



Building an Intelligence-Led SOC

CISO Checklist

 Mandos  mandos.io



Step 1: Define Your Threat Model and Prioritize Your Defenses

- Identify Critical Assets:** Catalog and classify data, systems, and applications crucial for business operations.



Example

For a hospital, this might include Electronic Health Records (EHR) systems, medical imaging equipment, and patient portals.

- Conduct Threat Assessment:** Analyze potential threats based on industry, geopolitical factors, and current security posture..



Example

A software company might prioritize intellectual property theft, while a government agency might focus on espionage and sabotage.

- Develop a Risk Register:** Rank threats based on likelihood and potential impact. This informs resource allocation and prioritization

Step 2: Embrace Threat Intelligence as Your Guide

- Determine Intelligence Requirements:**
 - What specific information do you need? (e.g., TTPs of relevant threat actors, vulnerabilities in your industry, emerging attack vectors).
 - What are your intelligence consumption needs? (e.g., real-time feeds for active monitoring, detailed reports for strategic planning)
- Source Threat Intelligence:**
 - Open-Source Intelligence (OSINT):** Valuable starting point but often lacks depth or timeliness. Examples: Cybersecurity news sites, vulnerability databases.
 - Commercial Threat Intelligence:** Provides more specialized, curated, and actionable insights, often tailored to specific industries or threats. Consider vendors like CrowdStrike, FireEye, Recorded Future.
 - Industry Information Sharing and Analysis Centers (ISACs):** Facilitate collaboration and intelligence sharing within specific sectors.
- Operationalize Threat Intelligence:**

- Threat Intelligence Platform (TIP):** Centralizes, analyzes, and integrates intelligence from multiple sources. Examples: Anomali, ThreatConnect, IBM QRadar.
 - Integrate with SIEM and Security Tools:** Enable automated threat feeds, correlation rules, and alerts based on relevant intelligence.
-

Step 3: Automate and Orchestrate for Efficiency and Scale

- Identify Automation Opportunities:** Target repetitive, time-consuming tasks to free up analysts for higher-level functions.



Example

Alert triage and enrichment, incident response playbook execution, phishing campaign analysis.

- Security Orchestration, Automation, and Response (SOAR):** Automates workflows, integrates security tools, and provides a centralized platform for incident response. Examples: Splunk Phantom, Palo Alto Networks Cortex XSOAR, IBM Resilient.
 - Develop and Refine Playbooks:** Standardize and automate responses to common incidents. Continuously review and update these playbooks based on new threats and intelligence.
-

Step 4: Build a Strong SOC Team

- Assess Existing Skills:** Identify knowledge gaps and training needs within your current security team.
 - Hire Strategically:** Prioritize candidates with experience in threat intelligence analysis, incident response, and relevant security technologies.
 - Foster a Culture of Continuous Learning:** Encourage trainings, attendance at industry conferences, and knowledge sharing within the SOC team.
-

Step 5: Implement Ongoing Monitoring and Improvement

- Define Key Performance Indicators (KPIs):** Track metrics like mean time to detect (MTTD), mean time to respond (MTTR), and the number of false positives to measure SOC effectiveness.
- Conduct Regular Security Posture Assessments:** Utilize penetration testing, vulnerability scanning, and red teaming exercises to identify weaknesses and validate defenses.
- Continuously Review and Update Processes and Technologies:** The threat landscape is constantly evolving, so your SOC should too. Regularly reassess your

threat model, intelligence sources, and security toolset to ensure they remain effective.