SeeMetrics

Case Study

A Fortune 500 Financial Institution invested millions

over several years building an in-house metrics program but struggled with efficiently measuring the performance of their security operations

SeeMetrics automated the entire journey

to proactively measure, track, and improve performance based on stack-derived data and out-of-the box metrics.

Company Snapshot

A world-leading financial institution and services provider with a strong track record and global reputation.

As technology evolved, so did the Company. Its 1,000s of users turned to a wide range of digital tools on a daily basis, generating massive amounts of data. The Company built a cybersecurity department which developed into a mature program that relied on diverse security tools.

12,000+
employees

80+
cybersecurity tools

Listed on Fortune World's Most Admired Companies

The Challenge

As the cybersecurity department grew, it struggled with a lack of clear and continuous understanding about stack coverage, utilization, and program performance. The number of legacy tools and the many M&As further complicated the already complex stack.

With no infrastructure for measurements, no baseline, and no common perspective of what really mattered:

- They couldn't measure the performance and effectiveness of their team, tools and processes.
- They didn't know how quickly they closed existing incidents, if they were effectively managing new ones, or if they were improving over time.
- Alignment between CISOs, their teams, and other relevant departments was extremely challenging.

"First time we've shifted from our "offline" Excel to a platform that provides us with real-time indication of our usability and performance. We're using it and really impressed."

Deputy CISO of the Financial Institution

SeeMetrics

Case Study

Why it was hard to resolve these issues in-house

$5M | 5+ years
To build and maintain it on their own

The options available were:

- **Manual collection and analysis of data from the security stack** would mean relying on relevant Subject Matter Experts (SMEs) or operations teams to export the data and the security team to manually analyze and manage everything in Excel.
- **Outsourcing analysis to consulting companies** would require in-house SMEs to extract the data - an option so expensive that most organizations couldn't afford to do it more than once a year.
- **Real-time home-grown metrics programs would require creating a pipeline** that automatically shifts data from each of the tools in the stack to one central place, and cleaning and contextualizing to reduce the noise. This requires significant technical and security SME resources.

The SeeMetrics Solution

1 Platform
Immediate performance insights

After a seamless integration that included connecting APIs, the SeeMetrics platform mapped the products in the Company's security stack to their capabilities, providing a dynamic understanding of:

- Which capabilities were covered
- Which capabilities were missing
- Which capabilities were overlapping
- Where there was a cost-effective way to consolidate without increasing risk
- How well the tools were performing
- How the performance of each capability impacted overall program performance

SeeMetrics introduced an incomparably efficient way to track stack performance.

With SeeMetrics the Fortune 500 Company achieved:

- **87%** reduction on time spent assessing coverage, performance, and utilization
- Automated mapping between security controls and **83 products**
- Continuous visibility to the organization's portfolio for **10 security leaders/BISOs**
- Reduced costs based on stack rationalization insights
- Maintained focus of security budget on securing the organization, rather than on data analysis

SeeMetrics

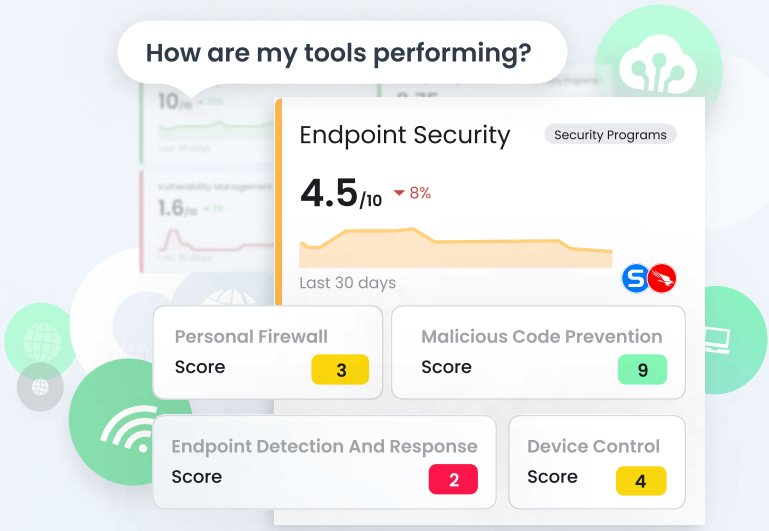
Case Study

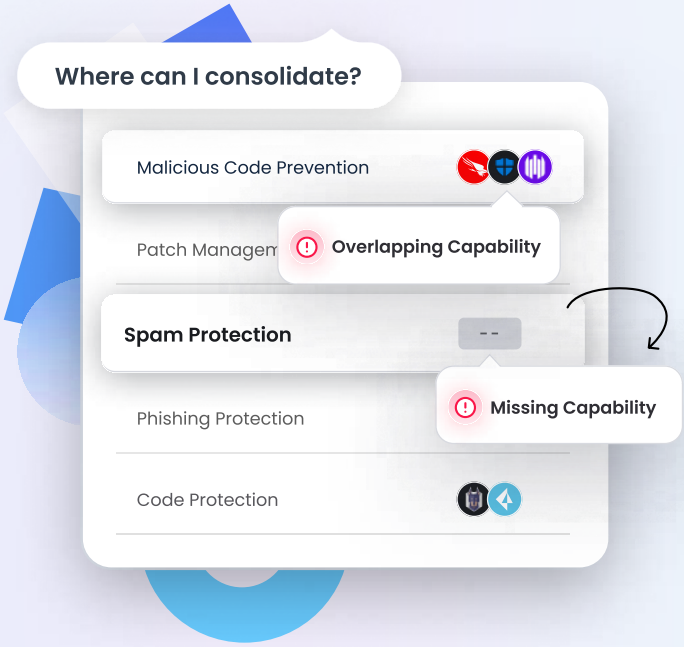
Summary

Understanding capability performance allows security organizations to:

Streamline Security Stack Management

With SeeMetrics, the Company's security leadership has access to automated, real-time, and continuous insights about the coverage and effectiveness of their security tools. This allows the Company's security leadership to achieve an improved understanding of their security stack.





Improve Tool Utilization

Powered by understanding into the stack utilization and capabilities coverage, the Company's security leadership is able to rationalize their stack and make better informed decisions regarding the expansion of existing tools, adoption of new ones or better leveraging what they currently have.

Communicate Efficiently and Proactively about Performance

Using a unified language for metrics, the leadership can now quickly communicate critical gaps and priorities to different teams, set measurable goals, and improve collaboration. They are able to convey the current status and progress to other stakeholders such as executives and board members, and validate their decisions and actions.