CASE STUDY

tenable

Process Transformation Powered by Tenable.sc and ServiceNow Integration

> *"We're transforming how we manage and keep track of vulnerabilities and also ticket items in the cybersecurity space, expanding our ability to better categorize and keep track of these kinds of vulnerabilities, and it's improving our ability to protect the organization."*

MATT
Team Leader

ORGANIZATION SNAPSHOT

COMPANY

Fortune 500 Oil & Gas Company

CHALLENGES

- Process inefficiencies made it difficult to meet service level agreements and manage longer-term remediation projects.
- A lack of automation was causing risky delays and team misalignment.
- Team members could not be held accountable because it was too difficult to track progress on each open ticket.

SOLUTION

tenable.sc

Tenable.sc with ServiceNow Security Operations - Vulnerability Response

RESULTS

- The automated process enables timely responses and eliminates the need for human intervention.
- The new system supports Security Orchestration Automation Response (SOAR) protocols.
- Improved tracking is resulting in better organizational intelligence about the state of each vulnerability.
- Improved visibility for managers in remote locations is leading to improved collaboration with SecOps team members.

A FORTUNE 500 OIL & GAS COMPANY

The vulnerability management team at a Fortune 500 Oil and Gas company was struggling with a slow, labor-intensive process which was putting the organization at risk. The team had been working with vulnerability scanners for approximately three years, and were pleased with the quality of the data they were receiving. Yet, they were still challenged to find and remediate vulnerabilities in a timely and efficient manner. About a year ago, the team decided to integrate its Tenable.sc suite with its ServiceNow Security Operations – Vulnerability Response platform. The integration – and resulting process improvements – eased their pain.

As an analyst in the cybersecurity group of a Fortune 500 Oil and Gas company, team leader Matt handles vulnerability scanning and mitigation for some 20,000 devices, including laptops, desktops and servers. He's part of a 25-person cybersecurity team charged with protecting the IT assets for more than 10,000 employees worldwide.

CHALLENGES

- **Inefficiencies in tracking vulnerabilities**
  Matt and his fellow team members had been working with vulnerability scanners for approximately three years, and while they were pleased with the quality of the data they were receiving, they were acutely aware of process inefficiencies which were making it difficult for them to find and remediate vulnerabilities in a timely and efficient manner.

- **Vulnerability scan reports were exported to a spreadsheet once a month and then manually entered into ServiceNow for tracking**
  "It was labor-intensive," says Matt. It would take one fulltime staffer up to two days per month to go through the process of exporting the vulnerability reports and manually assigning them to team members for analysis and remediation via the ServiceNow application. Team members needed anywhere from two days to a week to assess, remediate, and close out the ticket. "In the security space, the less time a vulnerability is in your network, the less damage it can cause," says Matt. "We would have something sitting there for a week or two weeks."

  The static nature of the process turned a minor issue, like a team member taking a sick day, into a major hurdle. It was nearly impossible for anyone else on the team to pick up the sick employee's work midstream. "We work on a team where we're thinking not only how we can continue what we're doing every day, but also how we can be better, more streamlined, more responsive," says Matt. That's why he says he and his team were pleased when they heard about Tenable's integration partnership with ServiceNow, **announced in February 2018**. "We knew we could now take the vulnerabilities and assign them quickly. We know the faster we can mitigate those issues, and keep an eye on the organization of it, the happier we'll be."

SOLUTION

About a year ago, the team deployed the Tenable.sc integration with its ServiceNow Security Operations – Vulnerability Response platform. The integrated solution delivered several benefits to the team, including:

- Central reporting on all past and present vulnerable systems
- Easily scheduled remediation scans for closed-loop remediation
- Vulnerabilities matched to assets without duplication

RESULTS

- **An easy deployment process and turn-key!**
  "It was really easy for us to roll out internally," says Matt. "We have ServiceNow developers in-house and our team has the Tenable subject matter experts in the company. We came to them and said we wanted to do this, and it was done along with the most recent ServiceNow update."

  "Another thing we really like is being able to use a new system or integration as out-of-the-box as possible. That's something we've really valued in the Tenable solutions we've used. It didn't take us a ton of man hours to customize them to make them function how we want them to. It came pretty much ready to go."

  The deployment challenges were less technological and more procedural. New knowledge documentation and training was required. Security analysts had to get used to processing vulnerabilities in buckets, rather than one by one. Many previously manual processes were now being automated, and everyone had to be taught how to make the most of that.

  "Convincing them was easy because we told them it would make their jobs easier," says Matt. "And it has."

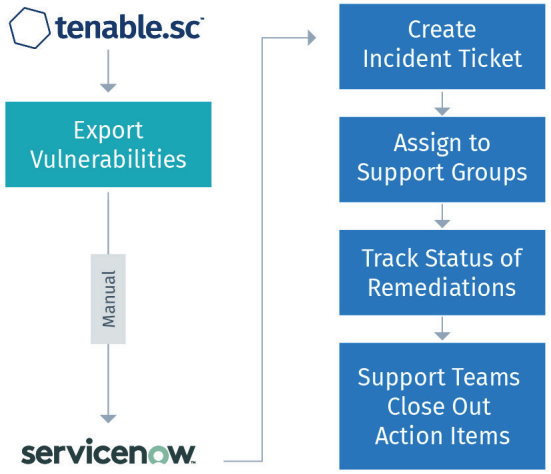
- **Elimination of spreadsheets**
  The simple phrase "there were no more spreadsheets to use" belies the tremendous impact this had on the team. Matt explains, "steps that previously took one full-time staffer up to two days to complete were now eliminated. Without all the busywork, the team can focus on what they do best: mitigating vulnerabilities."

  Instead of a cascade of vulnerabilities triaged one by one, the findings are pre-sorted into buckets based on a set of business classifications and user profiles and then automatically routed to the appropriate support group.

- **Efficient escalation of issues to the appropriate team members**
  The new system also enables the team to route issues to local support on-site at a specific location when needed. For example, says Matt, "we might find out an automated door system in use at one of our remote locations has a flaw, and we can send it to local support to handle right away."

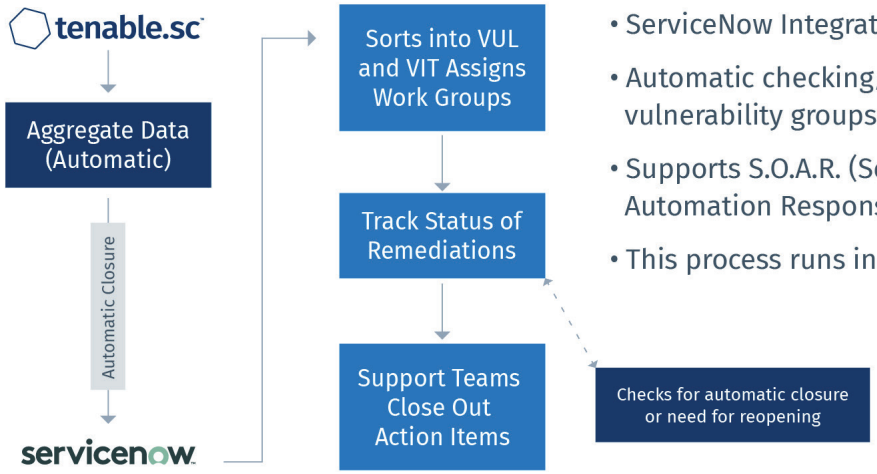
  "Let's say you have a group of laptops with vulnerability X," explains Matt. "Now, we can take that as a vulnerability group and, underneath it, you can put the list of computers needing remediation. Then you can check to see how many of those laptops are running the particular software that has the vulnerability. If it only affects the 20 computers you have running Mojave, you only see one item in your work bucket instead of seeing all 20 computers listed separately. If they're able to correct the issue and want to close out the vulnerability they can actually close out the entire group."

THE OLD PROCESS



- Labor Intensive and Manual
- Reporting, tracking and remediation
- Export out of Tenable.sc into spreadsheets
- Manually create incident tickets
  - Rigid SLA's
  - Tracking
  - Accountability
- Export and ticket creations were done on a per month basis

THE NEW PROCESS



- ServiceNow Integration with Tenable.sc
- Automatic checking/management of vulnerability groups
- Supports S.O.A.R. (Security Orchestration Automation Response)
- This process runs in the background daily

- **Improved efficiency in tracking and remediating vulnerabilities**
  "The only thing a human has to oversee in the process now is, essentially, that repository of items and where they're sorted," says Matt. "This new process takes away from the labor intensiveness as well as the manual process problems. It makes us more efficient and quicker at solving the issues at hand. We have better accuracy in mitigating the vulnerabilities we find."

- **Elimination of silos**
  Teams in both sites now have a unified way of organizing vulnerabilities, eliminating those workflow silos. The system is transparent, so supervisors can quickly see what's going on.

- **Improved vulnerability prioritization**
  Vulnerability prioritization is also improved, which is helping with employee engagement. Now, the team is prioritizing vulnerabilities based on their severity and risk to the organization, eliminating the stack-ranked approach. "We can put severity rankings on things, and it engages the remediation teams when they know they're working on something that's a higher priority. This helps them understand better what needs to be solved and they're motivated to fix it. It's expanded our reach as the hub of security to help those teams, to be more specific with them, and to provide concise answers to help them solve things in a more visible sense."

- **Increased speed and efficiency**
  The process is automatic on a daily cycle, aggregating data, pushing it to ServiceNow, and sorting it to the appropriate teams. There's no longer a concern about the single point of human failure if someone takes a sick day. Systems are in place to help the scanners determine which team a ticket needs to go to, so they're no longer relying on a single human to take care of routing the tickets. Added bonus: it works with the Security Orchestration and Automation Response protocols in use throughout the organization.

WHAT'S NEXT?

The team is exploring the capabilities of Tenable.io to see how the cloud offering might further enable process improvements. They're also working more closely with the IT team on fine-tuning the process, making sure configuration items are as accurate as they can be given the constant change in an environment like theirs, where devices are being added, swapped, or moved around.

"We'll be working more closely with those IT teams to make sure they're creating configuration items consistently with everything they're deploying," says Matt. "We're transforming how we manage and keep track of vulnerabilities and also ticket items in the cybersecurity space, expanding our ability to better categorize and keep track of these kinds of vulnerabilities, and it's improving our ability to protect the organization."

Click here to learn more | Contact Us: marketing@tenable.com