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

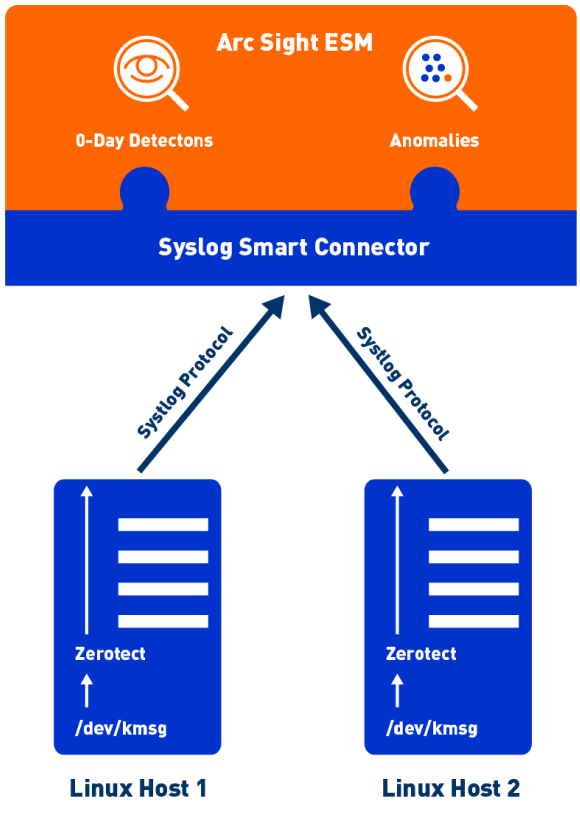
Detect zero-day exploits conclusively, without any prior knowledge, signatures or AI/ML

Finding, reporting and remediating zero-day attacks are the Holy Grail for information security professionals. Most detection agents are unable to detect "unknown" attacks like zero-day and file-less malware. Researchers spend years looking for these vulnerabilities. Whenever a new vulnerability is announced, enterprises scramble to quickly patch critical infrastructure. Waiting weeks or months for patches to be released, tested and deployed is not an option due to the destructive nature of these vulnerabilities.

On top of that, memory-based and file-less attacks are some of the toughest attacks to identify since 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 introduce 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, then interpreting and emitting them to ArcSight to raise alerts to SOC administrators, with no false positives or negatives.

Memory-based and file-less attacks produce side-effects such as process crashes, illegal instructions and invalid memory accesses. These aftereffects 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. Every attack is detected.



This capability is exponentially amplified when combined with Polyverse's Polymorphing for Linux Technology. A Polymorphic System is structured differently, and its structure is unknown to an attacker and impervious to a previously constructed attack. When an attacker attempts to exploit such a system, it simultaneously thwarts the attack, and in the process produces a fault that Zerotect detects and records, every time.

Therefore, when used as a complete analysis stack, Polyverse's Polymorphing and Zerotect detect attempted attacks, which are then reported and analyzed through ArcSight. Customers of Polyverse and Micro Focus experience compounded security benefits.

Key benefits

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

Use cases

- Looks for the side-effects of memory-based or file-less attacks rather than looking for the attack itself. Any time an attack occurs, the attack produces system "faults", which are detected.
- No false positives or negatives, all events gathered are useful and actionable
- Discloses new vulnerabilities by detecting zero-day attacks that have never before been seen, helping enterprises raise new CVEs and perform immediate remediation and disclosure
- Provides general crash analysis and upstream remediation

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.

About Micro Focus

Micro Focus delivers enterprise software to empower our 40,000 customers worldwide to digitally transform. With a broad portfolio, underpinned by a robust analytics ecosystem, the company enables customers to address the four core pillars of digital transformation: Enterprise DevOps, Hybrid IT Management, Predictive Analytics and Security, Risk & Governance. By design, these tools bridge the gap between existing and emerging technologies so customers can run and transform at the same time.