ManageEngine
Log360

The CISO's compass:

Strategic responses to cyber breaches

Author: **Tanya Austin**

www.manageengine.com/log-management/

Introduction

In today's complex digital landscape, organizations face a constant threat of cyberattacks. A well-executed incident response plan is vital in order to mitigate damage, protect data, and ensure business continuity. Chief information security officers (CISOs) play a pivotal role in this process, ensuring that organizations are prepared to respond effectively to security incidents.

CISOs' responsibilities extend beyond technical expertise. They bridge the gap between the technical team and the broader organization, including business leaders and board members. Effective communication from the CISO is essential to maintain transparency and trust among stakeholders, who need to be reassured that the incident is being handled professionally.

This e-book provides a comprehensive guide for CISOs to navigate the complexities of incident response. We delve into the immediate actions a CISO must take when confronted with a security incident, including:

- **Rapid threat analysis:** Assessing the severity and scope of the threat to prioritize response efforts.
- **Swift containment:** Deploying containment measures to limit the damage caused by the incident.
- **Effective remediation and recovery:** Eradicating the threat and restoring systems to a secure, operational state.
- **Post-incident analysis:** Conducting reviews to spot areas for improvement and enhance response strategies for incidents in the future.

By empowering their teams to identify, contain, and eradicate threats, CISOs can significantly improve their organization's resilience. Through real-world examples, this e-book will provide practical insights into the role of a CISO in each stage of the incident response process.

Threat analysis: How to understand the threat you're dealing with

As a CISO, one of your primary responsibilities is to assess the severity of security incidents and their potential impact on your organization. The first critical step toward effective incident resolution is understanding the nature of the threat you're facing. To do this, you'll rely on your team of analysts, who will provide you with key insights into the indicators of compromise (IoCs) and other threat intelligence.

Here's a structured approach to performing a comprehensive analysis of an incident:

1. **Allocate analysts for IoC analysis:** For every potential threat and alarm raised, your team will need to review IoCs. IoCs can include but are not limited to: unusual login patterns, unauthorized data transfers, suspicious network traffic, geographic irregularities, unusual software installations, unexpected start of services or processes, changes to system configurations, and large amounts of file activity on sensitive files. These indicators are often the first signs of an intrusion and can help identify the attack vectors and scope of the breach.

2. **Leverage threat intelligence feeds:** Utilize threat intelligence sources to evaluate the severity of the threat. These feeds can provide real-time data about emerging threats and help you assess whether the incident involves known threat actors; advanced tactics; or is part of a larger, coordinated attack.

3. **Assess IP reputation and vulnerability scores:** Instruct your analysts to check the IP reputation scores of any suspicious addresses involved in the attack. Cross-referencing these with threat intelligence feeds will allow you to confirm whether they are associated with known malicious activity. Additionally, review the vulnerability scores of affected systems to determine if any unpatched vulnerabilities have been exploited, contributing to the breach.

4. **Review user activity and asset inventory:** Pull detailed user activity reports to identify potentially compromised accounts or unauthorized access to sensitive systems. Conduct a thorough asset inventory check to determine which systems and data have been compromised or are at risk, allowing you to understand the full scope of the breach.

5. **Identify attack patterns and actor profiles:** Analyze the attack patterns to see if they match known tactics used by specific threat actor groups. Reference historical incident data, threat actor profiles, and frameworks such as the MITRE ATT&CK® knowledge base to gain insights into the attackers' motivations and methodologies. This context can provide a clearer picture of the severity of the threat and guide your response strategy.

6. **Rapid assessment:** Based on the systems affected or if there has been a confirmed breach of sensitive data, you'll have to do a quick financial impact calculation. This is an estimate of how much the incident is going to cost your organization. A quick estimate of the loss of revenue during downtime and the penalties you may incur as a result of regulations like the GDPR or the CCPA will give you an idea of how much the incident will affect the organization financially. You'll also have to factor in disruptions to other business operations, such as order processing, shipping, and customer support.

7. **Communication:** As a CISO, you'll also have to personally handle a couple of things. A crucial thing to do is to work together with a legal team to determine any sort of legal repercussions that might spring up due to the incident. You'll also have to be the person that delivers the news to the board, PR and customer-facing teams, and others in the C-suite. Communication is a critical aspect of the CISO job description. Here are some pointers to keep in mind:

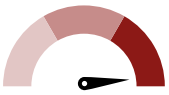
    a. Board members might not be technical experts. Therefore, choose simple, non-technical language to explain the incident. Highlight how the incident affects business operations, revenue, and reputation. The estimate you calculated earlier is something all board members will be interested in and will need to be part of your presentation as well.

    b. Share what is known about the incident, the response actions taken, and any uncertainties or risks. Provide regular updates at frequent intervals about how the situation is progressing.

    c. Use visuals to illustrate the scope of the incident, timelines, and the impact. This helps make complex information more digestible.

    d. Compare the incident to industry benchmarks or similar incidents in other organizations to give perspective on the severity and response.

    e. Reference past incidents and how the current response plan builds on previous lessons learned.



High-impact incident

The CISO's screen flashed with a massive data exfiltration alert. Analysts quickly reviewed unusual login patterns and large data transfers. Threat intelligence confirmed the attack was from a sophisticated nation-state group targeting sensitive customer data. After analyzing IP reputation scores, it became clear the attackers had exploited a legacy system vulnerability. The team examined the user activity logs and determined that high-value assets were compromised. Using the MITRE ATT&CK framework, they identified advanced tactics like phishing and lateral movement. The breach posed severe risks, including financial loss, reputational damage, and regulatory fines, leading the CISO to prioritize immediate breach containment efforts.

Low-impact incident

A brute-force attack on a less-sensitive system triggered an alert. A junior analyst investigated and found failed login attempts from known script kiddie IPs. Vulnerability scans revealed the system was fully patched with no vulnerabilities. The business impact assessment showed minimal risk to core functions. The analyst pulled user activity logs to confirm if there was malicious behavior or successful access. It was determined that this was not the case. This aligned with historical attack patterns from previous low-level threat actors. With no critical data at risk, the CISO classified it as a low-impact incident, allocating minimal resources to monitor and contain it while focusing on the high-impact breach.

Threat containment: Stopping the threat from spreading through your network

After assessing the severity of the incident and understanding the potential implications it holds for your business, containing the threat is the next crucial step. Some common containment strategies apply to a lot of different incidents that occur.

Isolation of affected assets involves segregating the affected system from the network or shutting it down to prevent the spread of the threat. Blocking malicious IP addresses at the firewall halts ongoing attacks. Disabling compromised user accounts limits unauthorized access. These are the first few containment strategy directives you can issue to your security team.

Automated incident response is essential for timely and effective containment. SIEM solutions can automatically isolate suspicious endpoints and block malicious processes and files.

We always recommend that you provide regular updates on how the incident is being handled to key stakeholders, including executive management, IT teams, and affected employees. This involves providing updates on the incident's status, potential impacts, and the actions being taken to mitigate the threat.

This is also the stage where you'll need to coordinate with external parties, such as the media, cybersecurity firms, and regulatory bodies, as necessary. This is, of course, only necessary if the incident is a breach of information that puts the public at risk. This involves managing public communication to protect the organization's reputation and seeking external expertise for incident resolution.

Things to consider while implementing containment measures

Here are some things to consider while deploying your containment strategy:

- Assess the impact on systems, data, and resources to choose a containment strategy that minimizes harm.
- Maintain logs, memory states, and affected files for forensic analysis.
- Balance containment with business continuity, ensuring critical services remain operational.
- Consider the time and resources required for different strategies, prioritizing quick and effective solutions.
- Evaluate past incident responses and the success of previous strategies.
- Ensure containment measures are sustainable until the threat is eradicated and systems are secure.

1. Ransomware attack

Threat: A ransomware attack encrypts critical systems and data, demanding a ransom payment for decryption.

CISO's containment strategy:

- **Incident response team activation:** Assemble an incident response team to coordinate the response effort.
- **Immediate isolation:** Disconnect affected systems from the network to prevent lateral movement of the ransomware.
- **Forensic analysis:** Collect and analyze system logs, network traffic, and encrypted files to identify the attack vector and potential vulnerabilities.
- **Negotiation (if necessary):** If deemed necessary, engage with the threat actor to assess the feasibility of negotiation and potential payment. However, this should be done carefully and with the guidance of law enforcement.
- **Law enforcement involvement:** Work with law enforcement to investigate the incident and potentially track down the attackers.

2. Insider threat

Threat: Malicious activities by an insider, such as data theft, sabotage, or espionage.

CISO's containment strategy:

- **Identify the insider:** Conduct a thorough investigation to identify the insider and their motives.
- **Isolate the insider:** Revoke the user's access to sensitive systems and data.
- **Forensic analysis:** Collect and analyze digital evidence, including system logs, emails, and documents.
- **Legal action:** Consider legal action against the insider, if appropriate.
- **Review access controls:** Strengthen access controls and implement stricter authentication and authorization policies.

Recovery and remediation

A major stage of incident response that requires all hands on deck is the recovery stage. You will need to remove the threat from the environment completely. This involves identifying and removing all malicious software, such as malware, ransomware, and backdoors. Patching vulnerabilities in systems and applications is essential to prevent future attacks.

At this stage of the process, your investigations should have revealed the attacker's objectives and the scope of the breach. The next part of recovery should prioritize **restoring critical systems and data,** like financial records, customer information, and intellectual property.

To prevent future incidents, a **vulnerability assessment** should be conducted to identify weaknesses in the organization's security posture. Apply **security patches and updates** to handle known vulnerabilities. Finally, **reviewing and strengthening security policies** and procedures can help to improve the overall security posture of the organization.

Once the threat has been eradicated, the focus shifts to restoring systems to a secure and operational state. This involves restoring systems from backups or rebuilding them from scratch, and configuring them with appropriate security settings and access controls. Testing restored systems is crucial to ensure that they are functioning correctly.

To maintain system integrity, security scans should be conducted to **identify any new vulnerabilities or threats.** Implementing security monitoring and detection tools can help to monitor network traffic and system activity for suspicious behavior.

The final step is to recover any lost or corrupted data using backups. Once the data is recovered, it should be validated to ensure its accuracy and completeness.

A healthcare organization experiences a ransomware attack that encrypts critical patient records, financial data, and operational systems. The organization's security team immediately initiates its incident response plan.

Threat eradication:

- **Malware removal:** Identify and remove ransomware from infected systems by using specialized tools, isolating systems, and halting network traffic.
- **Vulnerability patching:** Patch known vulnerabilities in OSs, applications, and network devices, and update antivirus software, firewalls, and other security solutions.

System and data restoration:

- **Prioritization:** Focus on restoring critical systems like patient records and financial systems first.
- **Data recovery:** Use backups to recover encrypted data, with manual data entry as a fallback for unrecoverable data.
- **System restoration:** Restore or rebuild systems with strong security settings (e.g., complex passwords, access controls, or encryption).

Vulnerability assessment and remediation:

- **Security audit:** Conduct a comprehensive audit to identify network, system, and application vulnerabilities (e.g., weak passwords, outdated software, or misconfigurations).
- **Patch management:** Implement a robust process to ensure all systems and applications are up to date with security patches.
- **Security policy review:** Strengthen security policies, including incident response plans, access controls, and data backup strategies.

Continuous monitoring and detection:

- **Security monitoring:** Deploy SIEM tools to monitor network traffic, system logs, and user activity for malicious behavior.
- **Intrusion detection systems (IDSs):** Leverage IDSs to detect and alert on suspicious network traffic and potential attacks.

Post-incident analysis

In the aftermath of a security incident and its containment, CISOs play a crucial role in conducting a comprehensive post-incident analysis. This analysis helps identify vulnerabilities, improve incident response, and strengthen overall security posture. Key metrics such as mean time to detect (MTTD) and mean time to recover (MTTR) are important metrics in assessing the effectiveness of the SOC.

Reviewing the security team's performance in addressing the incident

While MTTD and MTTR are common metrics that are used to evaluate the effectiveness of how the incident was dealt with, CISOs still need to look at the incident handling process more granularly to spot gaps that need to be closed. These four metrics are far more revealing in just how efficiently your team is handling incidents.

- **MTTD:** The average time taken to detect the incident from the moment it occurs.
- **Mean time to acknowledge (MTTA):** The average time between a system generating an alert and an IT staff member acknowledging and starting to address the issue.
- **MTTR:** The average time required to recover from the incident, including containment, eradication, and restoration efforts.
- **Mean time to contain (MTTC):** The total time taken to detect, acknowledge, and resolve an incident. It's calculated by averaging the sum of these times across multiple incidents.

MTTD:

Definition: The average time it takes to identify a security incident after it has occurred.

Calculation:

1. Record the time each incident occurred.
2. Record the time each incident was detected.
3. Calculate the time difference for each incident.
4. Average these detection times.

Example:

- **Incident 1:** Occurred at 2am, detected at 4am (Detection time = 2 hours)
- **Incident 2:** Occurred at 1pm, detected at 3:30pm (Detection time = 2.5 hours)
- **Incident 3:** Occurred at 3am, detected at 5am (Detection time = 2 hours)

MTTD = (2 + 2.5 + 2) / 3 = 2.17 hours

Analysis:

- **Benchmarking:** Compare the MTTD against industry standards or past performance.
- **Trends:** Improving metrics indicates enhanced incident response capabilities. A decreasing trend signifies faster detection and resolution of issues. Conversely, increasing metrics might signal a decline in performance, possibly due to less effective containment strategies. To understand these trends fully, consider factors like new tools, training, or changes in operational processes.
- **Improvements:** If the MTTD is higher than desired, investigate the efficiency of monitoring tools and training. Implement advanced detection technologies or enhance existing ones.

MTTA:

Definition: The average time it takes for the security team to acknowledge an incident after it has been detected.

Calculation:

- Record the time each incident was detected.
- Record the time each incident was acknowledged.
- Calculate the time difference for each incident.
- Average these acknowledgment times.

Example:

- **Incident 1:** Detected at 4pm, acknowledged at 4:15pm (Acknowledge time = 15 minutes)
- **Incident 2:** Detected at 3:30am, acknowledged at 3:45am (Acknowledge time = 15 minutes)
- **Incident 3:** Detected at 7pm, acknowledged at 7:10pm (Acknowledge time = 10 minutes)

MTTA = (15 + 15 + 10) / 3 = 13.33 minutes

Analysis:

- **Responsiveness:** Check if the response times are within acceptable limits. Refer to industry benchmarks from recognized standards to set realistic acknowledgement times.
- **Improvements:** If acknowledgment times are high, consider improving alert mechanisms and communication protocols. Use SIEM solutions and other monitoring tools to automate data collection and ensure precise timestamping.

MTTR:

Definition: The average time it takes to recover from a security incident, from detection to full restoration.

Calculation:

1. Record the time each incident was detected.
2. Record the time each incident was fully recovered.
3. Calculate the time difference for each incident.
4. Average these recovery times.

Example:

- **Incident 1:** Detected at 4pm, recovered at 10pm (Recovery time = 6 hours)
- **Incident 2:** Detected at 3:30am, recovered at 12am (Recovery time = 8.5 hours)
- **Incident 3:** Detected at 5am, recovered at 9am (Recovery time = 4 hours)

MTTR = (6 + 8.5 + 4) / 3 = 6.17 hours

Analysis:

- **Efficiency:** Identify timestamps for detection, acknowledgment, containment, eradication, and full recovery. Break down the recovery process into key steps (e.g., containment and eradication) and measure the time taken for each step.
- **Improvements:** If the MTTR is higher than industry benchmarks, consider automating recovery processes and enhancing training programs for faster response. Gather insights from team members on perceived inefficiencies or challenges encountered during recovery.

MTTC:

Definition: The average time it takes to contain a security incident after it has been acknowledged.

Calculation:

1. Record the time each incident was acknowledged.
2. Record the time each incident was contained.
3. Calculate the time difference for each incident.
4. Average these containment times.

Example:

- **Incident 1:** Acknowledged at 4:15am, contained at 5am (Containment time = 45 minutes)
- **Incident 2:** Acknowledged at 3:45pm, contained at 4:30pm (Containment time = 45 minutes)
- **Incident 3:** Acknowledged at 5:10am, contained at 6am (Containment time = 50 minutes)

MTTC = (45 + 45 + 50) / 3 = 46.67 minutes

Analysis:

- **Containment effectiveness:** Evaluate if containment strategies are efficient. Determine if the necessary resources (e.g., personnel, tools, and access) were available promptly during containment.
- **Improvements:** If containment times are longer, review containment protocols and consider integrating faster containment technologies. Conduct regular training sessions and simulations to ensure the team is well prepared and familiar with containment procedures.

Other things CISOs should know about

Strategies to improve key metrics:

- **Deploy advanced monitoring tools:** Implement advanced SIEM solutions to enhance real-time monitoring and anomaly detection.
- **Implement threat intelligence:** Use threat intelligence feeds to stay updated on emerging threats and proactively identify potential attacks.
- **Automate response actions:** Utilize automation for routine incident response tasks to reduce human error and accelerate recovery times.

Collaborating with the SOC team

Team integration and support:

- **Regular meetings:** Schedule regular meetings with the SOC team to review current metrics, discuss challenges, and brainstorm solutions.
- **Feedback loop:** Encourage a culture of feedback where team members can share their observations and suggestions for process improvements.
- **Pilot programs:** Test new detection and recovery strategies on a small scale before a full rollout to identify potential issues and refine processes.
- **Continuous improvement:** Use lessons learned from each incident to continually refine and enhance incident response strategies.

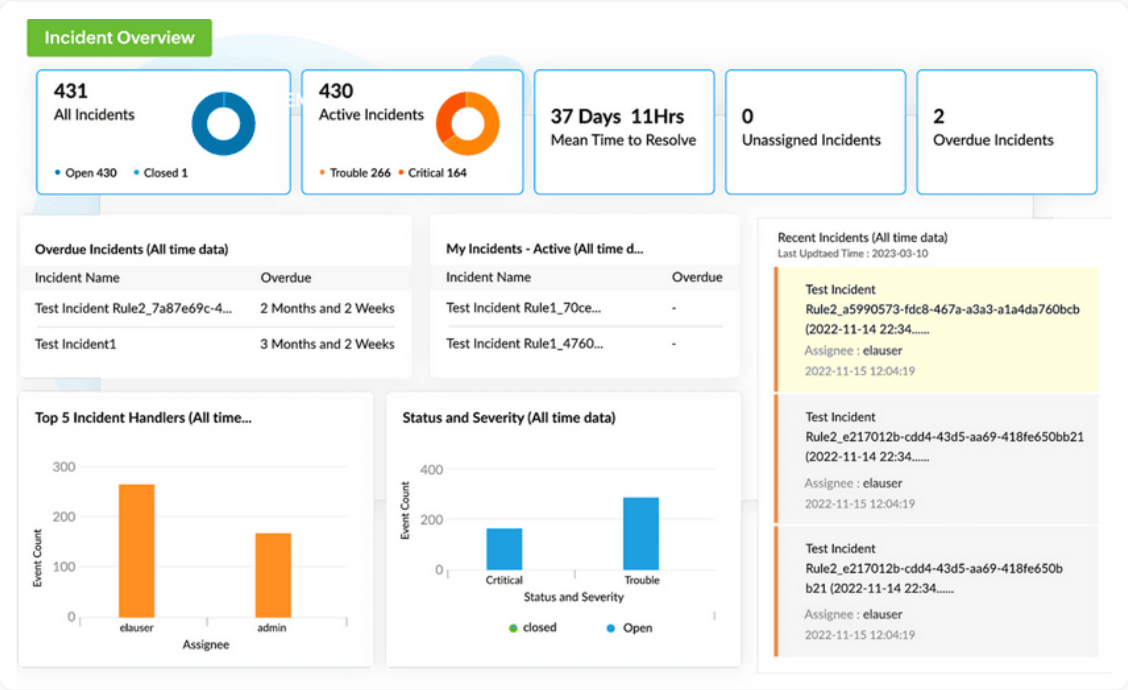
Presenting analysis to the board of directors

Effective communication:

- **Highlight key metrics:** Present clear and concise metrics for the MTTD and MTTR, emphasizing trends, improvements, and areas needing attention.
- **Business impact:** Explain the business impact of the security incident, including potential financial losses, reputational damage, and operational disruptions.
- **Strategic initiatives:** Outline strategic initiatives to improve detection and recovery times, detailing the expected benefits and resource requirements.
- **Budget and resources:** Provide a realistic budget proposal for implementing new tools, training programs, and additional resources needed for improved incident response.

How to communicate better with stakeholders:

- **Interactive presentations:** Use interactive presentations with data visualizations to engage board members and facilitate better understanding.
- **Q&A sessions:** Prepare for questions and ensure you can provide detailed explanations and justifications for proposed improvements.
- **Regularly update detection rules:** Ensure detection rules and signatures are up to date to recognize the latest threats.



Log360: The SIEM solution for CISOs

Strengthen your SOC's incident management with Log360's dedicated incident overview dashboard

Log360's powerful incident manager allows enterprises to optimize their SOC metrics by providing a streamlined incident resolution process. With the help of its actionable incident dashboard, businesses can easily track key metrics such as MTTD, MTTR, and more. The dashboard also provides insights into active and unresolved incidents as well as recent and critical incidents, giving insights into the workload of security analysts. With this information, enterprises can triage and prioritize incident resolution to ensure their SOC functions optimally.

Author bio:

Tanya Austin

is a seasoned cybersecurity author with extensive experience in SIEM systems. With a deep understanding of the MITRE ATT&CK framework, she provides insightful analysis and practical strategies to help organizations enhance their security posture. Passionate about cybersecurity, Tanya is dedicated to sharing knowledge and empowering others to navigate the complex landscape of digital threats.