MICRO FOCUS

Data Sheet
Security

ArcSight Operational Health Check

Micro Focus® ArcSight Operational Health Check Services—a holistic ArcSight SIEM health check including reviews of technology, people, and processes.

Overview

Technology Review

Periodic health checks are an important part of maintaining optimal performance and often identify and resolve minor issues before they result in major performance degradations that impact system availability and user satisfaction.

Operational Review

ArcSight Operational Health Check Services are also designed to assist customers with evaluating their current SIEM security monitoring and response capabilities and offer recommendations on how best to mature those capabilities. This is achieved by reviewing your existing SIEM operations using Micro Focus Cyber Security Services' Security Operations Maturity Model (SOMM) and identifying areas for improvement.

The SOMM is a hybrid of the Capability Maturity Model Integration (CMMI) process improvement approach and best practices for security. At the end of the review, Micro Focus Security Services will present a SIEM Operations Capability Maturity Report including the overall scorecard on your SIEM security operations capabilities and recommendations on how best to improve.

Service Implementation

Evaluate Performance & Bottlenecks

During the operational health check, a trained Micro Focus Security Services specialist will perform activities that may include:

- Evaluate host operating systems running components of ESM for performance bottlenecks by monitoring memory and CPU utilization along with I/O throughput.
- Analyze log files of ESM components for error messages and other messages known to impact performance
- Analyze memory utilization of ESM content including rules and data monitors
- Evaluate query performance and indexing to ensure optimal query response times for reports and trends
- Review the ESM architecture for potential performance bottlenecks
- Document all findings and recommendations
- Implement recommended fixes as time allows

Quick View

Micro Focus ArcSight ESM ("ESM") Operational Health Check Services are designed to optimize the performance of ESM by identifying and resolving performance bottlenecks within system components including SmartConnectors, Manager, database, and content such as rules, reports, and data monitors.

Evaluate Operations

During the Operational Health Check, trained Micro Focus Security Services specialists will perform activities that may include:

- Review the customer's existing SIEM and security operations capability through documentation review, discussions and observations. The operational review will focus in these key functional areas:
  - **People:** Review organizational structure, roles and responsibilities, personnel on boarding, skill tracking, training and career development
  - **Process:** Review analytical, operational, technological and business processes that support the SIEM implementation
- Provide an Operational Review Report outlining key findings and recommendations for improving SIEM operations

Service Planning and Deployment

The Micro Focus Security Services specialist will schedule the delivery of This Service at a time mutually agreed upon between Micro Focus and the customer, which shall be during local Micro Focus standard business hours, excluding holidays, unless otherwise agreed by Micro Focus. Any services provided outside of standard business hours will be subject to additional charges.

The Micro Focus Security Services specialist perform activities that may include:
Schedule and attend a kick-off meeting to review objectives, schedule, required audience and deliverables

- Verify that prerequisites have been met
- Evaluate performance bottlenecks in the following areas: ESM architecture, SmartConnectors, Manager, database, content, and host operating systems running ESM components
- Meet with your key stakeholders in order to assess the people, process, and technology components of your security operations
- Observe operations and evaluate sample artifacts of SIEM and security operations
- Document findings and recommendations
- Prioritize recommendations with customer and implement as time permits during the duration of the Services. Close-out meeting to discuss key findings and recommendations

The Micro Focus Security Services specialist will be available to answer questions during the onsite or remote portions of the service delivery.

Service Eligibility

Prerequisites

The customer must provide the following for delivery of this service:

- Conference room with white board and projector
- Access to key stakeholders for interviews and group discussions:
  - **IT Security Sponsor:** This is the CISO, CSO, Director of IT Security, IT Security leadership, IT Leadership, or champion of the Initiative that the SIEM implementation supports
  - **SIEM / Security Operations Manager:** This is the person who leads the personnel who perform SIEM management and/or security event analysis
  - **Security Operations Personnel:** These are the people who perform review and analysis of security events in the SIEM
  - **Security Engineering:** These are the people responsible for the management of the SIEM, security devices, or other security technology
- Sufficient network connectivity, rack space, power, and cooling at the customer site to support the Micro Focus ArcSight ESM solution
- Micro Focus ArcSight ESM, Connector Appliance, and SmartConnector hardware and software components
- ArcSight ESM must be preinstalled and configured
- All information required in the completed pre-installation customer questionnaire
- For any onsite services delivery, all requisite logistical accommodations to the Micro Focus Security Services specialist including but not limited to adequate physical work location, access to the customer's network, internet access, telephone access, and access to the customer's offices where work will be performed
- For any onsite or remote services delivery, any requisite access to the customer's network and servers including but not limited to VPN token and client software, server names and IP addresses, and administrative user names and passwords. In addition, the customer will be responsible for all applicable data backup.

Service Limitations

This service will be delivered as a single, continuous event. Environments requiring multiple engagements or phases over longer periods of time are not included in this service, but can be accommodated at additional cost through a Statement of Work. Activities such as, but not limited to, the following are excluded from this service:

- Installation and configuration of Micro Focus software or appliance
- Racking of appliances or servers
- Development of FlexConnectors
- Delivery of standard Education offerings Performance testing or modeling services that, in the opinion of Micro Focus, are required due to unauthorized attempts by non-Micro Focus personnel to

install, repair, maintain, or modify hardware, firmware, or software

- Services required due to causes external to the Micro Focus-maintained hardware or software
- Any services not clearly specified in this document or services beyond the license limitations of the included products
- In addition, the customer will be responsible for all applicable data backup.

Customer Responsibility

- Contact a Micro Focus Security Services specialist within 90 days of the date of purchase to schedule the delivery of the Service
- Coordinate Service deployment on third-party-maintained hardware/software (if applicable) with Micro Focus
- Assign a designated person from the customer's staff who, on behalf of the customer, will grant all approvals, provide information, attend meetings, and otherwise be available to assist Micro Focus in facilitating the delivery of this Service
- Ensure that all Service prerequisites as identified in the Service Eligibility section are met
- Ensure the availability of all hardware, firmware, and software required by the Micro Focus Security Services specialist to deliver this Service
- Retain and provide to Micro Focus upon request all original software licenses, license agreements, license keys, and subscription service registration information, as applicable for this Service

The customer shall provide reasonable access and working space at the site as Micro Focus may reasonably request. The customer will provide Micro Focus and Micro Focus subcontractor staff standard telephone and dial-up or comparable data access to Micro Focus' Network at industry standard speeds. Micro Focus shall observe the customer work rules and security and safety policies while performing Micro Focus Services at the site of which Micro Focus is informed of in writing in advance and that are not inconsistent with Micro Focus' own business practices.

Duration

Delivery of this Service will not exceed a total of 80 service hours. This Service will be delivered by two (2) Micro Focus Security Services specialists and includes one (1) onsite visit for up to five (5) days in duration followed by offsite compilation of findings and the report generation, and remote delivery of final report and recommendations.

Terms

This offering consists of a consulting and training effort and is governed by the Micro Focus Customer Terms. All capitalized terms used in this Data sheet, but not otherwise defined, will have the meaning assigned to them in the Terms. For purposes of this Data sheet, "services" mean consulting, integration, professional services or technical services performed by Micro Focus under this Data sheet. Services excludes hardware maintenance and repair, software maintenance, education services, or other standard support services provided by Micro Focus; software as a service, and outsourcing services.

Acceptance of Deliverables occurs upon delivery.

Hiring of Employees. You agree not to solicit, or make offers of employment to, or enter into consultant relationships with, any Micro Focus employee involved, directly or indirectly, in the performance of services hereunder for one (1) year after the date such employee ceases to perform services under the terms of this Data sheet. You shall not be prevented from hiring any such employee who responds to a general hiring program conducted in the ordinary course of business and not specifically directed to such Micro Focus employees.

Authorization to Install Software. During the provision of services, Micro Focus may be required to install copies of third-party or Micro Focus-branded software and be required to accept license terms accompanying such software ("Shrink-Wrap Terms") on your behalf. Shrink-Wrap Terms may be in electronic format, embedded in the software, or contained within the software documentation. You hereby acknowledge that it is your responsibility to review Shrink-Wrap Terms at the time of installation, and hereby authorizes Micro Focus to accept all Shrink-Wrap Terms on its behalf.

Intellectual Property. Micro Focus may provide Micro Focus tools, templates, and other pre-existing intellectual property of Micro Focus during the course of providing services ("Micro Focus Pre-existing IP"). Micro Focus Pre-existing IP does not include, nor is considered a part of, either the Deliverables or Micro Focus software products. Micro Focus retains all intellectual property ownership rights in such Micro Focus Pre-existing IP. All Micro Focus Pre-existing IP is Micro Focus Confidential Information. Micro Focus Pre-existing IP may be governed by additional license terms that are embedded in the Micro Focus Pre-existing IP.

Payment and Validity

This offering will be pre-billed. You agree to pay invoiced amounts within thirty (30) days of the invoice date. If applicable, you must schedule delivery of the offering to be completed within a period of one (1) year from the date of purchase. Notwithstanding the previous

Contact us at:
www.microfocus.com

Like what you read? Share it.

sentence, Micro Focus' obligations to deliver the offering under this Data sheet are considered fulfilled and your rights of receipt of the offering under this Data sheet will expire one (1) year from the date of purchase.

Pricing for the offering may vary by country.

Cancellation

To avoid a Cancellation Fee as defined herein, you shall notify Micro Focus in writing of cancellation or rescheduling at least ten (10) business days prior to the offering start date. Cancellations or rescheduling with less than ten (10) business days notification will incur 100% of the offering fee ("Cancellation Fee"). If you cancel with ten (10) or more business days in advance of scheduled delivery, you may reschedule only if delivery will be complete within one year from the purchase date.

Change in Scope

Changes in scope are not allowed. You can request additional or different services, if available and at additional cost, through a statement of work or change order.