servicenow

Now on Now: Automating Security Operations

How automated workflows reduced our threat response time by 20%

Table of Contents

Security landscape

Data breaches and other security incidents put not only a company's own information, business operations, and reputation at risk, but also those of its customers and partners. According to the Ponemon Institute, 48% of businesses say that they have had a breach in the last two years[1]. Of those breached, 60% said it was due to a vulnerability for which a patch was available but not applied. Moreover, the cost and potential damage caused by a breach grow quickly with time as the number of impacted records increases. On average, it takes 31 hours to contain a cyber-incident[2]—time that an attacker can use to go deeper into the infrastructure and do greater damage.

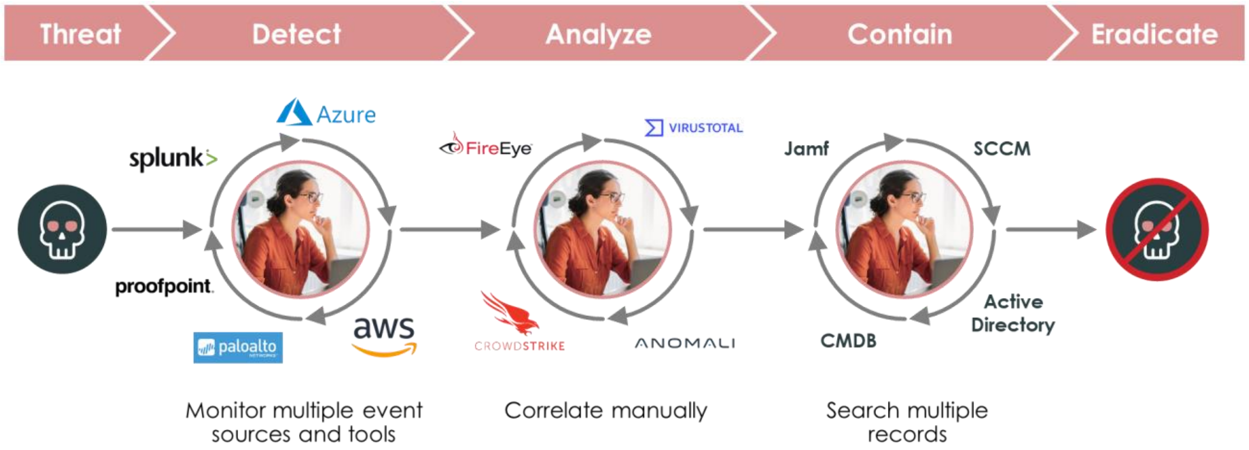
To address this challenge, the ServiceNow IT Security team turned to our own Security Incident Response product. Built on the Now Platform®, ServiceNow Security Incident Response automates workflows, prioritizes and accelerates triage, and provides actionable insight for continual improvement.

[1] Ponemon Institute 2019: Costs and Consequences of Gaps in Vulnerability Response
[2] Crowdstrike, 2019

Security incident response at ServiceNow

Previous approach

Prior to implementing ServiceNow Security Incident Response, we used a customized version of ServiceNow IT Service Management (ITSM).



- **Detect** – In order to detect a threat, analysts would swivel chair and individually monitor multiple event sources and security tools.
- **Analyze** – In order to properly investigate, analysts would again swivel chair to all our investigation tools to gather and manually correlate data.
- **Contain** – During the containment phase, analysts would swivel chair yet again to search multiple sources of information.
- **Eradicate** – Ultimately, we would contain the threat, but not without a great deal of extra time, effort, and expense.

Challenges

There were several shortcomings with the ITSM-based approach:

- **Swivel chair delays** – Having to monitor multiple tools and gather data from numerous systems and sources wasted precious time.
- **Process inefficiencies** – Not only was the overall process inefficient, but the lack of standardized processes impeded our global coordination and response.
- **Reporting** – In order to provide updates and reports to executives, auditors, and insurers, data had to be manually gathered from multiple sources and reconciled. Inevitable data inconsistencies did not instill confidence in the evidence or the Security program.
- **Agent experience** – Our security analysts were becoming increasingly frustrated with the inefficiencies, the perpetual swivel chair, and the wasted time.

Implementing ServiceNow Security Incident Response

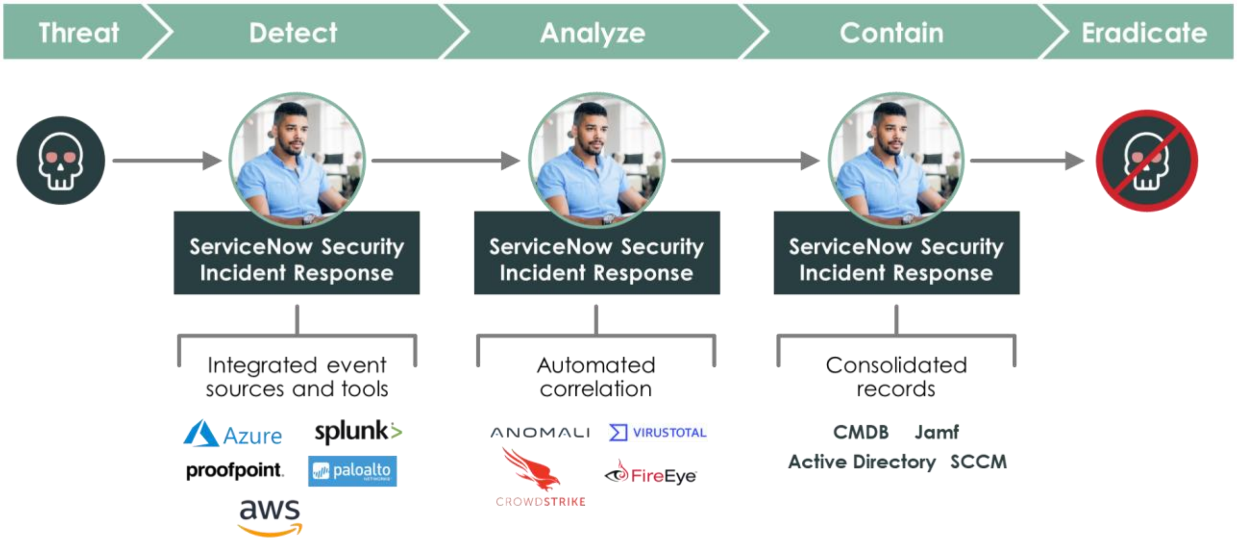
To transform our security program, we implemented an out-of-the-box version of ServiceNow Security Incident Response and integrated our many security tools. We built a knowledge base of playbooks and procedures to standardize processes globally. We then automated workflows and enrichment data.

Next, we optimized operations using ServiceNow Performance Analytics to measure our progress and make improvements to processes and enrichment data. As Customer Zero, we install and use the latest product releases as soon as they are available internally. This enables us to provide feedback to our product teams before products are released to customers.

The threat landscape is constantly changing, so we continually enhance our playbooks and procedures, and add new workflows based on new use cases.

Today's streamlined, automated process

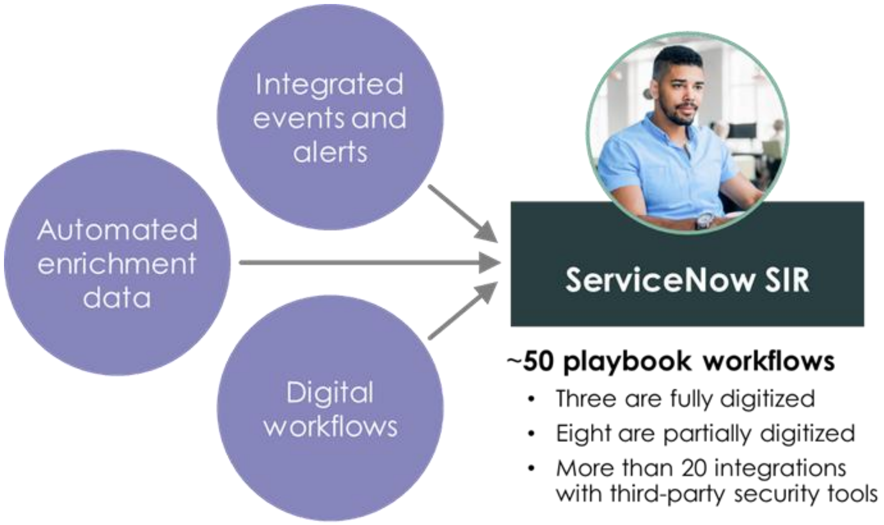
Our new process is far more automated and efficient than the previous ITSM-based approach.



- **Detect** – Now, when a threat is detected, all alerts and detections from our security tools are rolled up automatically into Security Incident Response. Analysts now monitor only one screen for notifications, rather than multiple screens and tools.
- **Analyze** – Information is correlated and enriched within the application. Observables are automatically uploaded to VirusTotal for analysis, and the results are placed in the incident record. When an analyst is alerted to an incident, all the data they need is in the record.
- **Contain** – Integrations aid in faster incident containment. Analysts can clearly see the scope of the incident, where they need to contain it, and which systems need to be isolated. Employees potentially impacted by the incident are notified of any actions they need to take, such as resetting their password.
- **Eradicate** – As a result of these process and product improvements, threats are now contained quickly and effectively.

The single pane of glass

Integrating everything within Security Incident Response gives our analysts a single pane of glass to monitor, analyze, and respond to threats. Events, alerts, and automated enrichment data are at their fingertips, and automated workflows offload tedious, manual effort.


Integrated events and alerts
Automated enrichment data
Digital workflows
ServiceNow SIR
~50 playbook workflows
• Three are fully digitized
• Eight are partially digitized
• More than 20 integrations with third-party security tools

As of Jan 2020, we had created approximately 50 playbook workflows and continue to create new ones. These workflows walk analysts step-by-step through the incident handling process. Three of these playbooks are fully digitized, and eight are partially digitized. In addition, more than 20 third-party security tools are integrated into the SIR app.

Benefits

Our fully integrated, highly automated solution has delivered considerable benefits:

- **Faster response** – Threat response time has been cut by 20%.
- **Reduced risk** – Faster response time means reduced risk, not just for ServiceNow, but for our customers.
- **Productivity savings** – Identifying and removing redundancies offloads work from our staff and improves productivity. Productivity savings for 2019 were $470K.
- **Improved analyst experience** – Eliminating the swivel chair and automating mundane work enables analysts to spend more time on value-added work. We’ve seen an 80% improvement in job satisfaction. And because of our standardized playbooks and automated workflows, we can train new analysts faster.
- **Enhanced reporting** – Thanks to built-in analytics and dashboards, we can now provide timely, accurate reports to executives, auditors, and insurers, and respond quickly and confidently to any questions.

Case study: phishing test campaign

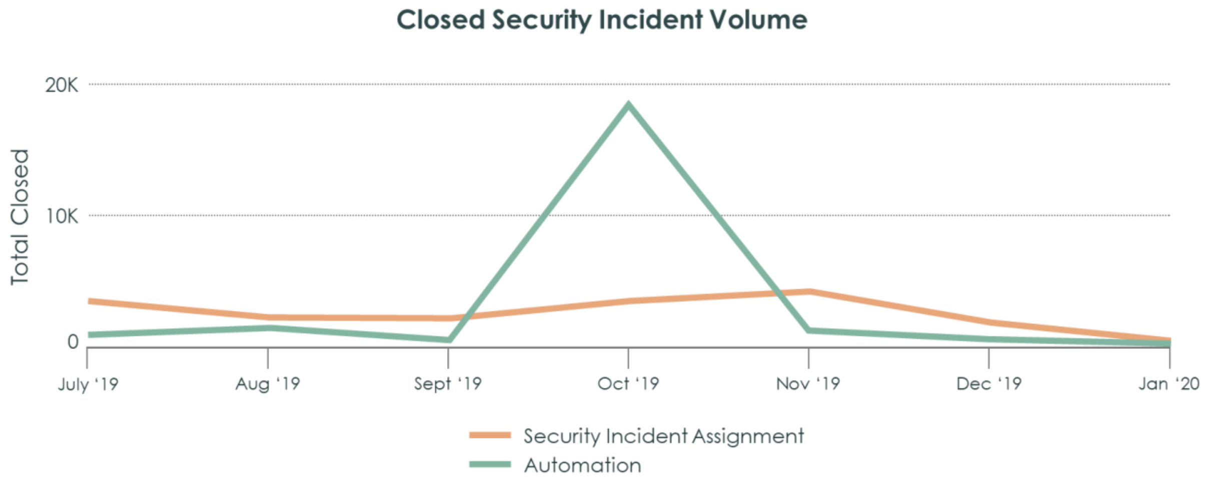
Our phishing test campaign is a great example of the value that automation has brought to the ServiceNow Security organization.

Like many companies, ServiceNow is required to test employees on their ability to spot and report phishing emails. Our security organization regularly sends out phishing emails to employees. When employees report them—whether by clicking the Report Phish button in Outlook or forwarding the email to the security team—their response is captured by the system.

Before we automated workflows, a security analyst would have to process the notification manually, respond to the employee, and close the ticket—a time-consuming process and a poor use of an analyst's time.

Now, the entire process is fully automated. When an employee responds correctly to a phishing test, the system sends them an email acknowledging receipt. A half hour later, the system sends the employee a second email telling them that they had correctly identified a phishing attempt and thanking them for keeping ServiceNow safe. The system then closes the ticket.

The following graph illustrates the positive impact automation has on our security organization.



The orange line represents the work of security analysts. The green line is work done by the system. In October, the Security organization sent out roughly 20,000 phishing emails to ServiceNow employees. Had the process not been automated, the huge spike in activity would have quickly overwhelmed our Security team.

Key takeaways

- **Target automation** – Integrate all security tools; prioritize use cases, processes, and procedures; and then automate workflows and enrichment data ingestion.
- **Focus on efficiency** – Focus on those areas where automation will drive the greatest efficiency to the team and the response processes.
- **Follow through with maturity** – Finally, continually measure the program to validate that automation is achieving the desired results and make any necessary adjustments.

To learn more

- Explore the ServiceNow Security Operations products web page.
- Browse the Community Forum for Security Operations to get tutorials and insights on a variety of security-related topics.

About ServiceNow

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 for employees and the enterprise. For more information, visit www.servicenow.com.

Now on Now is about how we use our own ServiceNow solutions to work faster, smarter, and better. With Now on Now, we're achieving true end-to-end digital transformation. To learn more, go to www.servicenow.com/nowonnow.