torq + epam

Digital Transformation Services Leader EPAM Systems Optimizes Large-Scale EDR Operations with Torq No-Code Security Automation

Background

EPAM Systems, Inc. (#721 in Fortune Global 2000) is an American company that specializes in service development, digital platform engineering, and digital product design, employing one of the largest software engineering workforces in the world to support a wide range of projects delivered to EPAM's customers.

To secure the remote endpoints of tens of thousands of engineers across the globe, EPAM is operating an award-winning 24x7 Security Operations Center that relies significantly on a modern Endpoint Detection and Response (EDR) infrastructure to cover the distributed fleet of devices.

To successfully handle the large volume of cybersecurity events, EPAM is required to implement automatic pre-processing of all events before they reach SOC Analysts in order to:

- Clean the high rate of false positives often generated by security tools, which previously involved a lot of manual time and effort to investigate and verify
- Pre-prioritize the most important events for handling to allow the information security personnel to efficiently protect the workforce's geographically-distributed endpoints
- Continuously implement the learnings made by analysts to ensure improvements in accuracy of detection and analysis

Because EPAM is a highly technical organization, it compared the options of implementing this approach in-house versus using a security automation platform, such as Torq.

Optimizing with Torq

In collaboration with Torq's Solution Architects, a framework was developed capable of handling more than 10,000 weekly events, applying a combination of "optimistic" and "pessimistic" automated checks on every identified information security threat in order to either proactively close it as one that doesn't require analyst attention or better prioritize its severity.

About EPAM

FOUNDED
1993

HEADQUARTERS
Newtown, PA

REGION
North America

 # OF EMPLOYEES
35,000+

SPECIALTIES
- Service Development
- Digital Platform Engineering
- Digital Product Design

Critical Success Factors

"Time-to-market" of adding and adjusting the logic that processes threats: A change in behavioral detection may lead to up to 40,000 new events within a short period of time, making human analysts unable to process anything close to the amount they are faced with; they need to be able to respond quickly with automatic pre-analysis and clean up.

Guaranteed processing time of under 4 minutes for each threat: Analysts need to engage with IT security threats that have the highest probability of being most dangerous within a quick response time.

Confidence in logic changes not deteriorating detection efficacy: Flooding analysts will result in blind spots and disability to handle the events and effectively protect the organization.

The Torq Solution

01

A collection of automated analysis rules performing optimistic/ pessimistic analysis, leveraging a specific endpoint platform (Windows / Mac / Linux)

02

A confidence level calculation system based on multiple analysis rules providing independent estimations for the eventual verdict

03

Test scaffolding allowing verification of new rules versus historical IT security events to understand the impact on the verdict

04

Rapid development and implementation in three weeks— From there, the system went into staging, parallel to the initial homegrown system, and then into full production replacing the homegrown system

Outcome

With Torq, EPAM Systems is benefiting from a stable environment that handles IT security events in under 4 minutes. It is now executing between 10,000-20,000 workflow runs per week with 100% success. And when it needs to introduce further changes to the environment, they can be implemented in mere minutes.

"Torq has transformed our IT security posture for the better, by introducing an easy-to-implement, high-velocity security automation platform capable of handling the ever-increasing workflows our complex environment requires," said Miroslav Sklansky, Senior Director, Global Head of Information Security Technology, EPAM Systems. "Torq has been a trusted partner, working with our IT security team to comprehensively calibrate its solution for our needs and ensuring business continuity for our employees and customers alike. With Torq, we're secure in the knowledge that our cybersecurity infrastructure is optimized for maximum efficiency and rapid remediation."

"Torq has transformed our IT security posture for the better, by introducing an easy-to-implement, high-velocity security automation platform capable of handling the ever-increasing workflows our complex environment requires."

Miroslav Sklansky

Senior Director, Global Head of Information Security Technology

See how Torq can help you today.

Get Started