A Practical Guide to Efficient Security Response

The Essential Checklist

servicenow

Start

The Critical Challenges to Information Security

Data breaches constantly threaten the modern enterprise. And the risk continues to grow: **In 2015, the total number of identities exposed via data breaches increased 23%, to 429 million.**[1] Time-to-compromise is now measured in minutes, and data exfiltration happens in days.[2]

Worse still, detecting a breach can take months, with a median of 201 days to discovery.[3] Unable to quickly respond, organizations risk exposing valuable data and confidential information. The recovery process can be incredibly expensive and the damage to the business reputation incalculable.

Why does it take so long to identify and respond to threats? Security and IT professionals point to one primary culprit: the disconnect between security and IT tools. Traditional approaches hamper efficient incident-response coordination across organizations:

- **Numerous, disjointed tools** cumulatively generate thousands of unprioritized alerts
- **Lack of automation** leads to hours wasted on manual processes
- **Organizational opacity** means the right contacts are hard to track down
- **Multiple, unsecured data sets and security runbooks** make it impossible to ensure everyone is on the same page

Beyond inefficiency, the manual processes associated with traditional security responses trigger other issues. Spreadsheets quickly become out-of-date, and emails frequently end up in the wrong inboxes. In both scenarios, defining and tracking performance metrics can be extremely difficult. And all too often, these manual processes force highly trained employees to focus on low-level tasks, resulting in high turnover.

Coordinating incident reponse across the organization is the biggest challenge for most enterprises.[4]

[1] Symantec Internet Security Threat Report, 2016
[2] 2016 Verizon Data Breach Investigations Report
[3] Ponemon Institute, 2016 Cost of a Data Breach Study
[4] ESG, Status Quo Creates Security Risk: The State of Incident Response

The Essential Security Operations Solution Checklist

How would you rate your organization's ability to respond to security threats and vulnerabilities? Use this short checklist to evaluate how the right security operations solution could support your enterprise.

Did you know the right solution could allow your security team to:

- **Rely on a single source of truth across security and IT?**
  All responders need access to the latest data. A shared system allows security and IT teams to coordinate responses.
- **Prioritize all security incidents and vulnerabilities?**
  The best way to handle an overload of alerts is to automatically prioritize them based on their potential impact to your organization. Analysts need to know exactly which systems are affected and any subsequent consequences for related systems.
- **Automate basic security tasks?**
  All vulnerability and incident data is pulled into a single system. By correlating threat intelligence data with security incidents, analysts have all the information they need to protect your business.
- **Integrate with the configuration management database (CMDB)?**
  With CMDB integration, analysts can quickly identify affected systems, their locations, and how vulnerable they are to multiple attacks.
- **Ensure your security runbook is followed?**
  Workflows are critical for ensuring adherence to your security runbook. Pre-defined processes enable Tier 1 personnel to perform actual security work, while more experienced security professionals focus on hunting down complex threats.
- **Quickly identify authorized approvers and subject matter experts?**
  It must be easy to identify authorized approvers and experts, and quickly escalate issues if service level agreements (SLAs) aren't met — while ensuring the security of "need to know" data.
- **Collect detailed metrics to track SLAs, drive post-incident reviews, and enable process improvements?**
  You need to be able to track SLAs and collect data for reviews. The security operations solution automatically generates complete, up-to-date timelines of all actions and approvals.

In short, the right solution enables efficient response to incidents and streamlines the remediation process. It also lets you clearly visualize your security posture. For the CISO and security team, it's an integrated response platform that answers the question, **"Are we secure?"**

Comparing Security Response Approaches: Traditional Versus New

When a high-profile vulnerability arises, there are several ways an enterprise can react. Compare the response of an organization using a traditional, disjointed approach with one using an integrated response platform.

Traditional Approach:

Once a threat is uncovered, the security team scrambles to address it. The CISO hears about it and wants to know if the organization is affected. The team races to assess systems and determine who needs to approve any emergency patching. Many processes are manual, so analysts struggle to quickly gather the information required to provide the CISO with an accurate assessment of the impact. Critical systems may be vulnerable, putting the business at risk of a data breach.

< BACK

NEXT >

Comparing Security Response Approaches: Traditional Versus New

A New Approach:

In comparison, the organization using an integrated response platform can immediately respond to the vulnerability. It quickly kicks off the following steps:

- First, data is automatically pulled into the security operations system from their vulnerability management system. Security analysts quickly ascertain this is a critical vulnerability, with a high probability of complete loss of data confidentiality, integrity, and availability if exploited. Pertinent information to remedy the situation is immediately made available to the security team.
- Then, hundreds of vulnerable items are correlated with the CMDB and prioritized based on business service impact, asset criticality, and the risk score of the vulnerability.
- Built-in workflows take care of the next steps, ensuring analysts follow the security runbook. The system automatically triggers requests to approve emergency patches for critical vulnerable items. An additional scan verifies the fixes.
- Once the critical items have been patched, security and IT can create a plan to address the remaining vulnerable items using a single response platform. Automated workflows help security analysts route change requests to the right people within IT. The common platform ensures they share information on a secure "need to know" basis, eliminating the need to memorize the organizational structure.
- Now, the CISO is briefed, and the security operations solution automatically generates a post-incident review with accurate metrics. The CISO is happy, and the organization is secure.

An innovative security operations solution is essential for responding to the increasing number and sophistication of today's threats and vulnerabilities. With complete visibility into disruptive issues, security and IT teams can easily coordinate with all stakeholders to investigate and remediate issues.

What's Next?

Efficient response to security incidents is among the biggest challenges for Information Security Leaders. That's why choosing an integrated response platform is so important.

ServiceNow Security Operations is the most innovative security response solution. It provides a single platform for responding to incidents and vulnerabilities across security and IT, and it can augment your enterprise's incident response capabilities with additional threat intelligence.

With a great security operations solution in place, your team can make threat and vulnerability identification, remediation, and coordination efforts more efficient. Automation permits responders to focus on more complex problems more effectively. And you have accurate data at your disposal to continuously assess your organization's security posture.

Learn more about transforming your security operations.

< BACK

servicenow

About ServiceNow

ServiceNow is changing the way people work. With a service-orientation toward the activities, tasks and processes that make up day-to-day work life, we help the modern enterprise operate faster and be more scalable than ever before. Customers use our service model to define, structure and automate the flow of work, removing dependencies on email and spreadsheets to transform the delivery and management of services for the enterprise. ServiceNow enables service management for every department in the enterprise including IT, security, human resources, facilities, field service and more. We deliver a 'lights-out, light-speed' experience through our enterprise cloud – built to manage everything as a service.

Learn more about transforming your security operations.
Follow us on Twitter or visit www.servicenow.com.

SN-EB-SecOpsGuide-082016