CYLANCE

Cymulate

Cymulate and Cylance
Solution Brief

Using Cymulate Breach and Attack Simulation to Continuously Validate and Optimize the Effectiveness of Your Cylance Endpoint Security Controls

The threat landscape is constantly evolving with new types of malware and attack techniques. Enterprise security teams must validate and optimize the effectiveness of their security controls against a myriad of attacks that develop over time and to changes in the IT environment that may create new security gaps.

CylancePROTECT and CylanceOPTICS

By constantly training on a vast set of real-world threat information, CylancePROTECT takes a formulaic data science approach to protection, harnessing the power of the cloud with the scalability and efficiency of artificial intelligence and machine learning. Cylance's mathematical approach statistically determines whether a file is safe to run before it is executed. CylanceOPTICS provides built-in incident investigation and threat hunting capabilities in addition to automated and manual response options.

Cylance has evolved endpoint security to tackle the volume and sophistication of threat developments by introducing new technologies that learn and adapt to changes in the threat landscape.

Security Validation Integration with Cylance

Cymulate integration with Cylance provides automatic correlation of attack simulations to Cylance findings in the Cymulate platform. Whether using customizable or out-of-the-box scenarios, Cymulate enables security teams to simulate malicious payloads and threat behaviors on their endpoints and correlate Cylance findings and actions to a broad spectrum of attacks. By challenging a Cylance endpoint security deployment with adversarial activity, an organization can validate effective and accurate baselines, quarantine and blocking policies.

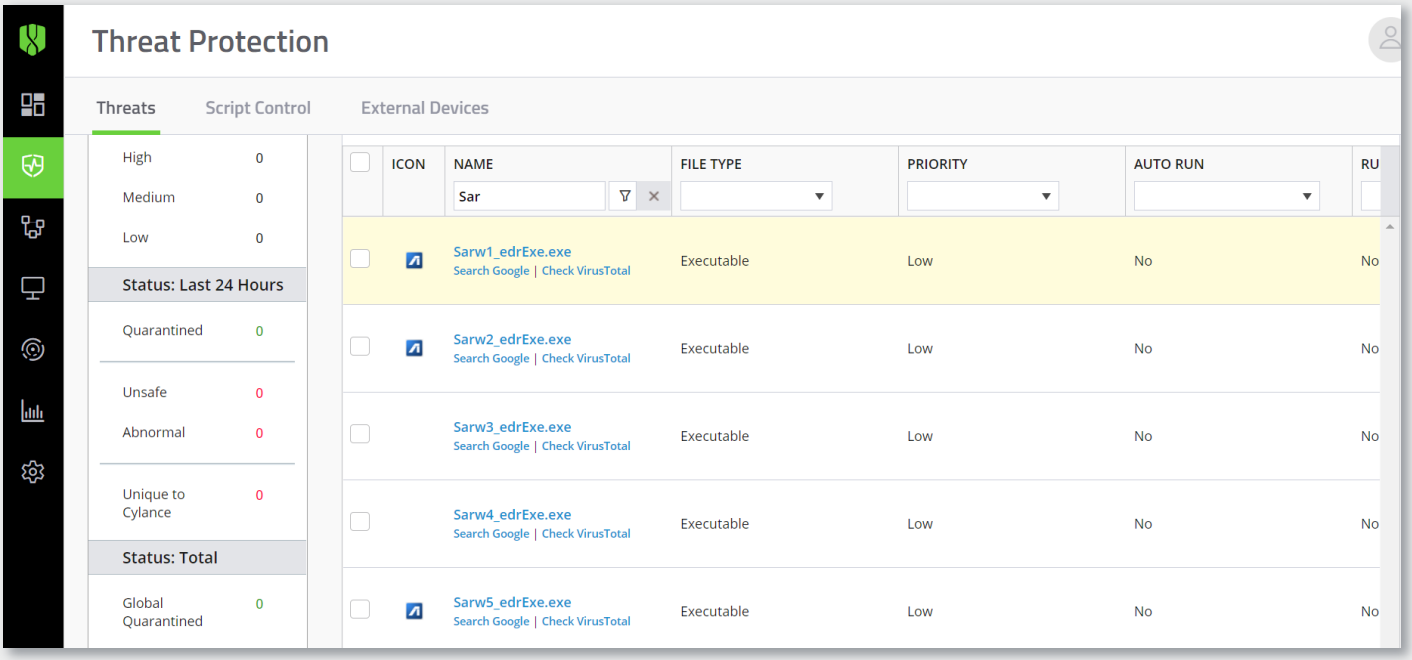
Immediate Threats

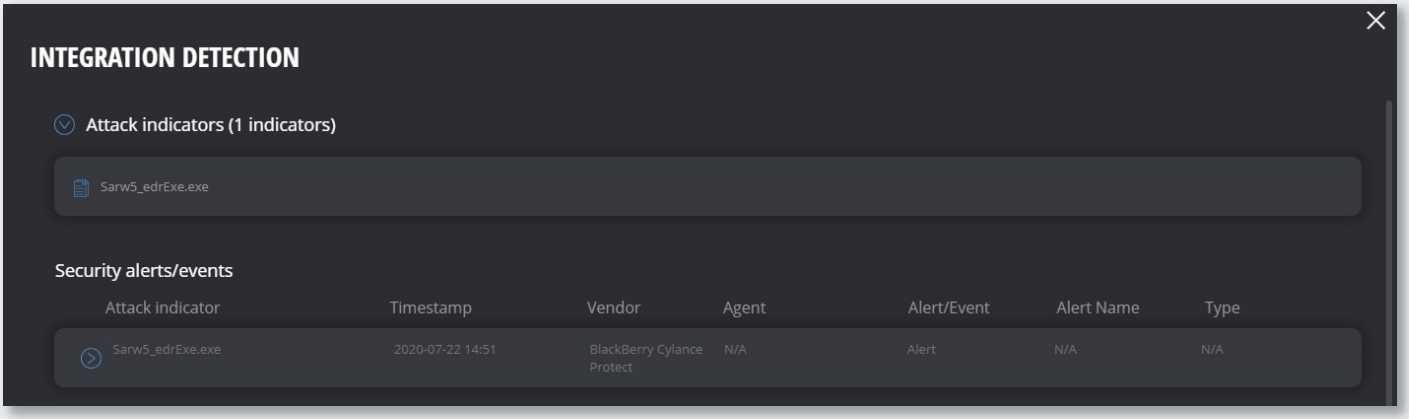
Security teams are challenged knowing whether their security controls protect them against the latest threats. The Cymulate Immediate Threats Intelligence module is updated daily with new threats, so that security teams can test the efficacy of their Cylance endpoint security controls to the evolving threat landscape.

One such example is a new version of a Windows malware called Sarwent. Once Sarwent is active on a system, the malware creates a new Windows user account, modifies the Firewall, and then opens the RDP ports.
This enables the attacker to use the new Windows user they created on the infected system to access the host without being blocked by the Windows firewall.

The assessment is executed, and in this case, Cylance detects and prevents the attack.
The security team sees the result in both the Cymulate platform and the Cylance platform.

In cases where the simulated attack is successful the platform provides the IoCs and the URLs associated with the attack. The assessments can be repeated to confirm protection.

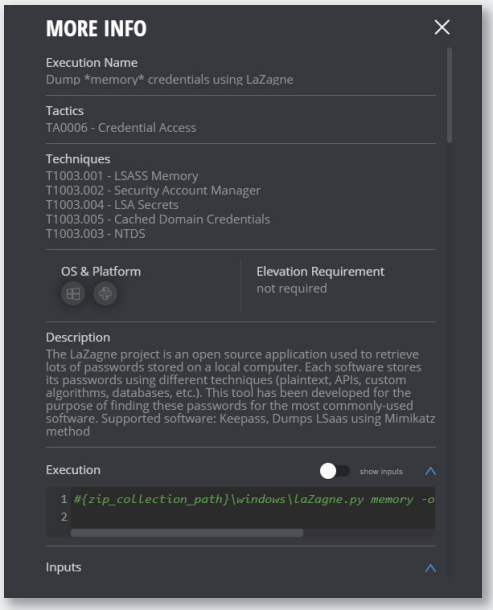




Cymulate

Validating Efficacy to MITRE ATT&CK Techniques

In many cases the security team will want to validate the efficacy of their security controls to a specific technique or set of techniques. These can be performed to identify specific weaknesses or to exercise an incident response playbook.
For example, a memory dump to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS), MITRE Technique: T1003.001 - LSASS Memory. This technique can be achieved using a variety of tools like LaZagne, Mimikatz, and ProcDump. Cylance integration with Cymulate enables the security team to validate accurate detection and response to this technique.
It also enables them to exercise their incident response playbook to this scenario, to contain the attack and gather artifacts related to the attack.



Integration Benefits

- Immediate insights: Security validation results and IOCs are always at the SOC team's fingertips, enabling them to optimize EDR capabilities.
- Latest threat intelligence: Detailed attacker TTPs and daily threat updates give SOC teams the latest insight on threat landscape developments.
- Unified visibility: Integration with CylancePROTECT and CylanceOPTICS maximizes team productivity for decision making and developing remediation or mitigation procedures based on true-to-life attack simulations.
- Mitigation guidelines: Teams receive guidance mapped to the MITRE ATT&CK™ framework for accelerating remediation of security gaps.
- Comprehensive coverage: Cymulate challenges controls across all vectors, as well as the entire kill chain, for comprehensive coverage and visibility.
- Continuous automated testing: Automation enables security teams to continuously challenge controls and immediately identify infrastructure changes or security gaps before they are exploited.
- Process optimization: Cymulate emulates full kill chain APTs to exercise a security teams detect and respond capabilities and outcomes, manual and automated.

Who We Are

With a Research Lab that keeps abreast of the very latest threats, Cymulate proactively challenges security controls against the full attack kill chain, enabling organizations to avert damage and stay safe.
Cymulate is trusted by companies worldwide, from small businesses to large enterprises, including leading banks and financial services. They share our vision - to make it easy for anyone to protect their company with the highest levels of security. Because the easier cybersecurity is, the more secure your company - and every company - will be.

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

Headquarters: 2 Nim Blvd., Rishon LeZion, 7546302, Israel | +972 3 9030732 | info@cymulate.com
US Office: 10001 | +1 212 6522632