SecOps transformation

Responding to security incidents and vulnerabilities is an ongoing process and reacting too slowly can have drastic consequences. Transforming your security operations enables and automates the collaboration of data and processes between IT, security, and risk. This automation will mitigate security risks quickly and effectively.

Transform security operations

- Reduce vulnerabilities in IT infrastructure, applications, cloud, OT, and services.
- Integrate security, risk, and IT for more efficient operations.
- Reduce breaches and data loss.

Optimize and orchestrate enterprise security operations

- Automate and centralize case management for SOC, DLP, and more.
- Scale resources and improve operational efficiency.
- Increase the impact and retention of scarce security talent.

Respond with agility to evolving cyber threats

- Manage high-profile security incidents, such as ransomware.
- Get real-time, actionable insights about changing your security posture.
- Optimize and automate responses based on risk.

servicenow.

For more, visit the ServiceNow Customer Success Center

Systematically harden the digital attack surface

Integrate IT, risk, and security data and systems to improve visibility into vulnerabilities, enable risk-based prioritization, and streamline mitigation. Take these actions to prepare your organization to deliver and support this capability:

Prepare to integrate IT, risk, and security information.

- **Ensure CMDB health.** Your teams will need accurate configuration items (CIs) in the ServiceNow® CMDB to add business context and risk information to vulnerabilities. This information helps prioritize and assign ownership for remediation.

Plan for greater collaboration between security operations and IT.

- **Identify opportunities to streamline vulnerability remediation.** Determine what groups handle patching what systems so you can set up automated rules for assigning remediation activities. Work with security and IT personnel to identify pain points in the current process that you can address with improved collaboration.
- **Reinforce expectations for collaboration between security operations and IT.** ServiceNow provides security and IT teams a single place to analyze security data, triage vulnerabilities, assign remediation, and manage IT changes. Align incentives and workflows with the two teams so they can take advantage of these new capabilities.

Standardize and improve risk-based vulnerability management.

- **Update your organization's current vulnerability management processes to enable faster workflows and automation.** ServiceNow will allow you to streamline assigning and managing vulnerability remediation. Define and document how to assign ownership for remediation and processes for requesting and approving exceptions. Look for opportunities to improve processes to take advantage of greater data integration and automated workflows.
- **Develop policies to define remediation requirements.** For example, a policy may require you to patch vulnerabilities that are related to a critical business priority or above a certain risk threshold. You can also use these policies to automate remediation processes.

Expand your security talent pool to make sure you can keep up with demand.

- **Consider nontraditional profiles when filling open security roles.** While unpatched vulnerabilities cause most major breaches, many companies can't keep with up basic patching due to staffing shortage. Alternative staffing approaches include merging network and security operations teams, recruiting IT personnel, or looking at nontraditional populations, such as military veterans, to staff your security program. Plan to invest in training to add cybersecurity to their skill sets.

Practitioner insight

Get leadership buy-in for long-term investment in improving your security hygiene. There is no quick fix to combat cyber threats, so be certain your leadership supports a sustained effort. Include security posture in the executive risk and compliance dashboards.

Optimize and orchestrate security operations

Use Security Orchestration and Automated Response (SOAR) to help reduce the burden on overworked security staff by automating areas like threat and vulnerability management, incident response, threat intelligence analysis, and cyber-risk mitigation. Take these actions to prepare your organization to deliver and support this capability:

Build automation in phases.

- **Start with quick wins.** Get input from the security operations team to identify pain points or inefficiencies that orchestration and automation can address. Map out a process-automation roadmap, starting with processes that will provide the greatest time savings returns and only require a low level of effort to implement.
- **Build flexibility and time to iterate into the automation roadmap.** As your teams implement the initial roadmap, they're likely to identify additional processes to automate and, possibly, additional tools and systems that you may want to integrate. If your budget isn't flexible, it will hurt your organization's ability to fully realize the value of your investment.

Help your teams adjust to new ways of working.

- **Anticipate team training needs.** Your security team may need training on how to best use new dashboards and automate detection, triage, and response.
- **Carefully manage change.** Most security organizations are already subject to high turnover, so consider overinvesting in change management. Take input from your security team on proposed changes and understand that productivity, and even some operational metrics, may dip slightly for a short time during adjustment.
- **Identify and support changes to how your teams use data and tooling to manage security.** Create incentives for your security team to identify new ways of working, including learning how to automate workflows for assigning, coordinating, and prioritizing incident remediation.

Consider the implications for your security staffing model.

- **Take advantage of security orchestration and automation to lessen the burden on senior security staff.** The shortage of skilled security professionals has increased the workload on existing staff, causing many organizations to turn to more junior personnel. Use automation and intelligent workflows to support junior analysts, freeing up time for senior staff to support processes that require more experience and judgment.

Respond with agility to evolving cyber threats

Develop automated playbooks and use systems integrations for faster and more effective incident response, improved incident analysis, and richer reporting. Take these actions to prepare your organization to deliver and support this capability:

Update your organization's incident response strategy.

- **Consider an incident response framework to help develop your organization's processes.** Frameworks such as NIST 800-61, CERT (CSIRT), and ISACA provide a great starting point for building out your organization's incident response plan across the four main stages of incident response: preparation; detection and analysis; containment, eradication and recovery; and post-incident activity.
- **Plan tabletop exercises to focus on preparation and response.** Assume that preventative controls won't be enough and that, one way or another, an attack will get through. Because of this, it's important to practice your response. Develop tabletop exercises that bring cross-functional teams together to understand your current response processes and identify opportunities for improvement. Keep an eye out for ways to improve efficiency through better data sharing and automation.
- **Build post-mortems into your organization's incident response process.** Analyze incidents after they occur to learn from them and improve response capabilities. Triage postmortem analyses and focus more on incidents where existing controls failed.

Practitioner insight

ServiceNow supports developing automated Security Incident Response playbooks. Resist the temptation to lift and shift existing processes when building your playbooks. Instead, and take the opportunity to update your incident response processes to take advantage of automated workflows and greater data integration.

Communicate the enterprise security posture and cyber risks.

- **Cultivate senior leadership support.** A high-profile security incident, such as a ransomware attack, will force your executives to make some very tough decisions. Develop dashboards to make sure your executives are well-informed about cyber risks and their cost and time of recovery.

Invest in threat prevention as well as response.

- **Expand your SecOps team's remit to include actively preventing threats.** Use "threat hunters" and other security analysts on the SecOps team to identify and neutralize threats.
- **Adequately fund emergency ops.** This team is responsible for mobilizing staff, activating response plans, and managing time-critical incident management and response activities for major breaches. Many enterprises underfund emergency ops despite the cost of these breaches.

Practitioner insight

Don't over-focus on cyber crises at the expense of your broader incident response program. Organizations that focus disproportionately on cyber crises frequently underinvest in their broader incident response program, making it more likely that small incidents go unaddressed and grow into bigger problems.