Siemplify ThreatNexus & Microfocus Arcsight Joint Solution Brief

Security Orchestration and Automation with Siemplify ThreatNexus Integration with MicroFocus ArcSight

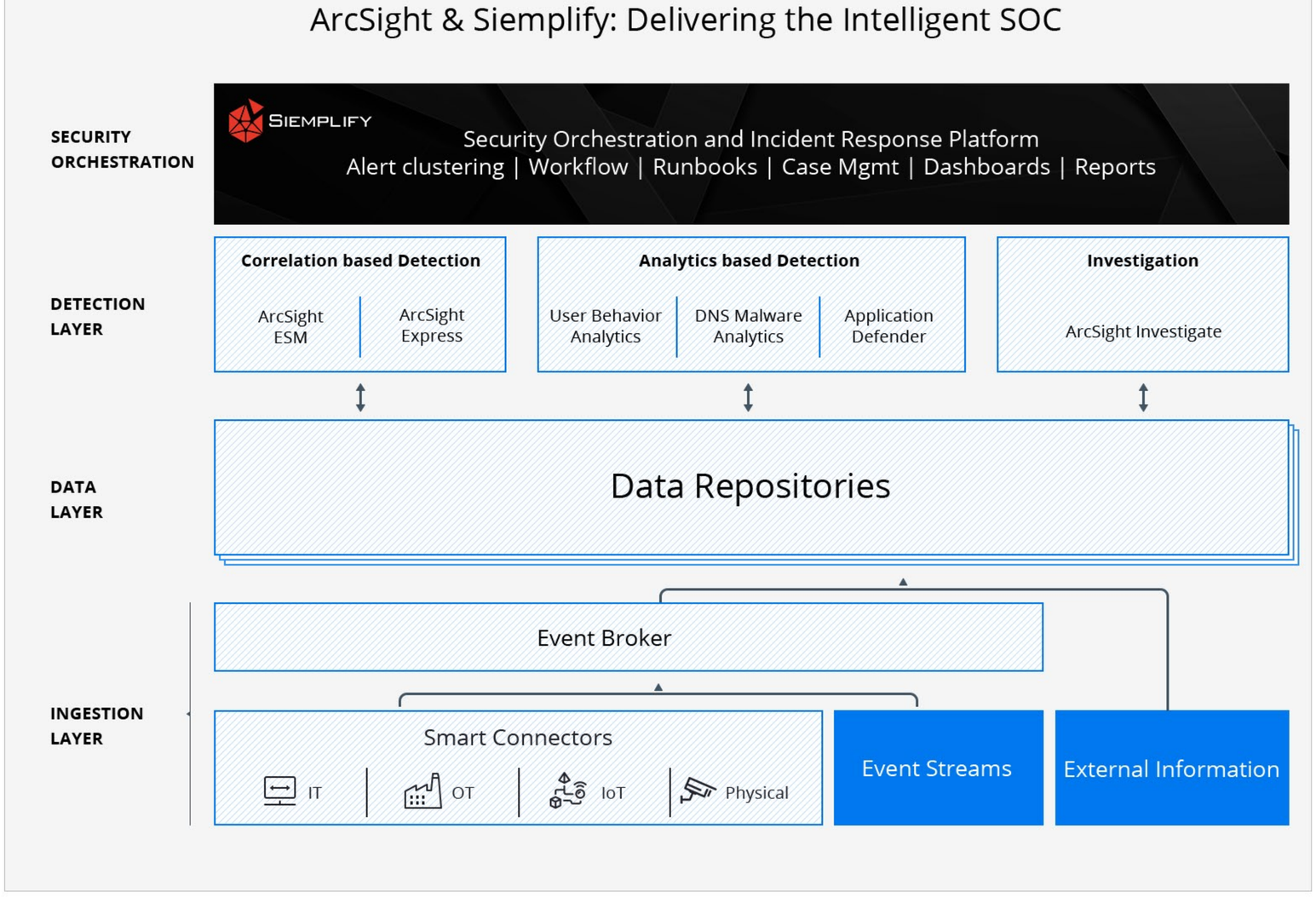
Security orchestration bridges the gap between amount of security alerts and analyst capacity. Executed effectively, an orchestration platform creates the integrated fabric across the security footprint bringing simplicity, context, and efficiency throughout security operations and incident response.

ThreatNexus is the only comprehensive security orchestration platform for the analyst to navigate the full scope of security operations and incident response.

MicroFocus (formerly HPE Software) is leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading profits from MicroFocus ArcSight, MicroFocus Fortify, and MicroFocus—Data Security, the MicroFocus Intelligence Platform uniquely delivers the advance correlation and analytics, application protection, and data security to protect today's hybrid IT infrastructure from sophisticated cyber threats.

Siemplify ThreatNexus is an integrated security orchestration platform designed for security teams to manage, investigate, and automate threat response from a single pane of glass. As the primary workbench for analysts, ThreatNexus provides the playbooks to drive consistency throughout the threat management process, delivering measurable ROI. ThreatNexus is the only comprehensive security orchestration platform to provide the full spectrum of case management, automation, and investigation giving analysts the ultimate balance in machine driven and analyst led response.

ARCSIGHT & SIEMPLIFY DELIVERING THE INTELLIGENT SOC



Coupled with ArcSight portfolio, ThreatNexus provides the day to day workbench for security teams to perform their jobs effectively and efficiently, giving them the command and control to confidently address all types of alerts and threats.

- ThreatNexus clusters, enriches, and contexualizes alerts
- Drives consistency throughout the threat management process and the multiple security controls by executing security processes and workflows
- Applies automation flexibly and selectively to optimize machine driven and human response
- Delivers comprehensive security operations center (SOC) management & visibility, from full lifecycle case management, to comprehensive dashboards, KPI's, and business intelligence
- Seamlessly integrates with ArcSight to enhance context of ArcSight cases and accelerate the investigation process

Solution Brief

ThreatNexus Security Orchestration & Incident Response Platform

Triage |Assess | Respond | Automate | Manage | Report

Common Uses Cases:

Alert clustering and case triage

As multiple alerts from different security controls are generated, ThreatNexus automatically consolidates and cluster the different alerts from the various tools into one cohesive interface, then automatically enriches these alerts with other important data sources within the ecosystem and provides analysts with the means to quickly and effectively triage. Fully informed this approach yields the highest level of productivity allowing low-priority alerts to be triaged and avoid escalation.

Workflow and automation

As correlations are generating alerts, the appropriate playbook would be executed within ThreatNexus to guide the analyst through the various step to finalize the determination of the case and trigger appropriate mitigation and remediation actions. All those will be properly collected into the case management system for reporting and auditing purposes.

Full Lifecycle SOC Management platform

With this complete workbench for the SOC team to process and navigate all types of alerts, cases, and incidents -- ThreatNexus delivers SOC Management unprecedented visibility and management of the people, process and technologies taking a role in the overall Security Operations life cycle. Setting and tracking the Key Performance Indicators that help organizations raise their security posture via the Intelligenct SOC.

Key benefits

- 5-to-1 consolidation of alerts into cases -- 80% reduction in triage volume
- 3x productivity of security analysts
- Process consistency throughout security operations
- Resolution time reduced by 70%
- Clarity and visibility of security posture

More Info

For additional MicroFocus information visit software.microfocus.com/en-us/home

For additional Siemplify information visit Siemplify.co

To learn more about Siemplify ThreatNexus
and give it a test drive

www.siemplify.co

contact@siemplify.co

facebook.com/siemplify