Tonic

CASE STUDY

Plarium cuts manual remediation effort by 50% with Tonic

How Plarium connected security findings to business context and ownership to prioritize the exposures that matter and accelerate remediation.

Too many vulnerabilities, too little context

Plarium Global Ltd., part of Modern Times Group MTG AB, creates mobile and PC games for more than 500 million registered gamers. Its portfolio spans 20 titles, with more than 1,300 specialists across seven offices and development studios.

For Oren Zenescu, Group CISO at Modern Times Group MTG AB, operating at this scale created a familiar security challenge: thousands of vulnerability findings, but not enough context to determine what actually mattered.

Technical severity alone could not show whether a vulnerable asset supported a crown jewel, critical service, or core business process. Plarium also needed to understand whether an exposure was reachable, exploitable, or internet-facing, what security controls were already protecting it, and which business processes could be affected.

Ownership created another bottleneck. Identifying the right asset owner could take days and was often based on imperfect signals such as the last user to log in. That slowed assignment, ticket creation, and ultimately remediation.

PLARIUM

Company

Industry: Media & Entertainment

HQ: Herzliya, Israel

Size: 1,300+ employees

Reach: 500M+ registered gamers

Revenue: ~$613 million

Challenges

Overload of vulnerabilities with little meaningful and actionable context.

Solution

Connected security and business data to correlate assets, identities, owners, processes, vulnerabilities, and controls.

Impact

Cut repetitive manual effort by about 50%, accelerated ownership and remediation, and exposed hidden identity, asset, and control gaps.

RESULTS

~50% less manual effort	Days → immediate	Automated workflows	Hidden risks uncovered
Reduction in manual vulnerability management	Asset owner identification	Ownership assignment, ticketing, and remediation coordination	Orphaned identities, idle assets, and missing security-control coverage

“Less manual effort, more business context, and a more satisfied SecOps team.”

Oren Zenescu, Group CISO, Modern Times Group MTG AB

Business context turns findings into priorities

Plarium connected Tonic to business systems ranging from spreadsheets to SaaS applications. Tonic correlated that data across servers, workloads, users, identities, business functions, and processes, then connected it back to security findings.

This gave Plarium two complementary views of the same exposure. The business view showed whether an asset supported a crown jewel or critical process. The cyber view showed whether the exposure was reachable, exploitable, internet-facing, or mitigated by another security control.

Bringing those signals together allowed the team to cut through vulnerability noise and focus remediation on the exposures that mattered most.

> **“Going over thousands and thousands of vulnerabilities isn’t helpful. I need to quickly understand the holistic picture and where we need to remediate, fast.”**

From ownership guesswork to action

Prioritization was only the first step. Tonic used Plarium’s connected organizational and security data to identify owners and associate them with the right assets.

What previously took days could now happen immediately. Ownership assignment and ticket workflows were automated, reducing the manual handoffs that delayed remediation and helping the team move more quickly from identifying an exposure to getting it fixed.

Oren estimates that Tonic saves about 50% of the time previously spent on repetitive manual work, while the same automation has helped reduce mean time to remediation.

Finding the gaps other tools miss

Connecting security and organizational data also exposed risks that were difficult to see when looking at individual systems in isolation.

Tonic surfaced active identities belonging to people who had left Plarium, including access to sensitive systems. It identified idle servers, computers, and other resources that remained online, carried vulnerabilities, and no longer served a useful purpose.

The same connected view highlighted gaps in security-control coverage. If EDR covered 80% of assets, for example, the team could identify the uncovered 20% and apply the same analysis across other controls. Attack-path analysis provided another perspective on risks that routine security operations could miss.

> **“Tonic helps us answer the question of what we don’t know that we don’t know.”**

Security connected to the business

For Plarium, the result is more than a cleaner vulnerability queue. Tonic connects findings to the business services and critical processes they can affect, helping the security team understand which exposures matter, identify who owns them, and move remediation forward faster.

The result is less manual work, faster remediation decisions, and a clearer understanding of where cyber risk intersects with the business.

> **“What I like best is the simplicity. It makes this complicated data fabric simple and easy to digest for me and my team.”**

About Tonic Security

Tonic helps security teams accelerate the prioritization and remediation of vulnerabilities and other findings with an Agentic Exposure Management platform. Tonic connects fragmented security and IT signals, identifies the exposures that pose the greatest risk to the business, and automates the path from detection to verified remediation, with human oversight throughout. The result is faster, safer risk reduction at the speed of AI. Learn more at www.tonicsecurity.com.