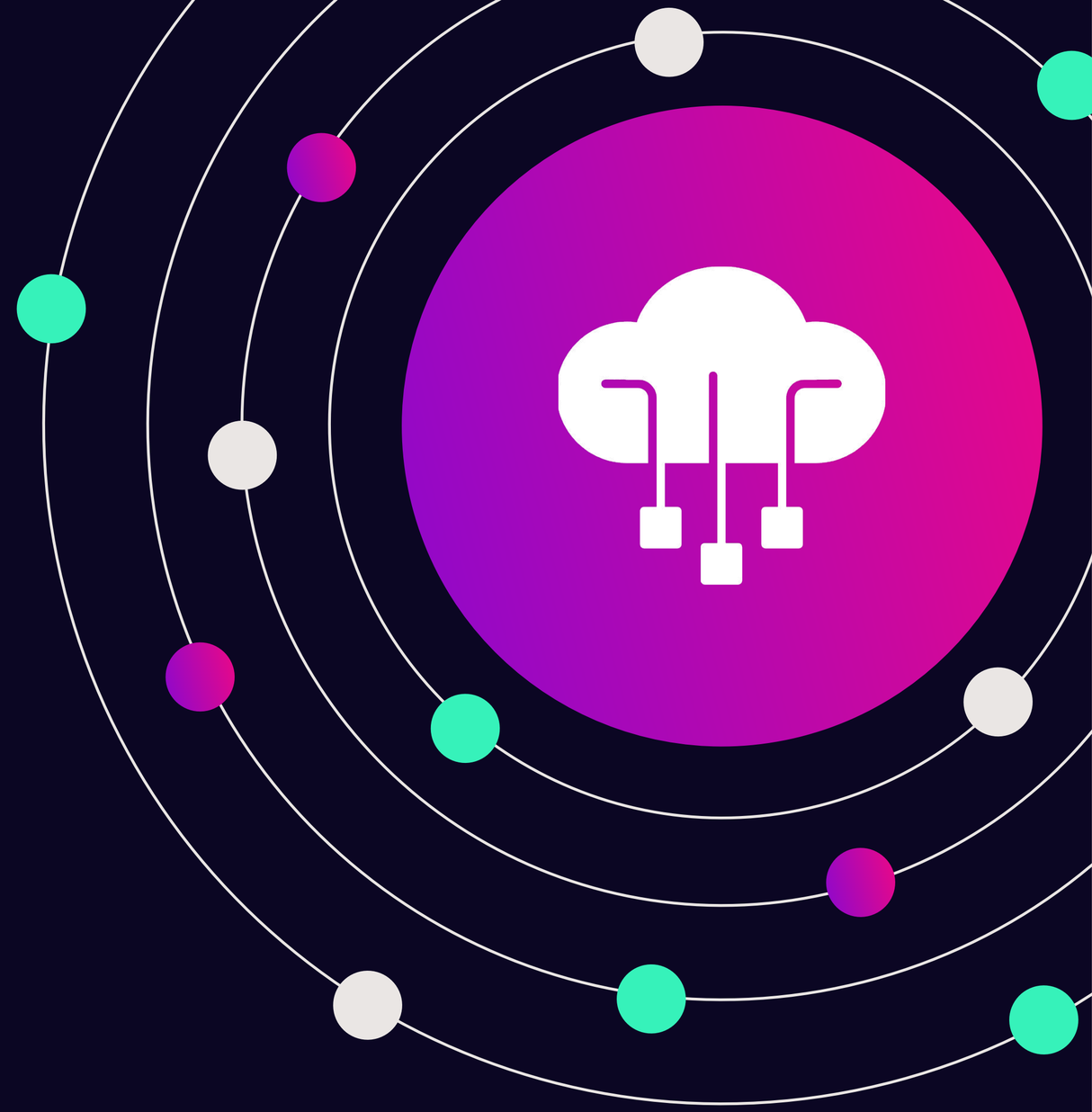
seemplicity

Large SaaS Company

streamlines and scales vulnerability remediation across infrastructure and applications.

CASE STUDY



Challenges

- Unscalable, ad-hoc process for vulnerability triage, ticket creation, and ticket closure for over 250,000 findings.
- Bottlenecks created by limited security resources to manage over 75 remediation teams.
- Manual data parsing and filtering of output from vulnerability scanners.
- Customized ticket formatting on a team-by-team basis

Solutions

- Automatic normalization, aggregation, and deduplication of vulnerability data to enable more manageable triage.
- Custom workflows for over 75 remediation teams to receive tickets in their desired format.
- Decreased backlog size from over 250,000 to 3,000 through deduplication and aggregation.
- Over 400 hours saved in the first year from automating ticket creation .

The large SaaS company, an organization with nearly 5,000 employees, provides software solutions trusted by over 50% out of the Fortune 100. Since its inception in the early 2000s, this company has adapted with the demands of digital transformation time and time again – and this time is no different.

Objectives

Managing cloud and IT infrastructure and product development vulnerabilities for this vulnerability management (VM) team has historically been a largely manual process – and until recently, a far more complex one. Their current vulnerability management solutions were creating one Jira ticket per vulnerability per business unit, creating a raw findings backlog that was creeping over the hundreds of thousands and therefore untenable to maintain with a manual process.

Their search for a solution had a few, but essential, criteria:

CUSTOMIZABLE TICKETING

The VM team would manually parse findings data and assemble tickets per each remediation team's specifications around ticket format, ticketing frequency, supplemental vulnerability information, and SLA time. The VM team needed to automate these specifications to save both time and manual labor.

> *"For the volume of vulnerability findings data we have, we'd need a whole team of people to manually generate these tickets." – John, VM team lead.*

SCALABILITY

This SaaS company needed a solution that would not buckle under the weight of findings for their cloud environments and massive on-premise IT infrastructure. This resilience would be crucial to implementing and maintaining a new, automated vulnerability remediation process.

TIME TO VALUE

The change management that comes along with a new vendor and process in the tech stack can often be challenging. The VM team needed minimal interruption in order to keep up with the current remediation velocity.

> *"We needed a way to get something practical and actionable into the hands of engineering and development teams so that they could intuitively perform the remediation," said John.*

FILTERABLE DATA

Each product in this organization falls under the jurisdiction of multiple engineering and development teams, each with targeted responsibilities for securing their respective product. This structure creates significant variability in the vulnerability data needed from team to team, calling for a solution that could deduplicate, filter, and parse data as needed.

Solutions

The ability to customize tickets and distribute them efficiently was at the center of this SaaS company's initiative to streamline their vulnerability remediation operations. The VM team ultimately chose to leverage Seemplicity's Remediation Operations (RemOps) platform to scale and streamline their remediation efforts across over 75 different engineering and development teams.

REDUCTION IN VULNERABILITY NOISE

Instead of manually sifting through hundreds of thousands of raw findings, they needed a solution that would remove false positives and duplicates before it even made contact with the VM team.

After integrating their vulnerability scanners with the Seemplicity platform, the VM team was able to reduce their backlog of over 250,000 findings by 98% before the triage process even began. The VM team now works from a much more manageable backlog of findings that aggregates affected systems into combined and actionable remediation tasks.

> *"If a product team has 30,000 affected hosts, they don't need 30,000 tickets – they just need one ticket. Seemplicity makes it so I don't have to do any parsing within my scanner to make sure the report pulls correctly, nor do I have to make any amendments," said John.*

TEAM BY TEAM WORKFLOWS

Getting tickets to the right team in the right format was previously strenuous. Because of their organizational structure, the right automation solution had to be flexible enough to accommodate this SaaS company's highly specialized sub-teams within the broader engineering and development organization.

In addition to keeping remediation progress organized with clear roles and responsibilities, remediation teams had a minimal learning curve. Because Seemplicity integrates with Jira, remediation teams did not need to learn another platform and could continue working within the tools they always use. Tickets are automatically opened, populated and prioritized with contextual information, and automatically closed when the vulnerability is fixed. The auto-closure takes the mental load off of engineers and developers to close the loop and instead pushes the process forward.

Getting consistent, information-rich tickets is crucial for efficient, actionable remediation. Seemplicity eliminates the need for security teams to chase down and enrich tickets with updates, freeing them up to work on other strategic initiatives.

> *"Just by virtue of using Seemplicity, we're getting tickets into the hands of remediation teams, which is a huge value. Previously, it would be me creating a ticket, and sending out, and chasing down email reports of vulnerabilities. Once a team's workflows are onboarded in the Seemplicity platform, there's already a value there." – John*

> *"If it doesn't exist in Jira, it doesn't exist," says John, "Seemplicity creating those Jira tickets for us and getting it on their boards frees us up to focus on things like reporting on vulnerabilities as a whole, SLA compliance, and other things we haven't previously been able to get to."*

Looking ahead

This SaaS company's Seemplicity deployment operationalized the entire remediation process across a range of business units, engineering and development teams, technology layers, and tools under the VM team. As the company scales, they're searching for even more opportunities to centralize vulnerability information and remediate faster.

"Our mantra looking ahead is that if there's vulnerability data, we have to get it into the hands of development and operations teams," stated John, describing possibilities to expand Seemplicity for container and cloud security, and more.

About Seemplicity

Seemplicity is remediation, simplified. By enabling smooth integration, cross-team collaboration, and scalability, Seemplicity yields unmatched cost savings and risk reduction for any organization.