Service Description

ArcSight SIEM as a Service

Log Management and Compliance

November 2021

MICRO FOCUS

Contents

“This Service Description describes the components and services included in Micro Focus ArcSight SIEM Software-as-a-Service (which also may be referred to as “SaaS”). Unless otherwise agreed to in writing this Service Description is subject to the Micro Focus Customer Terms for Software-as-a-Service or the applicable Micro Focus Pass-Through Terms and represents the only binding terms governing Micro Focus International plc and its affiliates (“Micro Focus”) respective obligations regarding its provision of this SaaS to the end-user customer. Any other descriptions of the features and functions of the SaaS, public statements, including advertisements, shall not be deemed as additional features or functionalities that Micro Focus is required to deliver

Standard Service Features

High Level Summary

ArcSight SIEM for SaaS with Log Management and Compliance, (LMAC) is a threat hunting, log search and management tool that increases SOC analyst effectiveness by making billions of logged events available for quick and easy search and visualization. LMAC helps SOC analysts gain a deeper understanding of specific alerts and hunt for hidden security threats. ArcSight SIEM with LMAC collects device logs by leveraging ArcSight's SmartConnector framework for log collection, routing, and enrichment. Once collected and received into the SaaS environment, logs are persisted into ArcSight's security information and event model and are optimized for search. LMAC provides an easy-to-understand search language to search logs and retrieve datasets that can be further explored by creating custom charts or selecting from a chart library. LMAC also supports log archival and compliance use cases and a full suite of reporting capabilities.

ArcSight SIEM as a Service with Log Management and Compliance Service Delivery Components

The Log Management and Compliance offering is provisioned with all of the components required to deliver a fully functional product/service offering. It is delivered as a single tenant within a multi-tenant environment. Each customer has their data logically and securely segregated in such an architecture. Each customer is referred to as a tenant.

Service Offering Options

Definitions

There are currently four (5) SKU's available for ArcSight SIEM for SaaS with Log Management and Compliance.

ArcSight SIEM as a Service Base Platform SKU

SA-AB989 is the ArcSight SIEM as a Service base platform SKU. The Base Platform SKU has a fixed price and will require an "Add-On" SKU to be quoted as well.

Log Management and Compliance Add-On SKU's

Log Management and Compliance SKU's all make use of the following Events per Second, (EPS) Tiering scale for pricing.

500 – 999
1000-2499
2500-4999
5000-7499
7500-9999
10,000-14999

15,000-24999
25,000-34999
35,000-49,999
50,000+

SA-AB989 is the ArcSight SIEM as a Service Base Platform
SA-AB849 is the 1-year Log Management and Compliance Add-On SKU.
SA-AB850 is the 2-year Log Management and Compliance Add-On SKU.
SA-AB851 is the 3-year Log Management and Compliance Add-On SKU.
SA-AB852 is the Archival Data Retention SKU.

Archive Data Retention SKU

The Archive data retention SKU is available to handle the "one-off" requests to add additional time for data retention. For example, a customer purchases SA-AB849, which provides for 1 year of data retention. At the end of the subscription the customer wants to renew for another year and wants to retain the previous year of data. The customer will need to purchase SA-AB849 and SA-AB852 in order to retain the previous year of collected data. The same EPS tiers are defined for both the Log Retention and Compliance SKU's as well as the "Archive Data Retention" SKU.

In the case of the 2-year and 3-year SKU options, the Archive data retention capabilities are embedded in those SKU definitions.

ArcSight SIEM as a Service Delivery Components

The ArcSight SIEM as a Service offering is provisioned with all of the components required to deliver a fully functional product offering. Each customer has their data logically and securely segregated in such an architecture. Each customer is referred to as a tenant.

Method for Accessing and Downloading Software Components

During the "On Boarding" process for ArcSight SaaS the customer will be given access to the CyberRes Service portal. This will facilitate submitting trouble tickets. A private AWS S3 location will also be made available which is where the customer will direct all data for ingest. In this S3 location there will also be a specific directory that will contain the software components available for download to facilitate data ingest from on-prem to the SaaS AWS tenant.

SaaS Operational Services

Operational Services	
Welcome Pack	✓

Help Desk Support	✓
Virtual Connector Host Appliance (vCHA, downloadable)	✓
ArcSight Smart Connector Library (downloadable)	✓
ArcSight Management Center (ArcMC, downloadable)	✓

✓ **= Included**

Virtual Connector Host Appliance (vCHA)

The Connector Host Appliance (CHA) was originally developed as a hardware appliance to enhance the deployment options available for the broad array of Smart Connectors that are currently available. As part of the ArcSight SIEM as a Service offering, Micro Focus has enhanced the CHA into a downloadable Open Virtualized Appliance (OVA) which can be imported into VMware vCenter for easy virtual deployment. This enables on-premise log collection which is then fed to the SaaS environment for search, hunt and retention availability.

ArcSight Smart Connectors

ArcSight uses smart connectors within the environment. Configuration changes can be made to include an additional destination for the data sources in question. The destination will be a web accessible storage location that is available via the Cloud instance of the ArcSight SIEM as a Service tenant that has been made available. With ArcSight Smart Connectors v8.2 and higher, an export directly to S3, is made available. This method requires a credential to be set during installation. This credential has to have a persistent AWS ID/Key with the correct role.

Once the data sources are identified and set up to be collected by ArcSight SIEM as a Service, and a secure connection has been established data ingest into ArcSight SIEM as a Service can begin.

ArcSight Management Center, (ArcMC) is also available for download for the purpose of managing the Smart Connectors, if desired.

All usage of downloaded components, CHA, Smart Connectors and ArcMC, are to be used ONLY for the purpose of populating ArcSight SaaS services with the customers data and are subject to termination in accordance with the ArcSight SaaS subscription service.

Application Administration

All data provided to the ArcSight SIEM as a Service will be considered Customer-provided SaaS Data per the Micro Focus Customer SaaS Terms. Micro Focus is not responsible for the accuracy of the data provided by the customer.

Service & Support Components

The Customer may contact Micro Focus via a dedicated email address cyberressupport@microfocus.com. The Micro Focus Support Team will either provide support to the Customer directly or coordinate delivery of this support. The severity of the request determines the response and resolution time. Online support and product documentation are available at the ArcSight SIEM as a Service support site locations.

- Standard support is available to users which allows for the logging of online issues as well as the ongoing management of issues and exchange of information
- Support is for subscription services only and does not include custom integrations.
- Support focus is on a break fix philosophy
- Standard support is on an as needed per SLA basis
- Additional Premium support is also available
- All support provided remotely

Service Support

The Customer may contact Micro Focus through the CyberResSupport@microfocus.com or access CyberRes Portal at https://support.cyberreshelp.com, or call 1(855)982-2261 . The Micro Focus Support Team will either provide support to the Customer directly or coordinate delivery of this support. The severity of the request determines the response from the team.

Severity Level	Technical response	Update Frequency	Target For Resolution	What Qualifies?
1	Immediate	Hourly	4 hours	Total or substantial failure of service. Known or suspected security events
2	30 mins	Every 2 hours	8 hours	Significant degradation of service, major feature inability
3	4 hours	Every 8 hours	24 hours	Performance issues outside the of the norm but not substantial enough to prevent usability of a feature. Issues with reports generated from within the customer's Tenant
4	As available	As available	Determined by the customer impact or LOE	Bugs in deployed products not substantial enough to prevent required customer functionality from being accessible but requiring development time to resolve

Service Monitoring

Micro Focus monitors ArcSight SIEM as a Service solution components for 24x7 availability. Micro Focus uses a centralized notification system to deliver proactive communications about application changes, outages and scheduled maintenance.

Capacity and Performance Management

The ArcSight SIEM as a Service environment is continually monitored for performance status. Proactive capacity and performance management procedures are in place to ensure the architecture of the environment meets the needs of its customers. The architecture allows for addition of capacity to applications, databases and storage.

Operational Change Management

Micro Focus follows a set of standardized methodologies and procedures for efficient and prompt handling of changes to SaaS infrastructure and application, which enables beneficial changes to be made with minimal disruption to the service. Changes to production environments are tested and reviewed prior to implementation to ensure they are appropriately scheduled and tested before promotion to production.

Solution Data Backup and Retention

The data backup and retention described in this section are part of Micro Focus's overall business continuity management practices designed to attempt to recover availability to Customer of ArcSight SIEM as a Service application and access to the ArcSight SIEM as a Service application, following an outage or similar loss of service.

Micro Focus's standard storage and backup measures are Micro Focus's only responsibility regarding the retention of this data, despite any assistance or efforts provided by Micro Focus to recover or restore Customer's data.

Disaster Recovery

Business Continuity Plan

Micro Focus SaaS continuously evaluates different risks that might affect the integrity and availability of Micro Focus SaaS. As part of this continuous evaluation, Micro Focus SaaS develops policies, standards and processes that are implemented to reduce the probability of a continuous service disruption. Micro Focus documents its processes in a business continuity plan ("BCP") which includes a disaster recovery plan ("DRP"). Micro Focus utilizes the BCP to provide core Micro Focus SaaS and infrastructure services with minimum disruption. The DRP includes a set of processes that Micro Focus SaaS implements and tests Micro Focus SaaS recovery capabilities to reduce the probability of a continuous service interruption in the event of a service disruption.

Backups (High Availability and Durability)

Micro Focus SaaS utilizes cloud-native functions such as replication between primary and secondary availability zones to ensure data availability and recoverability. All replicas reside within the same governmental compliance boundary to ensure adherence to all applicable data residency regulations. Real-time replication is used between primary and standby nodes to facilitate an RPO of 2 hours (Real-time replication is used between nodes). No removable media is used at any time to ensure the protection of customer data.

SaaS Security

Micro Focus maintains an information and physical security program designed to protect the confidentiality, availability and integrity of Customer Personal Data and confidential information (the "Micro Focus Security Program").

Technical and Organizational Measures

This section describes Micro Focus´s standard technical and organizational measures, controls and procedures, which are intended to help protect the Customer-provided SaaS Data. Micro Focus regularly tests and monitors the effectiveness of its controls and procedures. No security measures are or can be completely effective against all security threats, present and future, known and unknown. The measures set forth in this section may be modified by Micro Focus but represent a minimum standard. Customer remains responsible for determining the sufficiency of these measures.

Physical Access Controls

Micro Focus maintains physical security standards designed to prohibit unauthorized physical access to the Micro Focus equipment and facilities used to provide SaaS and include Micro Focus data centers and data centers operated by third parties. This is accomplished through the following practices:

- presence of on-site security personnel on a 24x7 basis
- use of intrusion detection systems
- use of video cameras on access points and along perimeter
- Micro Focus employees, subcontractors and authorized visitors are issued identification cards that must be worn while on premises
- monitoring access to Micro Focus facilities, including restricted areas and equipment within facilities
- Securing equipment hosting Customer-provided SaaS Data in designated caged areas; and maintaining an audit trail of access.

Access Controls

Micro Focus maintains the following standards for access controls and administration designed to make Customer-provided SaaS Data accessible only by authorized Micro Focus personnel who have a legitimate business need for such access:

- secure user identification and authentication protocols
- authentication of Micro Focus personnel in compliance with Micro Focus standards and in accordance with ISO27001 requirements for segregation of duties
- Customer provided SaaS data is accessible only by authorized Micro Focus personnel who have a legitimate business need for such access, with user authentication, sign-on and access controls
- employment termination or role change is conducted in a controlled and secured manner
- administrator accounts should only be used for the purpose of performing administrative activities
- each account with administrative privileges must be traceable to a uniquely identifiable individual
- all access to computers and servers must be authenticated and within the scope of an employee's job function
- collection of information that can link users to actions in the Micro Focus SaaS environment
- collection and maintenance of log audits for the application, OS, DB, network and security devices according to the baseline requirements identified
- restriction of access to log information based on user roles and the "need-to-know;" and prohibition of shared accounts.
- use of multi-factor authentication to provide state-of-the-art access to the SaaS systems.

Availability Controls

Micro Focus´s business continuity management process includes a rehearsed method of restoring the ability to supply critical services upon a service disruption. Micro Focus's continuity plans cover operational shared infrastructure such as remote access, active directory, DNS services, and mail services. Monitoring systems are designed to generate automatic alerts that notify Micro Focus of events such as a server crash or disconnected network.

Data Segregation

Micro Focus SaaS environments are segregated logically by Micro Focus SaaS access control mechanisms. Internet-facing devices are configured with a set of access control lists (ACLs), which are designed to prevent unauthorized access to internal networks. Micro Focus uses security solutions on the perimeter level such as: firewalls, IPS/IDS, proxies and content-based inspection in order to detect hostile activity in addition to monitoring the environment's health and availability.

Data Encryption

Micro Focus SaaS uses industry standard techniques to encrypt Customer-provided SaaS Data in transit. All inbound and outbound traffic to the external network is encrypted.

Audit

Micro Focus appoints an independent third party to conduct an annual audit of the applicable policies used by Micro Focus to provide the applicable Micro Focus ArcSight SIEM as a Service solution. A summary report or similar documentation will be provided to Customer upon request. Subject to the execution of Micro Focus's standard confidentiality agreement, Micro Focus agrees to respond to a reasonable industry standard information security questionnaire concerning its information and physical security program specific to Micro Focus SaaS provided pursuant to the applicable Supporting Material no more than once per year. Such information security questionnaire will be considered Micro Focus Confidential Information.

Micro Focus Security Policies

Micro Focus conducts annual reviews of its policies around the delivery of SAAS against ISO 27001, which includes controls derived from ISO 27034 – "Information Technology – Security Techniques – Application Security." Micro Focus regularly re-evaluates and updates its information and physical security program as the industry evolves, new technologies emerge, or new threats are identified.

Security Incident Response

In the event Micro Focus confirms a security incident resulted in the loss, unauthorized disclosure or alteration of Customer-provided SaaS Data ("Security Incident"), Micro Focus will notify Customer of the Security Incident and work to mitigate the impact of such Security Incident. Should Customer believe that there has been unauthorized use of Customer's account, credentials, or passwords, Customer must immediately notify Micro Focus Security Operations Center via cyberressec@microfocus.com.

Micro Focus Employees and Subcontractors

Micro Focus requests that all employees involved in the processing of Customer-provided SaaS Data are authorized personnel with a need to access the Customer-provided SaaS Data, are bound by appropriate confidentiality obligations and have undergone appropriate training in the protection of customer data. Micro Focus requests that any affiliate or third-party subcontractor involved in processing Customer provided SaaS Data enters into a written agreement with Micro Focus, which includes confidentiality obligations substantially similar to those contained herein and appropriate to the nature of the processing involved.

Customer-provided SaaS Data

All data provided to ArcSight SIEM as a Service will be considered Customer-provided SaaS Data per the Micro Focus Customer SaaS Terms. Customer will be responsible for all data cleansing and data accuracy as part of any assessment request. Micro Focus is not responsible for the accuracy of the data provided by the customer.

Scheduled Maintenance

To enable Customers to plan for scheduled maintenance by Micro Focus, Micro Focus reserves predefined timeframes to be used on an as-needed basis.

A twenty-four-hour period once a quarter starting at Saturday, midnight in the local data center region, and ending on Sunday, midnight.

- This window is considered an optional placeholder for major releases and events that could be significantly service impactful. If the window is to be exercised, and a major disruption expected, all customers should be notified no later than ten business days before.

A two-hour maintenance window once a month starting Wednesday, midnight in the local data center region.

- This is for patching of environments. Patching should be done in a non-service disrupting fashion; however, some elements may require a brief outage to update properly. Customers will be notified at least five business days in advance if any actual service disruption is expected.

A four-hour maintenance window once a month starting Saturday, midnight in the local data center region.

- This time is set aside for system updates and product releases that cannot be performed without a visible customer impact. Use of this window is optional, and customers should be notified at least ten business days in advance if any outage is expected.

In case of any holiday conflicts, the regularly scheduled window will automatically fall to the following week on the same day of the week.

Micro Focus determines whether and when to apply a SaaS Upgrade to Customer's Micro Focus ArcSight SIEM as a Service solution. Unless Micro Focus anticipates a service interruption due to a SaaS Upgrade, Micro Focus may implement a SaaS Upgrade at any time without notice to Customer. Micro Focus aims to use the Scheduled Maintenance windows defined herein to apply SaaS Upgrades. Customer may be required to cooperate in achieving a SaaS Upgrade that Micro Focus determines in its discretion is critical for the availability, performance, or security of Micro Focus ArcSight SIEM as a Service.

Service Decommissioning

Customer may cancel Micro Focus SaaS by providing Micro Focus with sixty (60) days written notice prior to the expiration of the SaaS Order Term ("Cancellation"). Such Cancellation shall be effective upon the last day of the then current SaaS Order Term. Upon Cancellation, expiration, or termination of the SaaS Order Term, Micro Focus may disable all Customer access to ArcSight ArcSight SIEM as a Service SaaS solution, and Customer shall promptly return to Micro Focus (or at Micro Focus's request destroy) any Micro Focus Materials.

Micro Focus will make available to Customer such data in the format generally provided by Micro Focus. The target timeframe is set forth below in the Termination Data Retrieval Period SLA section. After such time, Micro Focus shall have no obligation to maintain or provide any such data, which will be deleted in the ordinary course.

Service Level Commitments and Service Level Objectives

Micro Focus provides clear, detailed, and specific Service Level Objectives (SLOs) for the services that SaaS provides to its customers. These SLOs are targets used by Micro Focus to deliver the service and are provided as guidelines. They in no way create a legal requirement or obligation for Micro Focus to always meet these objectives.

1. **Solution Provisioning Time SLO**
   Solution Provisioning is defined as the Micro Focus ArcSight SIEM as a Service solution being available for access over the internet. Micro Focus targets to make Micro Focus ArcSight SIEM as a Service on SaaS available within five (5) business days of the customer's purchase order (PO) being booked within the Micro Focus order management system. Making SIEM as a Service "available" to the customer is defined by working login access definitions being sent to the customer so they can gain access to their isolated tenant application.

2. **Tenant Off boarding SLO**
   For production engagements, Micro Focus guarantees a tenant off boarding time of two days from the time in which the Customer submits the formal written request.

3. **User Removal SLO**
   Micro Focus guarantees that after the completion of this request, all data stored relevant to the customer users, current or archived will be removed and no longer be stored or available within the application.

4. **Measurement Method**
   On a quarterly basis, the availability of stored data, current or archived will be measured using the measurable days in the quarter (total days minus planned downtime, including maintenance, upgrades, etc.) as the denominator. The numerator is the denominator minus the number of days where a tenant's deadline is not met, to give the percentage of days that met the SLA (e.g., 119 days / 120 possible days = 99% availability).

5. **Boundaries and Exclusions**
   The Analytical Results SLA Metric shall not apply in any of the following exceptions, and neither the ArcSight SIEM as a Service will be considered unavailable, nor any Service Level Failure be deemed to occur in connection with any failure to meet the requirement or impaired ability of Customer or its Authorized Users to access or use the ArcSight SIEM as a Service solution:
   - Overall Internet congestion, slowdown, or unavailability
   - Unavailability of generic Internet services (e.g., DNS servers) due to virus or hacker attacks
   - Force majeure events as described in the terms of the SaaS agreement
   - Actions or omissions of Customer (unless undertaken at the express direction of Micro Focus) or third parties beyond the control of Micro Focus

- Unavailability due to Customer equipment or third-party computer hardware, software, or network infrastructure not within the sole control of Micro Focus
- Scheduled Maintenance
- Scheduled Version Updates

6. **Reporting**
   Micro Focus will provide Analytical Results SLA Report ("SLA Report") to the Customer upon request. If the Customer does not agree with the SLA Report, written notice of non-agreement must be provided to Micro Focus within fifteen (15 days) of receipt of the SLA Report

Termination Data Retrieval Period SLO

The Termination Data Retrieval Period is defined as the length of time in which the customer can retrieve a copy of their customer ArcSight SIEM as a Service data from Micro Focus. Micro Focus targets to make available such data for download in the ArcSight SIEM as a Service format generally provided by Micro Focus for 30 days following the termination of the SaaS Order Term.

Standard Service Requirements

Roles and Responsibilities

This section describes general Customer and Micro Focus responsibilities relative to the ArcSight SIEM as a Service SaaS solution. Micro Focus's ability to fulfill its responsibilities relative to SaaS is dependent upon Customer fulfilling the responsibilities described below and elsewhere herein:

Customer Roles and Responsibilities

Customer Role	Responsibilities
Business Owner	• Owns the business relationship between the customer and Micro Focus • Owns the business relationship with the range of departments and organizations using the ArcSight SIEM as a Service SaaS solution • Manages contract issues
Subject Matter Expert	• Leverages & educates other users about the product functionality designed by the ArcSight SIEM as a Service SaaS solution • Provides periodic feedback to the ArcSight SIEM as a Service Administrator

Micro Focus Roles and Responsibilities

Micro Focus Role	Responsibilities
Primary Support Contact (PSC)	• Serves as the customer liaison to Micro Focus • Coordinates Micro Focus resources including system and process experts as necessary as well as day to day issues with the SOC staff • Facilitates ongoing mentoring • Coordinates with the customer during required and periodic maintenance • Oversees the customer onboarding process
Service Operation Staff (SOC)	• Primary point of contact for service requests. • The Service Operations Center staff is responsible for all services such as support and maintenance, or issues regarding availability of the ArcSight SIEM as a Service SaaS solution • Provides 24x7 application support
Operations Staff (Ops)	• Monitors the ArcSight SIEM as a Service SaaS solution for availability • Provides 24x7 SaaS infrastructure and application support • Performs system-related tasks such as backups, archiving, and restoring instances according to Micro Focus's standard practices

Assumptions and Dependencies

This Service Description is based upon the following assumptions and dependencies between the Customer and Micro Focus:

- Customer must have internet connectivity to access this Micro Focus ArcSight SIEM as a Service SaaS Service.
- Micro Focus ArcSight SIEM as a Service SaaS Service will be performed remotely and delivered in English only.
- A SaaS Order term is valid for a single application deployment, which cannot be changed during the SaaS Order term.
- The service commencement date is the date on which Customer's purchase order (PO) is booked within the Micro Focus Order Management system. The term of service will begin within five (5) business days of the customer's purchase order (PO) being booked within the Micro Focus Order Management system.
- The service commencement date is the date on which Customeŕ s application / tenant is made available to its users.

- The import of Customer data into the ArcSight SIEM as a Service SaaS solution during the implementation requires that the information is made available to Micro Focus at the appropriate step of the solution implementation and in the Micro Focus designated format.
- Customer must ensure that its administrators maintain accurate contact information with Micro Focus SaaS.
- Customer has determined, selected, and will use options in the Customer environment that are appropriate to meet its requirements, including information security controls, connectivity options, and business continuity, backup and archival options.
- Customer will establish and follow secure practices for individual account-based access for accountability and traceability.

Furthermore, this Micro Focus ArcSight SIEM as a Service is provided based on the assumption that Customer will implement and maintain the following controls in its use of Micro Focus ArcSight SIEM as a Service:

- Appointing authorized users
- Configuring its Micro Focus ArcSight SIEM as a Service Service account to require that end user passwords are sufficiently strong and properly managed
- Procedures for access approvals, modifications and terminations.

Good Faith Cooperation

Customer acknowledges that Micro Focus's ability to perform the Services depends upon Customer's timely performance of its obligations and cooperation, as well as the accuracy and completeness of any information and data provided to Micro Focus. Where this Service Description requires agreement, approval, acceptance, consent or similar action by either party, such action will not be unreasonably delayed or withheld. Customer agrees that to the extent its failure to meet its responsibilities results in a failure or delay by Micro Focus in performing its obligations under this Service Description, Micro Focus will not be liable for such failure or delay.