert still indicates potential security concerns or requires further investigation, proceed with the incident response actions.

10. Escalation:

- Identify triggers for escalation based on organization's policies and alert severity:
  - Triggers may include compromise of critical systems/assets, ongoing attacks, unfamiliar/sophisticated techniques, widespread impact, or insider threats.
- Assess the alert against escalation triggers, considering potential consequences if not escalated.
- Follow internal escalation process, notifying higher-level teams/management responsible for incident response.
- Provide comprehensive alert summary, severity, potential impact, enrichment data, and risk assessment.
- Document all communication related to escalation.
- In some cases, escalate to external entities (law enforcement, incident response providers, CERTs) based on legal/regulatory requirements.

11. Continuous Monitoring:

- Continuously monitor the situation and incident response progress.
- Maintain open communication with escalated teams, providing updates on developments, findings, or changes in severity/impact.
- Collaborate closely with escalated teams for a coordinated response.

12. De-escalation:

- Evaluate the need for de-escalation as the incident response progresses and the situation is under control.
- De-escalate when the risk is mitigated, incident is contained, and further escalation is unnecessary.
- Notify relevant parties, providing a summary of actions taken, outcomes, and lessons learned.

learned.

Regularly review and update the process, aligning it with organizational policies, procedures, and guidelines.

Adapt the process to address emerging threats and evolving needs.

Previous Next Mark Complete & Next

Powered by HACKTHEBOX