Service Description

ArcSight Intelligence for CrowdStrike

August 2023

Contents

This Service Description describes the components and services included in Micro Focus ArcSight Intelligence for CrowdStrike Software-as-a-Service (which also may be referred to as "SaaS") and, unless otherwise agreed to in writing, is subject to the Micro Focus Customer Terms for Software-as-a-Service ("SaaS Terms") found at https://www.microfocus.com/en-us/legal/software-licensing. Capitalized terms used but not defined herein shall have the meanings set forth in the SaaS Terms.

Standard Service Features

High Level Summary

ArcSight Intelligence provides a security analytics capability, previously known as Interset Security User Entity Behavioral Analytics (UEBA), whereby entities such as user accounts, workstations, and servers, are scored for risk based on the scope and scale of anomalies observed. It uses online unsupervised machine learning, which means that the solution automatically builds baseline data for all behaviors being monitored (aka, models). The actual models that are triggered are determined by the type of data being ingested as well as the data attributes that are present in the data.

The unsupervised machine learning approach is ideally suited to help threat hunters find insider threats and external advanced threats (such as nation-state attacks) that manifest as internal threats. This is because the nature of these types of advanced threats is such that an exhaustive set of examples cannot practically be described. This makes these types of threats impossible to find with supervised machine learning.

SaaS Delivery Components

SaaS Delivery Components	
One Production Instance	✓
ArcSight Intelligence Threat Hunting	O
✓ **= Included**	
O **= Optional for a fee**	

The ArcSight Intelligence for CrowdStrike SaaS offering is provisioned using a single Tenant within a multi-tenant environment. Each customer has their data logically and securely segregated in such an architecture. Each customer is called a tenant.

ArcSight Threat Hunting
The Threat Hunting Service for this offering is designed to maximize the value obtained from the solution, by minimizing the amount of time to detect potentially malicious activity and maximize the opportunity to catch malicious activity before a breach occurs.

Threat hunting resources are difficult to attract and retain. This service allows organizations to extend their capacity without committing to permanent headcount increases.

ArcSight Threat Hunting	
Daily threat hunting in your CrowdStrike data	✓
Weekly reports and optional meeting to review activities that were found	✓
Critical escalation for urgent issues discovered while threat hunting	✓
✓ **= Included**	

SaaS Operational Services

Operational Services	
Welcome Pack	✓
Help Desk Support	✓
✓ = Included	

Architecture Components

The ArcSight Intelligence for CrowdStrike Offering is a SaaS-based analytics engine that consumes CrowdStrike EDR events, analyses those events for risky, unusual behaviors, and provides daily results back. The CrowdStrike application periodically sends data to the ArcSight Intelligence for CrowdStrike analytic engine for analysis via API integration, and analytical results are published daily via the ArcSight Intelligence UI for exploration.

The ArcSight Intelligence as a Service offering is a multi-tenant environment, meaning that each customer receives their own unique tenant. This tenant segregates and secures their analyses and underlying data from all other tenants.

Micro Focus does not install, deploy, or manage on-premises components that may be required to use ArcSight Intelligence SaaS.

Application Administration

All data provided to the ArcSight Intelligence for CrowdStrike will be considered SaaS Data per the Micro Focus Customer SaaS Terms. CrowdStrike is responsible for all data collection and data accuracy as part of any assessment request. Micro Focus is not responsible for the accuracy of the data provided by CrowdStrike. The import of Customer data into the ArcSight Intelligence for CrowdStrike solution requires that the information is made available to Micro Focus at the appropriate step of the ArcSight Intelligence for CrowdStrike solution and in the agreed-to format. The analysis will be performed remotely and delivered in English only.

Analytical Results Delivery

The ArcSight Intelligence for CrowdStrike application performs its analysis once a day at a different time for each tenant. These results include:

- Entity risk scores
- Anomalous events
- Descriptions and visualizations for anomalous events

The Analytics process will generate a number of outputs. The main outputs are the riskiest entities ranked by risk score, along with the anomalies that impact the entity risk scores. Also contained in the output are the identified events that participated in the raising of these risk scores.

Service Support

Customer may request support from Micro Focus by submitting online support tickets (https://support.cyberreshelp.com) or by telephone (1 (855) 982-2261). The Micro Focus Support Team will either provide support to the Customer directly or coordinate delivery of this support.

Micro Focus staffs and maintains a 24x5x52 weeks Service Operations Center with on-call coverage on weekends and holidays for Severity 1 issues which will be the single point of contact for all issues related to the support for SaaS. Customer will maintain a list of authorized users who may contact Micro Focus for support. Customer's authorized users may contact Micro Focus for support via the Web portal or telephone 24 hours a day, 7 days a week.

The severity of the request determines the response from the team.

Severity Level	Technical Response	Update Frequency	Target For Resolution	What Qualifies?
1	Immedate	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 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	Issues 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 Intelligence for CrowdStrike 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 Intelligence as a Service SaaS 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.

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 Intelligence for CrowdStrike application and access to the ArcSight Intelligence for CrowdStrike 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.

SaaS Data

The following types of SaaS Data reside in the SaaS environment:

- Security events collected from CrowdStrike as authorized by Customer; these events can contain, but are not limited to:
    - Identities of various entities (users, machines, etc.), including user ids, domain names and email addresses
    - Actions performed by entities
    - Files and file shares accessed
    - IP addresses / URLs accessed
- List of Customer-authorized users allowed to access the offering

Micro Focus performs a backup of SaaS Data every day. Micro Focus retains each backup for the most recent seven (7) days.

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. Customer may request via a service request for Micro Focus to attempt to restore such data from Micro Focus's most current backup. Micro Focus will be unable to restore any data not properly entered by Customer, or lost or corrupted at the time of backup or if Customer´s request comes after the 7 days data retention time of such backup.

Disaster Recovery for SaaS

Business Continuity Plan

Micro Focus continuously evaluates different risks that might affect the integrity and availability of SaaS. As part of this continuous evaluation, Micro Focus 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 SaaS and infrastructure services with minimum disruption. The DRP includes a set of processes that implements and tests SaaS recovery capabilities to reduce the probability of a continuous service interruption in the event of a service disruption.

Backups
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 SaaS Data.

Technical and Organizational Measures

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
- Maintaining an audit trail of access

Access Controls

Micro Focus maintains the following standards for access controls and administration designed to make 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
- 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 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”
- Prohibition of shared accounts

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.

Controls regarding disruption prevention include:

- Uninterruptible power supplies (UPS) and backup power generators
- At least two independent power supplies in the building
- Robust external network connectivity infrastructure

Data Segregation

SaaS environments are segregated logically by 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 uses industry standard techniques to encrypt 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 SaaS. A summary report or similar documentation will be provided to Customer upon request. Subject to Customer’s 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 SaaS 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 SaaS Data (“Security Incident”), Micro Focus will notify Customer of the Security Incident and work to reasonably 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 softwaresoc@microfocus.com.

Micro Focus Employees and Subcontractors

Micro Focus requires that all employees involved in the processing of SaaS Data are authorized personnel with a need to access the SaaS Data, are bound by appropriate confidentiality obligations and have undergone appropriate training in the protection of customer data. Micro Focus requires that any affiliate or third-party subcontractor involved in processing 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.

Data Subject Requests

Micro Focus will refer to Customer any queries from data subjects in connection with SaaS Data.

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.

Scheduled Version Updates

“SaaS Upgrades” are defined as major version updates, minor version updates, and binary patches applied by Micro Focus to Customer’s SaaS in production. These may or may not include new features or enhancements.

Micro Focus determines whether and when to develop, release and apply any SaaS Upgrade. Customer is entitled to SaaS Upgrades during the applicable SaaS Order Term unless the SaaS Upgrade introduces new functionality that Micro Focus offers on an optional basis for an additional fee.

Service Decommissioning

Upon expiration or termination of the SaaS Order Term, Micro Focus may disable all Customer access to SaaS, 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 any SaaS Data in Micro Focus' possession in the format generally provided by Micro Focus. The target timeframe is set forth below in Termination Data Retrieval Period SLO. 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 Objectives

Micro Focus provides clear, detailed, and specific Service Level Objectives (SLOs) for SaaS. 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 meet these objectives.

Micro Focus will provide self-service access to Customer to the Service Level Objectives data online at https://home.software.microfocus.com/myaccount

Solution Provisioning Time SLO

Solution Provisioning is defined as the Micro Focus ArcSight Intelligence for CrowdStrike solution being available for access over the internet. Micro Focus targets to make Micro Focus ArcSight Intelligence for CrowdStrike on SaaS available within five (5) business days of the customer's Order being booked within the Micro Focus order management system.

Tenant Off boarding SLO

Micro Focus guarantees a tenant on boarding time of two days from the time in which the Customer submits the formal written request.

User Removal SLO

Micro Focus guarantees that after the completion of this request, analytical results about the removed user will no longer be stored or available within the application.

Analytical Results SLO

Data to be analyzed is moved from the CrowdStrike Cloud to the ArcSight Intelligence Cloud Service via API. This upload happens continuously, and results in the collection of data within the tenant's storage area (e.g., S3). At a scheduled daily start time, Intelligence will analyze the pending data from a tenant, analyze the collected data, and publish the analytical results back for consumption by the Client, within their assigned tenant.

Micro Focus guarantees that the files in the tenant's daily set events will be analyzed and the results published to the application's user interface before a specified time for each tenant, every 24-hour period, at least 99% of the time.

Online Support Availability SLO

Online Support Availability is defined as the SaaS support portal https://support.cyberreshelp.com being available for access and use by Customer over the Internet. Micro Focus targets to provide Customer access to the SaaS support portal on a twenty-four hour, seven days a week (24x7) basis at a rate of 99.9% ("Online Support Uptime").

Measurement Method

Online Support Uptime shall be measured by Micro Focus using Micro Focus monitoring software running from a minimum of four global locations with staggered timing. On a quarterly basis, Online Support Uptime will be measured using the measurable hours in the quarter (total time minus planned downtime, including maintenance, upgrades, etc.) as the denominator. The numerator is the denominator value minus the time of any outages in the quarter (duration of all outages combined) to give the percentage of available uptime (2,198 actual hours available / 2,200 possible available hours = 99.9 availability).

An "outage" is defined as two consecutive monitor failures within a five-minute period, lasting until the condition has cleared.

Boundaries and Exclusions

Online Support Uptime shall not apply to or include any time during which the SaaS support portal is unavailable in connection with any of the following (specifically, the number of hours of unavailability in the measured period per the Measurement Method section above due to the following shall not be included in either the numerator or the denominator for the measurement):

- Overall Internet congestion, slowdown, or unavailability
- Unavailability of generic Internet services (e.g., DNS servers) due to virus or hacker attacks
- Force majeure events
- Actions or inactions 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 SaaS Upgrades

Initial SaaS Response Time SLO

The Initial SaaS Response Time refers to the support described herein. It is defined as the acknowledgment of the receipt of Customer's request and the assignment of a case number for tracking purposes. Initial SaaS Response will come as an email to the requester and include the case number and links to track it using Micro Focus online customer portal. The Initial SaaS Response Time covers both service request and support requests. Micro Focus targets to provide the Initial SaaS Response no more than one hour after the successful submission of Customer's request.

SaaS Support SLOs

There are two types of SaaS Support SLOs: Service Request and Support Request SLOs.

- The Service Request SLO applies to the majority of routine system requests. This includes functional system requests (product add/move/change), informational, and administrative requests.
- The Support Request SLO applies to issues that are not part of the standard operation of the service and which causes, or may cause, an interruption to or a reduction in the quality of that service.

The Response and Resolution Targets are provided as guidelines and represent typical request processing by Micro Focus SaaS support teams. They in no way create a legal requirement or obligation for Micro Focus to respond in the stated time. The Response and Resolution Targets, including their scope and determining factors (such as impact and urgency), are further described above in the scheduled maintenance.

Termination Data Retrieval Period SLO

The Termination Data Retrieval Period is defined as the length of time in which Customer can retrieve a copy of their SaaS Data from Micro Focus. Micro Focus targets to make available such data for download in the 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 SaaS. 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 SaaS • Manages contract issues
Subject Matter Expert	• Leverages the product functionality designed by Customer's SaaS administrators. • Provides periodic feedback to the SaaS Administrator
Administrator	• Serves as the first point of contact for SaaS end users for problem isolation • Performs SaaS administration • Provides tier-1 support and works with Micro Focus to provide tier-2 support • Coordinates end-user testing as required • Leads ongoing solution validation • Trains the end-user community • Coordinates infrastructure-related activities at the customer site • Owns any customization

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 SaaS solution • Provides 24x7 application support
Operations Staff (Ops)	• Monitors the 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 SaaS
- SaaS will be delivered remotely 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 Order is booked within the Micro Focus order management system
- The import of Customer data into SaaS 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.
- 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, SaaS is provided based on the assumption that Customer will implement and maintain the following controls in its use of SaaS:

- Configuring Customer’s browser and other clients to interact with SaaS
- Configuring Customer’s network devices to access SaaS
- Appointing authorized users
- Configuring its SaaS 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 provide SaaS and related 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.