seemplicity

Carlsberg Group

CASE STUDY

Carlsberg Group Transforms Remediation Operations With Seemplicity

Objectives

- Disparate dashboarding for security posture management and incident prevention
- Manually correlated vulnerability findings across security testing tools, cloud environments, and teams
- Unoptimized processes around remediation actions and owners
- Risk of burnout, task duplication, and misalignment across security and remediation teams

Outcomes

60%	reduction in vulnerability findings in platforms integrated with Seemplicity
Centralized, Normalized Hub	for proactive security posture activities
Automated Workflows	and cross-system processes for swift remediation operations from finding to validation
Ability to Trigger Remediation Actions	beyond opening and closing tickets to execute auto-remediation
Parallel Objectives	and work management across departmental boundaries and work management systems with accessible, consumable information

> We want to use Seemplicity as the centerpiece for all things connected to preventative security and posture management, our whole vision is to have a single, unified security posture dashboard, and that vision is ultimately coming true with Seemplicity.
>
> **TAL ARAD, CTO OF CARLSBERG**

The bulk of incident response and remediation is centered around an organization's SIEM and SOAR technologies. But there weren't any similar solutions to address the proactive prevention half of the equation.

The team at Carlsberg Group set out to find a solution that offered a complete view into security posture and incident prevention to quickly answer the question "what does my security posture look like today?"

Carlsberg Group, the world's third largest and sustainable brewing company, strives to globalize their growing portfolio of over 140 brands to bring communities together. Over the past few years, they have scaled their digital operations to include more operational technology and have added tens of thousands of dynamic and fixed assets, such as cloud computing containers.

As a manufacturer, much of Carlsberg's operations are geared toward minimizing downtime, making vulnerability management crucial to maintaining operational efficiency. When Venicia Solomons, Cloud Security Architect at Carlsberg, found a large chunk of her team's daily tasks centered around coordinating the logistics of remediation rather than priority-based remediation, she knew that the current processes needed to change.

OBJECTIVES

With a vulnerability like Log4j, the team at Carlsberg previously would have had to analyze the risk using three or four security systems from a variety of different angles to understand the real severity and risk at hand. With findings overload and largely manual remediation operations processes, effective and timely vulnerability management was a difficult task.

⊗ Over-Visibility Into the Attack Surface

Modern enterprise organizations like Carlsberg often utilize multiple cloud providers, a plethora of vulnerability scanners, attack surface management platforms, and much more. Although these solutions provide in-depth visibility and are designed to simplify security, they instead provide too much information, and piecing these views together amplifies complexity. Carlsberg wanted to gauge the actual level of security and visibility they were getting from their security tools because of platform-specific scoring systems, varying degrees of coverage, and domain-specific visibility.

Routing Alerts

Continuous vulnerability scanning, while crucial, generates mountains of data with little to no context on severity or priority. Carlsberg, like many organizations, uses multiple vulnerability scanners that can even overlap and create duplicate findings. Triaging these findings took massive amounts of manual effort and left room for error. Further, finding the correct remediation project owner took hours of cross-team syncs and coordination across multiple ticketing systems to weigh the remediation team's bandwidth against the criticality of their aggregated vulnerabilities.

OUTCOMES

Confidence in Risk Posture

Although fragmented over-visibility can result in a false sense of security, Seemplicity's centralized view of risk provided the Carlsberg team with an accurate evaluation of their risk posture by continuously aggregating, de-duplicating, normalizing, and organizing their vulnerabilities into one consumable dashboard. In fact, Venicia and her team saw a 60% reduction in findings immediately after using Seemplicity. Carlsberg harnesses this simplified single source of truth every day to make more informed decisions throughout their remediation operations.

> From an overall risk posture perspective, we now know what we're up against. We know how many remediation teams we have and we're able to categorize, measure, and make sure that the most critical risks get remediated in order of priority. It's automatically executed through the remediation queues, which is an even bigger advancement for us.

VENICIA SOLOMONS, CLOUD SECURITY ARCHITECT

Automated Workflows and Remediation Queues

The ability to not only view and understand remediation actions, but also be able to execute on those remediation actions is a huge added plus for the cloud security team at Carlsberg Group.

By automating the triage and assignment of findings, the Carlsberg security team saved hours of manual evaluation and planning. Further, the Seemplicity platform segments the backlog into remediation queues that make the backlog more manageable. These queues help Carlsberg concentrate on the most critical findings and receive a new batch once those are closed. The number of tickets in each queue is based on the team's bandwidth, thus ensuring that workload never exceeds bandwidth.

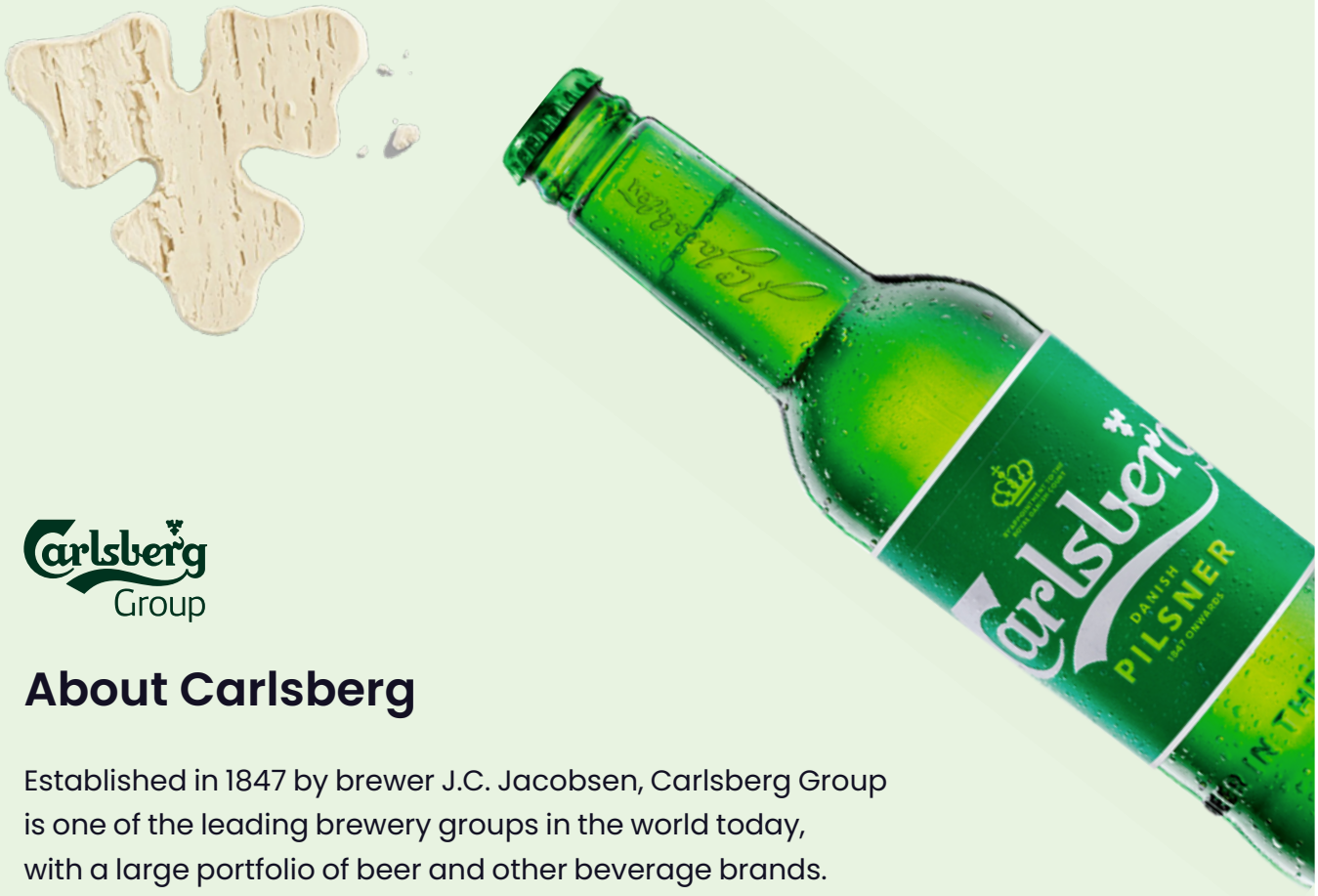
> The value is not just automating ticket management. It's being able to set processes that trigger automatic remediation, or being served batched backlogs of the most critical findings. Seemplicity gives us the capability to execute.
>
> **TAL ARAD, CTO AT CARLSBERG GROUP**

Positive Security Culture

By implementing automated remediation operations, Carlsberg is working towards creating a more positive and collaborative security culture. Carlsberg executive teams can access a unified view to track remediation efficiency and progress, and practitioners are eager to use the Seemplicity platform to gauge where they stand in terms of vulnerabilities and the effectiveness of their remediations. This transparent, accessible, and easy-to-understand flow of information across teams and stakeholders encourages a positive security culture throughout the organization.

CONCLUSION

By elevating remediation operations with the Seemplicity platform, the Carlsberg Group's cloud security team transformed a once ad-hoc, manual process into a streamlined machine. Over the last two years, Carlsberg's optimized mean time to remediation empowered them to expand usage beyond cloud security to fuel other security initiatives like GRC and application security.



About Carlsberg

Established in 1847 by brewer J.C. Jacobsen, Carlsberg Group is one of the leading brewery groups in the world today, with a large portfolio of beer and other beverage brands. More than 40,000 people work for Carlsberg Group, and our products are sold in more than 150 markets.

Getting Started with 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.

Visit **seemplicity.io** to learn more about transforming the way your organization handles risk.