servicenow

Now on Now: Accelerating Security Operations

How automation speeds up incident response and helps ServiceNow retain scarce security talent

START

"When our analysts investigate a security incident, they have all the data they need in one place. Our platform provides the relevant vulnerabilities and patching cycles, problems (PRBs) and remediation projects, CMDB data, threat intel, and many other types of valuable data that now all tie together to give us a full picture."

Yuval Cohen
ServiceNow Chief Information Security Officer

Introduction

ServiceNow takes cybersecurity seriously. Our reputation depends on it. Our customers rely on us to provide a highly-secure cloud environment for their mission-critical services and data, and we're committed to delivering the security they demand. That's why we have a single-minded focus on leading-edge security technology and expertise.

It's also why we use ServiceNow® Security Operations for security incident response and vulnerability response. In fact, we have always leveraged ServiceNow to strengthen and accelerate our security processes–even before we had commercially available security products.

Meet Bob Smith[1]

Bob Smith (not his real name) runs our security incident response team, both for our cloud and internal corporate environments. Bob and his team are instrumental in keeping our customers and business safe, successfully fending off attacks—ranging from phishing emails to sophisticated multi-vector assaults—and everything in between.

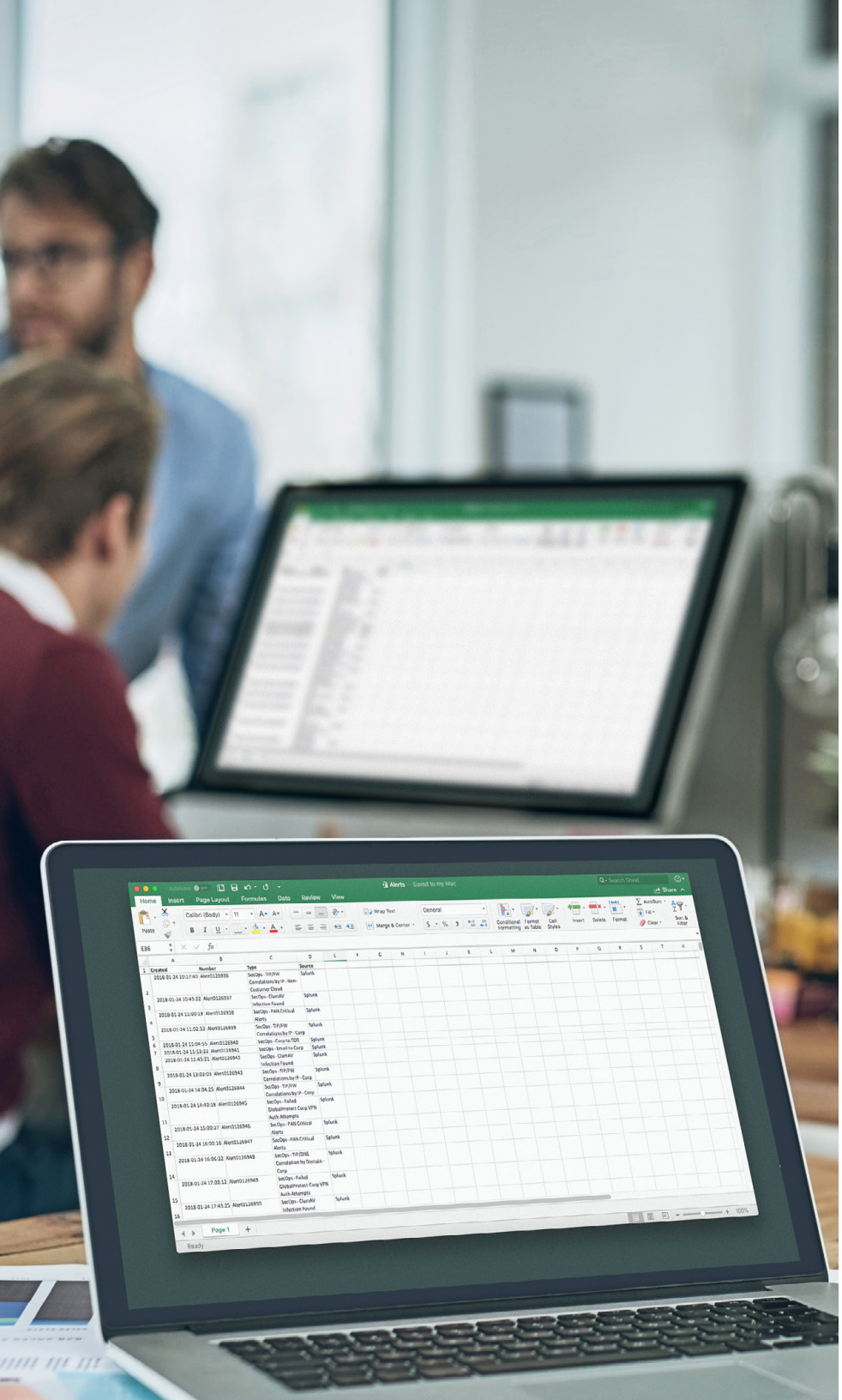
For Bob, better security started with automating our incident response processes. "Right from the outset, we used ServiceNow for security incident response. Since we didn't have a commercialized solution at the time, we adapted our ITIL Incident Management application and built other custom ServiceNow apps to create an integrated security incident response environment. Now that we have a security operations product, we've transitioned to that—and we're seeing big benefits. But we laid the foundation long before."

[1] We've changed Bob's name to protect his identity from hackers.

Why manual processes don’t work

“Think about how most companies manage security incident response. They rely on emails and spreadsheets. Someone reports a potential incident, or a security information and event management system sends an email alert. This goes into a giant spreadsheet along with hundreds of other alerts, and somehow, you’re supposed to use this to drive things forward,” complains Bob.

“For example, how do you track status? Yes, you can add a column to the spreadsheet and update it manually, but that takes time–and people make mistakes or forget. And, you can’t have a single spreadsheet for an entire team. It just isn’t practical. Try to edit a spreadsheet when 15 other people are updating it at the same time, and you’ll see what I mean.”



Lack of visibility and prioritization

"You end up with each security analyst having their own spreadsheet. Now, you've lost visibility," says Bob. "There's no central place for all of your security alerts. That creates huge problems. For example, how do you prioritize alerts, so you know what to work on first? Again, you can put this into the individual spreadsheet that contains the alert, but there's no overall prioritized queue where you can pick things off the top. And, at the end of shift, handover is a nightmare. It takes the new analyst an hour or more reading spreadsheets to figure out what's going on."

Cutting and pasting instead of investigating

However, this pales in comparison with the effort of analyzing each alert. Bob reveals, "We get 300 to 400 alerts every day. 95% are false positives rather than real incidents, but we have to investigate each one. That means chasing down contextual information from lots of different sources–for example, threat feeds, public tools like Shodan and VirusTotal, and detailed logs from the system that raised the alert. If we had to go and retrieve all of this information manually, our investigation times would skyrocket. And, of course, you then have to put all this data in a spreadsheet or document, which means that people wear out their keyboards cutting and pasting."

How ServiceNow accelerates security incident response

With the Security Incident Response application of ServiceNow® Security Operations, we automate alert processing. When a monitoring system sends an alert, ServiceNow automatically prioritizes it based on the type of alert. ServiceNow also automates retrieval of contextual information, attaching data from monitoring tools, public security tools, and threat feeds directly to the incident.

According to Bob, "We want to bring data to the analyst, rather than having the analyst chase the data. That way, they can focus on investigation, instead of wasting time manually collecting the data they need. In fact, we process alerts six times faster this way than if we did everything manually."

Automated workflows also help us to drive efficiency. Bob points to an example: failed authentications. "When there's an authentication failure, ServiceNow automatically contacts the user asking them if they tried to log in. Once they confirm, ServiceNow closes the alert. We only open a security incident if the user didn't try to log in. That's a huge timesaver. Instead of wasting our analysts' time, it's all handsfree. And, that's only one example. For instance, we also use automated workflows to handle phishing email reports."

Making the most of scarce security staff

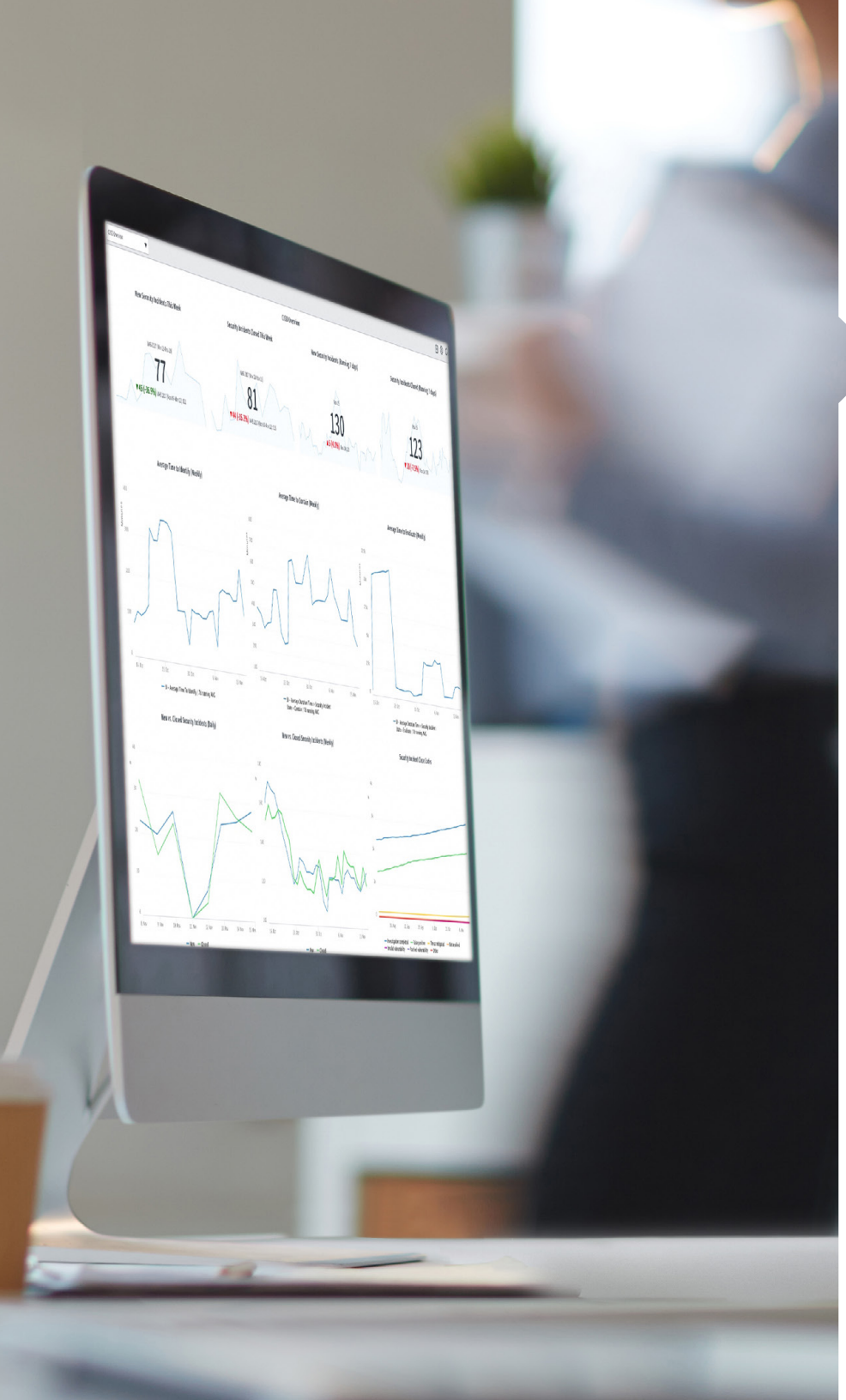
For Bob, that time saved is critical–and not just because we respond more quickly to security incidents. He explains, "ServiceNow is a rapidly growing company, so we don't face as many budgetary constraints as some other security organizations. However, there's enormous competition for experienced security analysts. We can't just hire more people. We can't just hire more staff, given that the security industry is facing a talent shortage of 1.8 million people within the next four years[2]."

"We need to get the most out of our existing team and automation lets us do that. Yes, we're saving money–conservatively, more than $400,000 a year–but the real headline is that we've increased the number of incidents each analyst can handle by 50%."

Attracting and retaining security expertise

Automation isn't just increasing the productivity of our security analysts. It's also making them happier. "Giving our team a great work experience is incredibly important. If you're spending all of your time cutting and pasting data, you're going to get frustrated," says Bob. "By automating these mind-numbing tasks, we're freeing up time for high-value, fulfilling activities. Our analysts want to do interesting work, whether that's investigating incidents or writing knowledge base articles that help us respond better to future incidents. That dramatically increases job satisfaction, so that we attract and retain the best talent. Given the huge amount competition out there, we need to be that preferred place to work."

[2] Frost & Sullivan 2017 Global Information Security Workforce Study



From customized to off the shelf

As stated previously, Bob and his team started out with a custom ServiceNow app. What benefits have they seen now that they are using ServiceNow® Security Incident Response?

One security analyst on Bob's team talks about moving from ITIL incidents to security incidents. "When we used ITIL incidents, it was very basic. We could only put in the category and subcategory. Everything else had to go in the incident notes. That made it hard to find the information we needed or to track the state of the ticket. Now, information is in searchable fields, and we've got full support for NIST incident response steps, so we can easily follow the ticket through detection and analysis, containment, eradication, and recovery."

End-to-end visibility with Performance Analytics

Bob agrees and points to the management visibility that this delivers. "Because we've got security-specific fields and states, we can now look at our incident data much more effectively using ServiceNow® Performance Analytics. We've got dashboards that show us exactly where we are and track our progress, and historical analysis lets us pinpoint areas for improvement and demonstrate compliance to our audit teams."

Rich integrations and value-added functionality

"Of course, we also get the full benefits of the ServiceNow roadmap," continues Bob. "Instead of building and maintaining our own integrations to data sources, we get these out of the box–and they are much richer than the ones we created by ourselves. We also get new functionality with every release. For example, we're looking forward to some significant UI enhancements in the London release, which will increase our efficiency even further."

Painless migration

Bob says that the cutover was straightforward. "We went from using ITIL incidents to using security incidents in a day. Previously, we didn't automatically convert alerts into incidents, so this made the transition easy. If we had, we would have needed to run ITIL incidents and security incidents in parallel until we were sure we were getting the same results for both. That's something to keep in mind if you're transitioning from a custom solution to the out-of-the-box application."

servicenow

Is automation always the right answer?

What about other types of automation, such as orchestration of preventative controls? Here, Bob is more cautious: "Security and IT teams have different priorities. For IT, it's all about keeping systems up and running. For instance, let's suppose security detects a virus on a domain controller. We can't just shut it down automatically. Instead, we need to talk to IT to understand the impact and take a risk-based decision together."

"That's why automated security orchestration needs to be approached with caution. We do automate some activities, but we are careful about the impact on the environment. We only take automated orchestration decisions with trusted threat information providers."

What about the future?

Bob is enthusiastic about what the future holds, planning to take further advantage of existing ServiceNow Security Operations capabilities, such as the ability to integrate CMDB data. "There's huge value in enriching security incidents with configuration information. When you have the right CI data at your fingertips–assets, relationships, system owners, and so on–it makes it much easier to investigate and remediate service issues. And, by using information such as service maps, you can prioritize much more accurately by including business impact. There's just one caveat. You need a highly accurate CMDB for security incident purposes–more accurate than you need for IT alone."

With ServiceNow Security Operations, we've strengthened and accelerated our security processes. We've moved away from time-consuming emails and spreadsheets, creating an automated security response environment that simplifies investigation, eliminates time-consuming data collection, and provides end-to-end visibility. Now, we respond faster and can scale as our business grows. In fact, we're already saving 8,700 hours a year in our security operations center, and we expect that to increase as we continue on our security automation journey.

Just as important, we are creating the fulfilling experience that our security analysts deserve. This allows us to attract and retain the best security talent, so that we continue to meet our security promise of protecting our customers and our business.

servicenow

Now on Now

How we use our own technology

LEARN MORE

About ServiceNow

ServiceNow was started in 2004 with the belief that getting simple stuff done at work can be easy, and getting complex multi-step tasks completed can be painless. From the beginning, ServiceNow envisioned a world where anyone could create powerful workflows to get enterprise work done. Today, ServiceNow is the cloud-based platform that simplifies the way we work. ServiceNow software automates, predicts, digitizes, and optimizes business processes and tasks, across IT, customer service, security, human resources, and more, to create a better experience for your employees and customers while transforming your enterprise. ServiceNow is how work gets done.

© Copyright 2018 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, and other ServiceNow marks are trademarks and /or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company and product names may be trademarks of the respective companies with which they are associated.