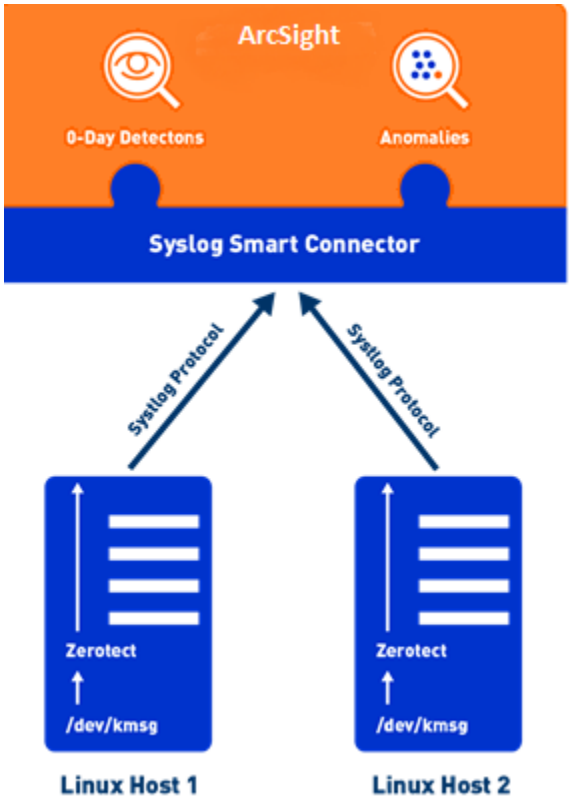
Detect zero-day cyberattacks with Micro Focus ArcSight and Polyverse Zerotect

Detect zero-day exploits conclusively and in near real-time, without any prior knowledge, predefined 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 fileless 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 fileless 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. As the attacker probes and makes attempts to inject the malware, these memory-based and fileless attacks produce side effects such as process crashes, illegal instructions and invalid memory accesses. Each of these failures is detected and recorded, without prior-knowledge, predefined signatures or dictionaries.

ArcSight and Zerotect introduce a new class of zero-day detection for enterprises and SOCs to improve their security posture, situational awareness and cyber response. Zerotect detects memory-based attacks on all Linux operating systems. It monitors and interprets various system events and records and emits suspect events to ArcSight, which then raises near real-time alerts to SOC administrators – with no false positives or negatives.



This capability is exponentially amplified when combined with Polyverse's Polymorphing for Linux Technology. A Polymorphic system's code base 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 for ArcSight to raise an alert on.

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 fileless zero-day attacks without any predefined signatures or rules
- No false positives or negatives, all events gathered are useful and actionable
- Near real-time alerting to the SOC by Micro Focus ArcSight, enabling immediate remediation response
- Discover and disclose new vulnerabilities by detecting zero-day attacks that have never before been seen, helping enterprises raise new CVEs
- Structured visibility into free-form kernel logs for other analyses
- Learn and understand how attacker is adapting through long-term and cross-machine analyses
- Provides general crash analysis and upstream remediation

Additional information

For additional Micro Focus ArcSight information visit:
https://marketplace.microfocus.com/arcsight/category/partner-integrations

For additional Polyverse information visit: polyverse.com

About Polyverse

Polyverse is a leading provider of zero-trust software cybersecurity solutions. Its Polymorphing technology protects against the most sophisticated attacks, even on unpatched and legacy systems. Used by governments and security-conscious organizations worldwide, Polyverse protects against memory exploits, script injections, supply-chain attacks and the like anywhere Linux runs, from devices to the cloud. CNBC has 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.