Detect zero-day cyberattacks with Micro Focus ArcSight and Polyverse Zerotect

Detect zero-day exploits conclusively without any prior knowledge, signatures or AI/ML.

Finding, catching and reporting zero-day attacks are the holy grail for information security professionals and whenever a new vulnerability is announced enterprises scramble to implement patches and protections for their critical infrastructure. Researchers spend years looking for these vulnerabilities because there is a real tactical advantage to securing critical systems faster than competitors who may have to wait weeks or months for patches to be released, tested and deployed.

However, most detection agents are unable to detect unknown attacks like zero-days and fileless malware. On top of that memory-based and fileless attacks are some of the toughest attacks out there as they bypass all of the traditional cybersecurity defenses like firewalls and antivirus. Of all successful attacks, almost two-thirds of them are memory-based.

ArcSight and Zerotect enable a new class of zero-day detection for enterprises and SOCs to improve their security posture and situational awareness. Zerotect detects memory-based attacks by monitoring various system events and interpreting them in a structured format that is emitted to ArcSight for analysis. Memory-based and fileless attacks produce side-effects such as process crashes, illegal instructions and invalid memory accesses. These effects enable detection of the very first attack, and without false-positives, flag it. This is all accomplished while having no prior-knowledge, signatures or dictionaries even if it is the first time in history the attack occurred.

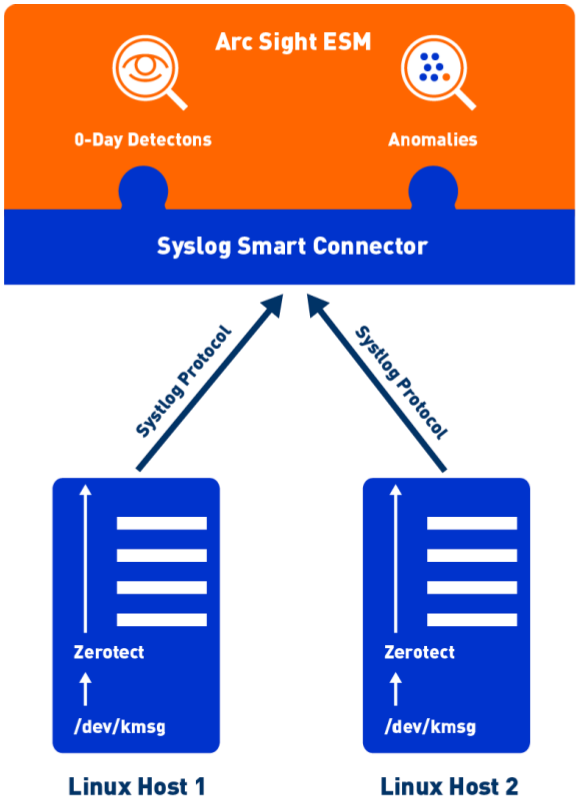
Key benefits

- Detect file-less memory-based zero-day attacks without any signatures/rules
- Structured visibility into free-form kernel logs for other analyses
- New Vulnerability (CVE) Disclosures and reporting
- Long-term and cross-machine analyses to learn/understand how attacker is adapting

Use cases

Fileless or memory-based attack occurs when an attacker operates directly in memory, these attacks are missed by traditional anti-malware solutions.

- Zerotect looks for the side-effects of these attacks rather than looking for the attack itself.



- Any time an attack fails, it produces system “faults”, which are monitored by Zerotect.

Zerotect provides general crash analysis and upstream remediation.

- All events gathered by Zerotect are useful and actionable with no false positives or negatives, which improve the security posture of the entire system.

Zerotect discloses new vulnerabilities.

- Since Zerotect detects zero-day attacks that have never before been seen it can help organizations raise new CVEs and perform responsible disclosure.

Additional information

For additional Micro Focus ArcSight information visit:
For additional Polyverse information visit: polyverse.com

About Polyverse

Polyverse develops leading-edge cybersecurity technology to build diversity across multiple system dimensions, stopping attacks before they start. Its technology is used by government and security-conscious organizations to mitigate against zero-day memory exploits. It is also embedded into devices, hardware and security solutions to provide the ultimate protection against hackers. Founded in 2015, Polyverse is led by founder and CEO Alex Gounares and brings together top talent from Microsoft, Amazon, Google, among others. CNBC recently named Polyverse as one of the world's top 100 startups.