Cymulate

Trend Micro - Vision One Joint Solution Brief

Challenge

Security teams are inundated on a daily basis with novel attacker strategies, new threats, IOCs to track and block, new technology capabilities, and more. In addition, there are a seemingly endless number of tools and technologies to manage in an organization. It is critical to ensure an appropriate level of protection and threat mitigation exists in an organization. Managing the correct configurations of technology is vital, particularly as threats evolve and change and vendors release new and enhanced feature sets.

Furthermore, training security team members to be skilled in recognizing and responding to new threats can be difficult. How does a new threat type manifest itself in events, alerts, and user interfaces? What kinds of things should a SOC team member be looking for to determine if the activity is actually malicious or just a false positive? Addressing these questions is not easy, unless you have a very skilled red team, to train against.

Integrated Solution

Cymulate risk validation and exposure management solution combines Breach and Attack Simulation (BAS), Automated Red Teaming, and Purple Teaming. The Cymulate platform enables teams to conduct automated or manual assessments. Ready-made templates and customizable assessments give the flexibility to accomplish any desired outcomes, from validating configurations efficiency or verifying that alerts perform as intended to running tabletop exercises to train teams or simply understand the system's overall risk level.

Trend Micro's Vision One platform with managed XDR provides detection, response, and protection workflow automation. Instrumentalizing the safe simulation of cyber-attacks and behaviors in context identifies security gaps in attack routes and correlates them with inadequate configuration, unpatched vulnerabilities, and other security flaws, accelerating the in-context optimization of Trend Micro's Vision One configuration performance.

Joint Solution Benefits

- Automate control assessments and measure control performance
- Quickly and easily identify where controls are robust and where they are weak against actual attacker tactics and techniques
- Identify opportunities for blocking and tuning to stay protected against most current threats
- Correlate findings with Vision One to expand detection and response capabilities

Key Benefits

01 Validate Trend Micro Vision One configurations are correct and optimized for your organization

02 Safely execute real-world attacker behaviors and tactics against assets protected by Trend Micro Vision One

Use Cases

Continuous Validation

Challenge

Security teams need to understand and validate their ability to reduce enterprise risk through their people, processes, and technology. Executing validation testing for new rulesets, detections, alerts, and policy configurations is time-consuming and challenging.

Solution

Cymulate provides out-of-the-box and customizable testing templates to test broad or specific attack scenarios. After setting up the Trend Micro Vision One integration, these templates can be used to test on a regular or ad-hoc basis to prove that defensive controls are operating as expected and at the right level to mitigate and respond to threats.

SOC Optimization

Challenge

SOC teams have a lot to handle. With constantly changing IT architectures, applications, and technology, alert fatigue causes teams to miss critical alerts or overlook malicious activity.

Solution

Cymulate enables you to execute periodic planned assessments to ensure that events are delivered to the right teams, investigation processes kick in on time, and response operations begin with defined SLAs. These assessments can also serve as training opportunities for more junior resources to show the series of activities that string together to create a malicious attack scenario. Using Cymulate and Trend Micro Vision One together allows SOC teams to conduct assessments of their own processes and to create a cyclical testing process, as well as a mechanism for implementing continuous process and personnel improvement.

SOC Optimization

Challenge

Threat landscape constant evolution, frequent deployment, third-party providers updates, and other factors can lead to a potentially catastrophic security drift if unnoticed.

Solution

Cymulate's automated attack simulation can be run continuously, and setting up baselines is easy with Cymulate's scoring, enabling monitoring of real-time, in-context variance from those baselines. Precise identification of the source of detected variance and actionable remediation guidance accelerate remediation. The result is a robust and stable security posture.

About Trend Micro Vision One

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, the platform delivers a powerful range of advanced threat defense techniques optimized for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com.

About Cymulate

The Cymulate SaaS-based Security Posture Management provides security professionals with the ability to continuously challenge, validate and optimize their on-premises and cloud cyber-security posture with end-to-end visualization across the MITRE ATT&CK® framework. The platform provides automated, expert, and threat intelligence-led risk assessments that are simple to deploy and easy for organizations of all cybersecurity maturity levels to use. It also provides an open framework for creating and automating red and purple teaming exercises by generating tailored penetration scenarios and advanced attack campaigns for their unique environments and security policies.

Contact us for a live demo, or get started with a free trial

Start Your Free Trial

info@cymulate.com | www.cymulate.com