TASE Implements a Continuous Security Validation Process

Organization

The Tel Aviv Stock Exchange (TASE) provides a market infrastructure and plays a critical role in the Israeli economy, ranging from helping Israeli companies raise capital and meet their growth and liquidity needs to providing investors with a reliable trading platform. TASE is the only stock exchange in Israel and includes divisions tasked with clearing and auditing, as well as various administrative functions. The organization is required to comply with stringent security and data privacy regulations and standards, both local and international.

Security Challenges

TASE relied on in-house and outsourced periodical manual pen testing exercises to assess the effectiveness of its security program. By nature, those security validation processes were limited in scope, only provided a point-in-time evaluation of the security posture, and required a significant investment in time and resources. Understanding the dynamic nature of the threat landscape and the potential dire consequences of an attack, TASE required a tool that could enable it to continuously validate its security posture on an ongoing basis. TASE was most concerned about ensuring that its network segmentation was configured correctly to prevent attacks through email or any infected external sources. It was also important to the organization to harden its resilience against malware remote code execution, like Powershell commands, as well as ensure it was protected against supply-chain attacks.

Challenge

TASE required continuous security validation because any cyberattack on TASE's network could have catastrophic financial consequences for Israel's economy.

Solution

Implementing Cymulate hardened TASE's security posture and enables its risk department to establish a tolerable risk scale with data-based, quantified KPIs.

Benefits

TASE has full continuous visibility of its security posture and can combat security drift with Cymulate's easy-to-digest mitigation guidance.
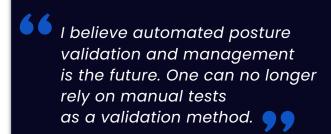
Solution

TASE started using Cymulate to continuously validate its security posture. Running Cymulate assessments both in the staging environment and again in production ensures that there is no misconfigurations before implementing infrastructural or systematic changes. The platform provides TASE with ongoing visibility into its security posture as well as optimizes its vulnerability management. Cymulate enables the security team to recalibrate SIEM alert policies to minimize false positives and prevent missed alerts. The TASE team was able to implement a continuous security validation process and has incorporated it into their weekly routine.

> *I believe automated posture validation and management is the future. One can no longer rely on manual tests as a validation method.*
>
> Gil Shua, Director of Information Security, TASE

Benefits

Mapping potential attack paths, from policy breaches on endpoints to lateral movement security gaps before an attack takes place, enables TASE to harden their security posture and prevent hostile intrusions and security drift. Cymulate's comprehensive assessments include resilience against emerging threats and new vulnerabilities as well as detection and actionable remediation recommendations against excessive permissions and misconfigurations.

> *Cymulate's scale and variety of automated assessments enhances the team's productivity and provides the most comprehensive picture a CISO needs to address his concerns.*
>
> Gil Shua, Director of Information Security, TASE

About Cymulate

Cymulate was established with the vision of empowering security professionals to make better decisions faster, based on real-time data. Founded and led by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is determined to become the golden standard for security professionals and leaders to know, control, and optimize their cybersecurity posture end to end. Trusted by hundreds of companies worldwide, Cymulate constantly enhances its methods to prepare organizations for any attack scenario or campaign.
With Cymulate, organizations continuously measure security performance in real-time, shore up defenses, and assure operational effectiveness.
Measuring your cybersecurity performance is fundamental towards creating a more secure organization!