

Security Streamlined

A Comprehensive View for Federal Agencies

The average cyber threat lives undetected on a network for an average of 201 days, with each identified breach costing agencies an estimated \$4 million. But the damage goes beyond the direct financial and security costs of compromised data and systems—public confidence suffers as well.

Agencies are focused on reducing time for identifying threats as a front-line strategy for reducing exposure, damage, and costs associated with breaches. And while 70% of cyber pros say they can monitor streams of cybersecurity data in real time, fewer can analyze the data with similar agility, leaving data in danger.

This raises the questions: What else are agencies missing? How can they gain the real-time identification and response capabilities that transform cybersecurity operations?



Not Getting the Full Picture

Because security teams are typically disconnected from the rest of IT, they lack an understanding of the potential agency impact from a security incident or vulnerability. This separation makes it impossible to get a complete picture of the severity of an issue or to know which issues to address first.

For example, if an agency simultaneously receives two security alerts that look identical, which one should they work on first? When security is working in isolation, they choose which issue to address at random. But if the security analyst knew that one was tied to an electronic lunch menu and the other to personally identifiable information (PII), the PII issue would be prioritized. When security and IT are disconnected, agencies are unable to rapidly and accurately assess and prioritize according to the magnitude of the threat.

Overwhelmed with the influx of threats, security teams take a reactive posture—spending excess time and resources analyzing instead of solving the problem. Security analyst resources are stretched to the limits, further complicating the situation.

Lastly, most agencies are unable to quantify the cost of a cyber incident because teams lack visibility into what it costs the agency to mitigate the threat and restore the system.

Switching Up the Status Quo

As the stakes rise, agencies are focused on transforming their cybersecurity posture—rapidly and definitively. Security teams seek solutions that offer a single place for response, where automation powers faster time to resolution and a more definitive view of an agency's actual security status can be found. By integrating critical security and IT data, agencies can set the foundation for addressing—and preventing—future incidents.

As agencies gain more intelligence on known threats, teams can respond more quickly. While complete automation is the ultimate goal, automating even basic tasks, such as handoffs from one team to another or automatically importing more information about a security incident, gives teams more time to focus on proactively defending future incidents.

How can agencies achieve these goals to drive short- and long-term impact?

Seeing the Secure Federal Future

ServiceNow[®] Security Operations provides a much-needed single point of visibility and control to drive faster security response time and facilitate integration of security and IT data. The solution follows the National Institute of Standards and Technology (NIST) incident handling guide, instructing agencies on analyzing incident-related data and providing an appropriate reaction to mitigate incidents.

Security Operations prioritizes threats based on severity and the impact to the agency, providing security teams the information they need to act quickly. In addition, the Vulnerability Response module efficiently informs which vulnerabilities to remediate first based on potential impact.

Dashboards provide security teams with an in-depth look at which critical services may be affected after an attack. This is also where security and IT can communicate in real time to collaborate on incidents and execute an action plan, coordinating a response strategy across services.

Now, with basic tasks automated and security and IT working together, teams have more time to proactively defend an agency from attack as they work to meet compliance and security goals.

The Security Operations suite provides the visibility CIOs are striving to achieve through the Federal Information Technology Acquisition Reform Act (FITARA). And thanks to the clear view across systems, agencies can better quantify the threat impact. The ServiceNow platform also has Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB) certification for agencies to automate basic tasks and focus on IT modernization.

The Foreseeable Future – Agencies Take Action

Threats become more sophisticated as technology advances. Agencies need visibility over their services not only to mitigate threats, but to proactively defend their networks. ServiceNow is evolving the federal service delivery experience and providing agencies the tools they need for a secure future.

For more information, visit: <http://www.servicenow.com/products/security-operations.html>.

¹Ponemon Institute, 2016 Cost of a Data Breach Study

²<https://www.meritalk.com/study/go-big-security/>

