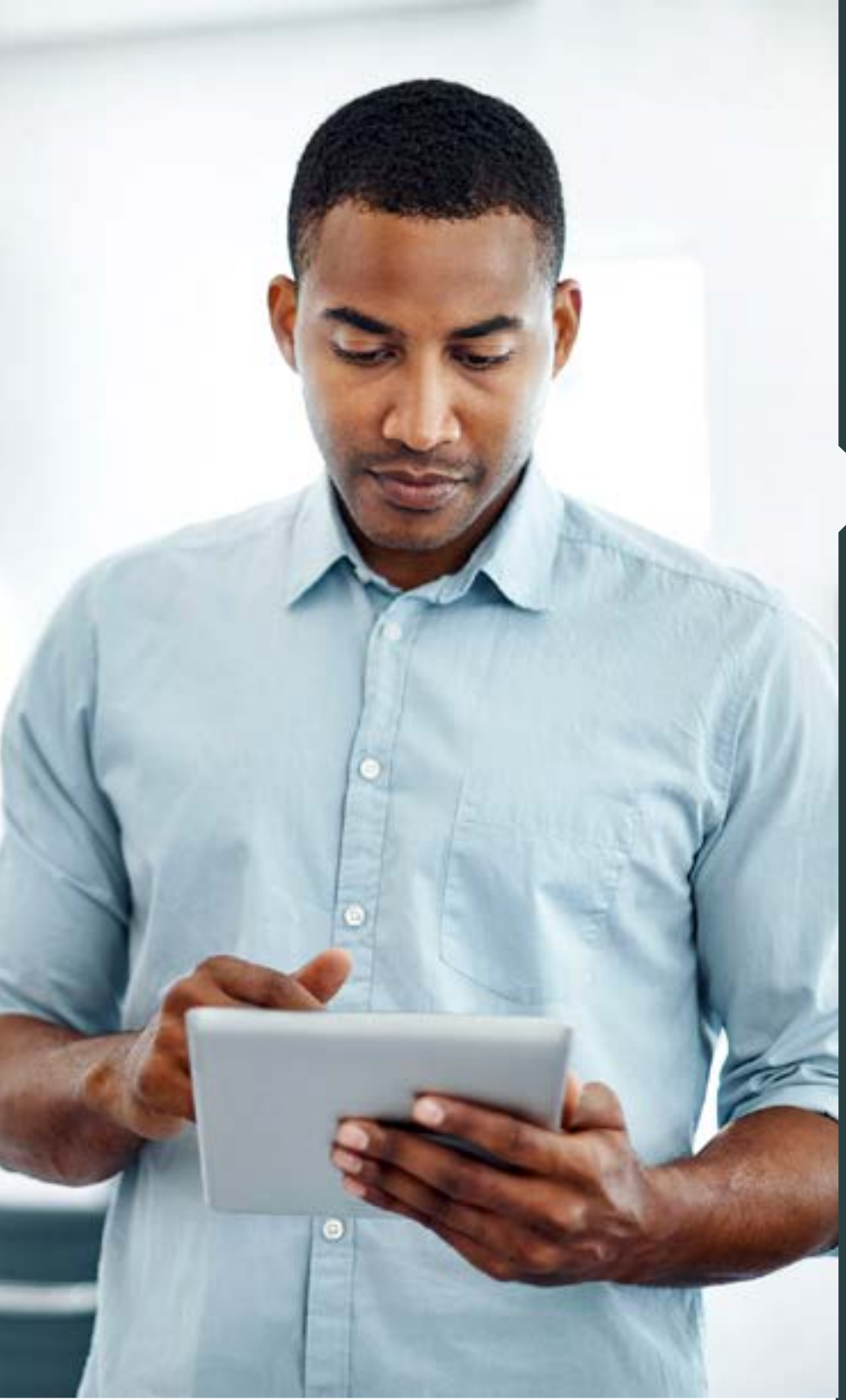

servicenow

Implementing agile security responses

The essential checklist for financial services institutions

START

Critical information security challenges facing the financial services industry

Cyberattacks against financial services institutions are escalating – increasing by more than 70% since 2017.[1] Time-to-compromise is now measured in minutes, and data exfiltration happens in days.[2]

And the stakes are rising higher. The cost of a data breach now averages $3.92 million, a 12% increase over the last five years.[3] Delayed responses put valuable data and confidential information at risk of being exposed. 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 institutions:

- **Numerous, disjointed tools** cumulatively generate thousands of unprioritized alerts
- **Lack of automation** leads to hours wasted on manual processes
- **Organizational opacity** and difficulty tracking down the right contacts
- **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 Spreadsheets quickly become out-of-date, and emails frequently end up in the wrong inboxes.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 response across the institution is the biggest challenge for most enterprises.[4]

1 HTF Market Intelligence, “Global Cybersecurity in Financial Services Market (2018-2023),” 2019
2 Verizon, “2018 Data Breach Investigations Report,” 2018
3 IBM Security and Ponemon Institute, “2019 Cost of a Data Breach Report,”2019
4 Enterprise Strategy Group, “Status Quo Creates Security Risk: The State of Incident Response,” 2016

The essential security operations solution checklist

How would you rate your institution'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.
Do your security operations:

- **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.
- **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.
- **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?**
  Analysts need critical information in seconds to respond to security threats. Automating manual tasks like threat enrichment can help with consolidating the response process quickly.
- **Respond faster with orchestration?**
  Your security operations should allow you to take action from a single console that can interact with other security tools to speed up remediation.
- **Ensure your security runbook is followed?**
  Workflows are critical for ensuring adherence to your security runbook. Security playbooks 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 performance, drive post-incident reviews, and enable process improvements?**
  You need to be able to track team performance and collect data for reviews. Metrics captured should provide trend data to support improvements.

In short, the right solution enables efficient response to incidents and vulnerabilities and connects security and IT teams. It also lets you clearly visualize your security posture. For the chief information security officer (CISO) and security team, it's an integrated security orchestration, automation, and response platform that answers the question, "Are we secure?"

As the volume of cyberattacks has grown, patching vulnerabilities in a timely manner has become increasingly difficult. Among the biggest problems for financial services institutions: lack of a common view of applications and assets across security and IT teams (82%) and difficulty prioritizing what to patch first (70%).[6]

Comparing security response approaches: traditional versus new

When a high-profile vulnerability arises, there are several ways an enterprise can react. Compare the 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 and how the institution 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. Manual coordination between teams can take days[5], leaving critical systems vulnerable and putting the business at risk of a data breach.

[5] Ponemon Institute, "Today's State of Vulnerability Response: Patch Work Requires Attention," 2018

[6] ServiceNow, "The State of Vulnerability Response in Healthcare: Patch Work Requires Attention," 2019

Every second counts when security is breached. We help you prioritize and remediate vulnerabilities and security incidents faster, replacing manual tasks with automated security orchestration.

A new approach

In comparison, the institution using a security orchestration, automation, and response platform can immediately respond to the vulnerability. It quickly kicks off the following steps:

- **Assessment:** First, scan data is automatically pulled into the security response system from a vulnerability management system. This is correlated with external sources such as the National Vulnerability Database and their internal asset database to prioritize vulnerabilities by both the potential risk of the vulnerability itself and the impact to the institution's services.
- **Notification:** Then, a pre-built workflow notifies the security team of a critical vulnerability impacting high-priority assets. Analysts can review information about the vulnerability and the items at risk in a single console.
- **Response:** In parallel, a workflow starts the response process. The system automatically triggers requests to approve emergency patches for critical vulnerable items. Once the patches have been implemented, an additional scan verifies the fixes before the vulnerability can be marked closed.
- **Mitigation:** Now that the critical items have been patched, security and IT can create a plan to address the remaining vulnerable items using a single response platform. Change requests are automatically routed to the right people within IT, eliminating the need to memorize the organizational structure. The common platform ensures they share information on a secure "need to know" basis.
- **Report:** 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 institution is secure.

What's next?

The financial services sector will continue to accelerate its digital transformation, moving more of its services online and harnessing technology to make operations more agile. Changes are opening the door to new vulnerabilities and security threats; responding deftly and efficiently is a top priority for information security leaders. That's why choosing a security orchestration, automation, and response platform is so important.

ServiceNow® Security Operations is designed to help security teams respond faster and more efficiently to incidents and vulnerabilities. Built on the Now Platform™, Security Operations uses intelligent workflows, automation, and a deep connection with IT to streamline security response.

With a great security orchestration, automation, and response 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 instead of on manual tasks. And you have accurate data at your disposal to continuously assess your organization's security posture.

Learn more about transforming your security operations.

servicenow

Transform your security operations to improve your resiliency.

Discover more about our comprehensive approach to managing, mitigating, and remediating vulnerabilities for financial services institutions.

LEARN MORE

Learn how companies like yours use Security Operations to respond to threats faster.

GET DETAILS

About ServiceNow

ServiceNow (NYSE: NOW) is the fastest-growing enterprise cloud software company in the world above $1 billion. Founded in 2004 with the goal of making work easier for people, ServiceNow is making the world of work, work better for people. Our cloud-based platform and solutions deliver digital workflows that create great experiences and unlock productivity to approximately 5,400 enterprise customers worldwide, including almost 75% of the Fortune 500. For more information, visit www.servicenow.com.