STATEMENT OF WORK - Service Description

Atos Prescriptive Security – SIEM / SOC

Contents

1 Scope of Services

1.1 Atos Prescriptive Security (APS): SIEM / SOC Services

1.1.1 Service Disclaimer

The APS service, as described in this document, is an Atos hosted and fully managed Security Information and Event Management (SIEM) technology and supporting Security Operations Center (SOC) service. This service is not providing managed services for any other security function such as managed Firewalls or managed Intrusion Prevention Services or even a managed Identity and Access Management service. Where an agency may be in need of such additional services, Atos can provide these services in addition to the managed SIEM / SOC services.

1.1.2 Description

APS Security Information and Event Management (SIEM) technology and supporting Security Operations Center (SOC) enables real-time analysis of Security events, generated by Network, Hardware, Servers and Applications, such as Firewalls, IPDS, Vulnerability scanners, End-point security management systems, database servers, DNS servers, Active Directory servers, etc...

APS SIEM / SOC deals with real-time monitoring, correlation of events, notifications, and console views. The basic level of service provides long-term log storage of six months for normalization of event data and pre-defined reports, based on the received events.
(Additional storage needs will be quoted and priced based on client requirements).

APS SIEM / SOC service will provide you with a secure, flexible, subscription based SIEM / SOC service that is designed to identify a wide range of security threats.

It will deliver your business security monitoring needs by providing:

- Real-time monitoring and alerting of the security status of your services by sophisticated analysis of events passed through our correlation engine.
- Support from US SOC Analysts who are able to monitor, react and contain security events from our 24x7 staffed SOC.
- Simple pricing model that is based on number of devices to be monitored, and the number of events analyzed.
- We do the complex setup of common correlation rules and analytics, with the option of customer rules and alerts.

1.1.2.1 The APS service is offered in two levels of service, Silver & Gold, as well as optional modules / functions, as defined below:

Silver and Gold

- Cloud Standard Service - Atos DC hosted SIEM / SOC platform with default configuration
- Threat Intelligence Service
- Open DXL Communications fabric
- Monitored Equipment configuration
- Implementation of common Out of the Box (OOB) policies and correlation rules
- One Receiver (CPE) on-site in customer location
- Service setup / Transition (customer on-boarding)
- Continuous security monitoring
- Automated alerting

- Log management platform
- Standard Service Requests (SSRs)
- Standard Reporting
- Production support
- Security Management of APS SIEM systems

GOLD:

- Development and adjustment of parsing data provided by data sources
- Compliancy packs
- Periodic fine tuning
- Implementation of additional Customer policies and correlation rules
- Executive Dashboard
- Advanced Reporting

APS Optional Service Modules include the following:

- Link between CPE and Supplier data center
- Atos Computer Security Incident Response Team (CSIRT) Services
- Additional Receivers
- Risk Analysis and Monitoring on IT assets
- Optional service reports
- Identity and Access Management integration (based on T&M)
- Standard Service Requests (SSRs) for the optional modules

1.1.2.2 Benefits of the Service include:

- Real-time monitoring & alerting of the security status of your services
- Supported from US only using our skilled SOC staff
- 24 x 7 staffed Security Operations Center
- Simple pricing based on number of devices & events analyzed
- We do the complex setup of correlation rules and analytics
- Service may be tailored to individual customers and specific requirements
- Optional reports to understand and control the risk profile
- Optional Application monitoring services

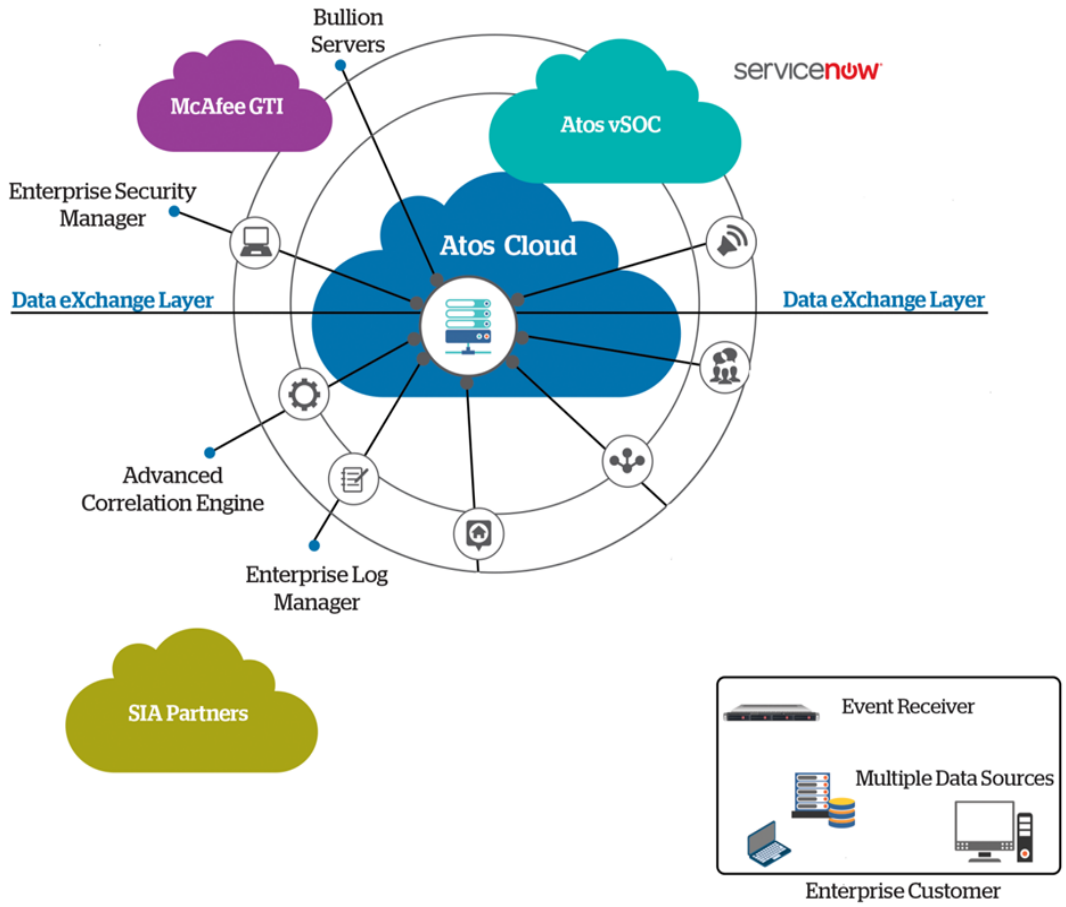
1.1.3 Technical Product Summary

The Atos Prescriptive Security service provides you with a remote protective monitoring service with connectivity to many device types for analysis. The following table provides a summary of these options:

Table 1 Provided Products

Product	What we provide to you
APS Remote Monitoring	Atos provides an Event Receiver / Log Collector on your infrastructure estate, and connect to the devices that you specify that require to be monitored. The customer must provide the log files in the appropriate format and data quality to enable our Remote Monitoring service to analyse events on your behalf.
Storage	We will store your log files (both in native and enriched form) for 6 months. Due to the size and volume of logs, these will be archived to an offline storage mechanism for later use.

1.1.3.1 Logical Solution Structure



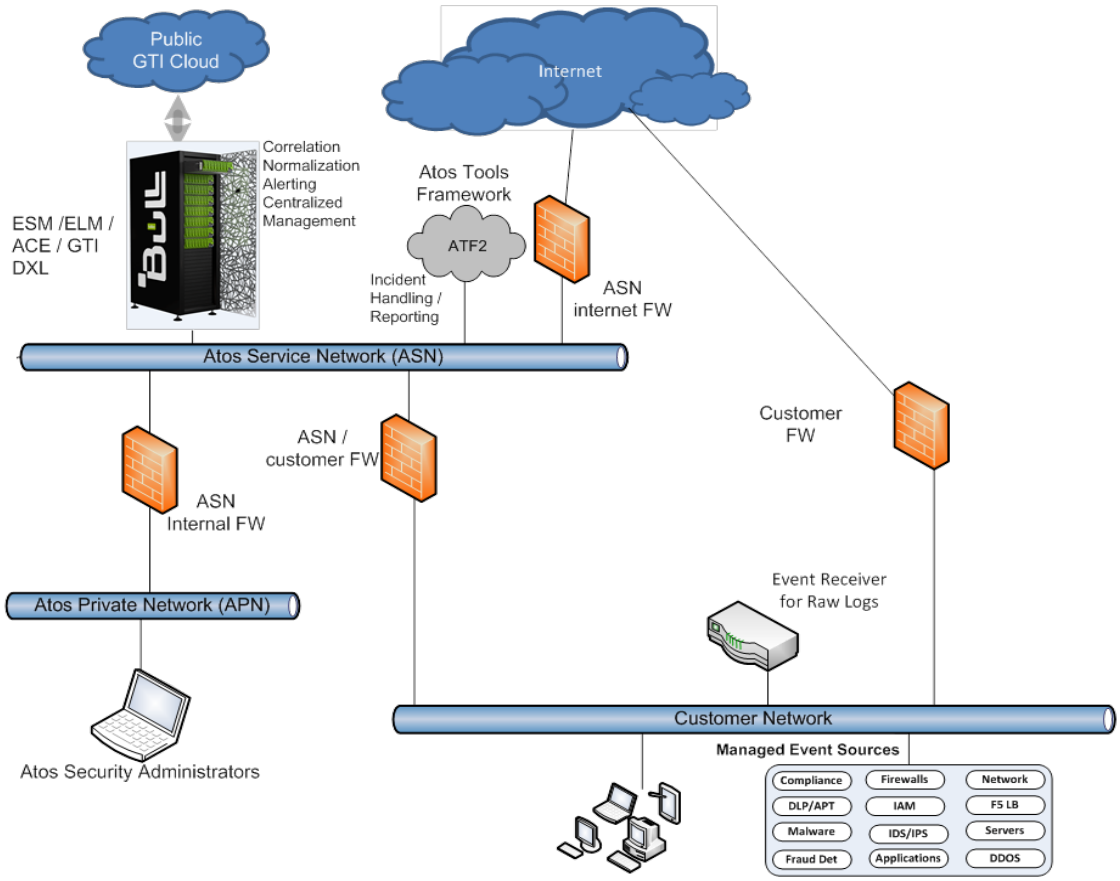
Atos' Prescriptive Security service introduces a new option for protecting the client's enterprise and data.

- The service combines the technology known as the McAfee Threat Defense Lifecycle, with Atos' advanced computer functionality of Bullion servers; and deliver it as an 'Atos Cloud Services' service offering.

The Service includes the following components:

- Atos Bullion Server Platform
  - EMC Unity Storage
- Atos Cloud Services
- Atos Tools Framework (ATF2)
- McAfee Enterprise Security Manager (Security Information and Event Management)
- McAfee Open Data Exchange Layer (DXL)

1.1.3.2 High Level Technical Structure



The service supplies continuous visibility and actionable intelligence from an integrated command and control environment for the Atos Security Operations Center (SOC). McAfee Enterprise Security Manager (ESM), which includes Advanced Correlation Engine (ACE) and Event Log Manager (ELM), is at its heart, and facilitates SOC personnel to collect, process, act on, and monitor events and risk over time.

The solution provides for full integrations with:

- Non-Intel security products that communicate over DXL (McAfee's open Data Exchange Layer); the different products learn and adapt from each other as incidents unfold.

In addition to the automation, integration and orchestration techniques, the service also provides:

- A team of highly-trained and experienced security personnel;
  - SOC staff maintains cyber-security certifications and use state-of-the-art tools to respond to security incidents and events at near-real time speeds.

1.1.4 Service Constraints

The Atos Prescriptive Security Service is generally limited to the following constraints:

Table 2 Atos Prescriptive Security Service Constraints

Subject	Condition
Security Policy	Customers are required to provide their security policy as one of the baselines for the APS service
Monitored systems	It is a responsibility of the customer to provide a list of the monitored systems/network devices/applications to ensure they are compatible with, and can provide the event information in the correct format.
Customer Premise Equipment (CPE) link	A link to CPEs is required for secure data exchange between the Atos Prescriptive Security service and CPE. If not provided by Atos as part of a wider managed services contract this will need to be provided by either the customer or separately by Atos depending on what is the most practicable and cost effective solution.
Alerting	It is a responsibility of the customer to provide alert matching correlation rules beyond those provided by Atos.
Incident response	Timely contact to the nominated customer personnel as to the potential security incident.

1.1.5 Technical Requirements

The technical requirements for the successful operation of the Atos Prescriptive Security service are:

- Connectivity between the customer's environment and Atos' Hosting environment.
- Sufficient network bandwidth to accommodate the number of monitored devices and Events per Second (EPS) produced by those devices.
- Necessary communication allowed on the customer firewalls to maintain CPE, and transfer required events onto the service backend.
- Appropriate event logs are to be produced in a compatible format with the Atos Prescriptive Security service for analysis.
- Appropriate access to the customer premises to install the service.

1.1.6 On-Boarding

Atos performs all the behind the scenes configuration of the remote monitoring service, subject to appropriate access being made available to Atos, taking away the complexity from the customer. The following activities are included as part of the APS product during on boarding phase.

Example of the activities during the on-boarding phase:

Table 3 On-Boarding Activities

On-boarding Activity
Installation & configuration of standard Collector Manager
Collector Manager fine tuning
Analysis of the incident cases and definition of remediation steps
Setup filters for identified high severity incidents
Base-line OOB Correlation Rules are implemented in our centralized service
SOC configuration and readiness preparation for receipt of the log files/events
Pre-configure Network connectivity and assign network bandwidth
Setup your storage allowances
Establish the Service Management Wrapper (Incident, Problem, Change Control Processes)
Service Transition Planning

1.1.7 Monitored Equipment Configuration

APS SIEM natively supports collection of the log data from more than two hundred and fifty (250) types of systems and Applications.

The Customer and Atos shall comply with the responsibilities, as set out in the following table.

Table 4 Monitored Equipment Configuration Responsibility Matrix

No.		Atos	Customer
1.	Configure predefined systems to enable log data sharing.		X
2.	Configure time synchronization.		X

1.1.8 Implementation of OOB Policies and Correlation Rules

The Customer and Atos shall comply with the responsibilities, as set out in the following table.

Table 5 Implementation of OOB Policies and Correlation Rules Responsibility Matrix

No.	Task	Atos	Customer
1.	Provide, on request, a detailed description of the logs that are produced by the systems or Applications that are to be monitored.		X
2.	Tune the standard filter and correlation rules according to Customer requirements.	X	
3.	Provide written acceptance of the solution functionality.		X

1.1.9 Optional Silver – Gold Standard: Development and Adjustment of Data Sources

Collector Software is the connection between the event and log managers and the monitored Application and Devices. In this case a new Data Source will be developed (for GOLD level service, up to 5 new Data Sources) to gather information from an Application or device not included in the standard list (over 250 different types of applications and devices available). Depending on the specific application, a new Data Source will be created or a new customized parser will be provided.

The Customer and Atos shall comply with the responsibilities, as set out in the following table.

Table 6 Development and Adjustment of Collectors Responsibility Matrix

No.	Task	Atos	Customer
1.	Provide all required information to create an appropriate receiver.		X
2.	Develop a Data Source and/or Customized Parser that handles the log messages of the appropriate event source.	X	
3.	Provide written acceptance of the solution functionality.		X

1.1.10 Production Support of SIEM Systems

Production support is a set of operational activities including regular housekeeping of the SIEM Servers, maintenance activities, and controlling the correct functioning of these tasks.

The Customer and Atos shall comply with the responsibilities, as set out in the following table.

Table 7 Production Support Responsibility Matrix

No.	Task	Atos	Customer
1.	Coordinate Incident Management and monitoring-related activities.	X	
2.	Update ticket status.	X	
3.	Update work instructions.	X	
4.	Start, shut down, and re-start (scheduled and non-scheduled) Servers or services/tasks and related Applications routinely, after a failure of the Operating System and for maintenance.	X	
5.	Coordinate recovery of Hardware/Software to a known/consistent state after failure.	X	
6.	Execute system commands on the console command line, such as commands needed to install patches, commands for Device information, check status.	X	

1.1.11 Security Management of SIEM systems

The Customer and Atos shall comply with the responsibilities, as set out in the following table.

Table 8 Security Management of APS SIEM Systems Responsibility Matrix

No.	Task	Atos	Customer
1.	Monitor Security settings.	X	
2.	In the case of any deviation in Security settings, notify Atos's Security officers to take appropriate actions.	X	
3.	Provide Security baselines and policies that shall be adhered to.	X	X
4.	Enforce a Security policy, e.g. password length, strength and duration, data-protection according to Atos baselines.	X	
5.	Provide physical Security of the Hardware Infrastructure based on Atos's data center policies.	X	

1.1.12 Log Management Platform

This service collects the log information sent from the monitored devices and Application via the Receiver (CPE Equipment) and is the foundation for APS SIEM.

The Customer and Atos shall comply with the responsibilities, as set out in the following table.

Table 9 Log Management Platform Responsibility Matrix

No.	Task	Atos	Customer
1.	Provide a hosted shared log management service for log collection, maintenance, and secure storage.	X	
2.	Securely transfer captured log data to Atos data center.	X	
3.	Store captured log data in the APS SIEM storage environment.	X	
4.	Define offline retention period.		X
5.	Retain data as required by the Customer.	X	

1.1.13 Receiver

The Receiver (RCV) is an appliance (physical or virtual) usually placed at the Customer's premises. The Customer Premise Equipment (CPE) in the Customer Network is a Customer

dedicated log data appliance that collects and forwards captured log data to the log management platforms.

Atos includes in both Silver & Gold levels of service 1 event receiver, this receiver can be a dedicated hardware appliance from the system vendor, or hosted in a virtual environment on customer premise as a virtual appliance.

The Customer and Atos shall comply with the responsibilities, as set out in the following table.

Table 10 Collector Manager Responsibility Matrix

No.	Task	Atos	Customer
1.	Provide physical Hardware or virtual Server, sufficient memory, storage and Network connectivity for the RCV according to Atos requirements and sufficient performance to collect Customer logs and forward them to Enterprise Log Manager (ELM) and Central Data Processing Center (CDPC).		X
2.	Install, configure, and maintain the RCV Software on the appropriate platform provided by the Customer.	X	
3.	Tune the RCV to the Customer-specific requirements.	X	
4.	Work collaboratively with Atos to tune the RCV to the Customer-specific requirements.		X
5.	Work collaboratively with the Customer to tune the RCV to the Customer-specific requirements.	X	

1.1.14 Link between CPE and Atos Data Center

The Customer and Atos shall comply with the responsibilities, as set out in the following table.

Table 11 Link between CPE and Atos Data Center Responsibility Matrix

No.	Task	Atos	Customer
1.	Provide a data link to send data from the RCV to the log and event managers.		X
2.	Optionally and at the Customer's request, provide Virtual Private Network (VPN) service to secure data exchange between CPE and hosted log management platform via the Internet. This optional service will be costed separately from standard solution.	X	

1.1.15 Automated Alerting

The Customer and Atos shall comply with the responsibilities, as set out in the following table.

Table 12 Automated Alerting Responsibility Matrix

No.	Task	Atos	Customer
1.	Provide automated alerting on Security Incidents via email.	X	
2.	Provide designated contacts and email addresses to receive alerts.		X

1.1.16 Hosted SIEM Platform

The SIEM platform is a foundation for the intelligent processing of the Security log data. The SIEM platform enables additional features such as Advanced Correlation Engines (for Real-Time and Historical correlation), Global Threat Intelligence integration and regulation compliancy modules.

The Customer and Atos shall comply with the responsibilities, as set out in the following table.

Table 13 Hosted SIEM Platform Responsibility Matrix

No.	Task	Atos	Customer
1.	Provide detailed requirements for correlation rules.		X
2.	Provide a hosted shared SIEM Service with alerting and correlation rules.	X	
3.	Integrate correlation rules according to Customer requirements.	X	
4.	Integrate alerting process according to Customer requirements.	X	
5.	Maintain shared SIEM platform.	X	

1.1.17 Compliancy Pack

The Compliancy pack provides high-level, business-focused controls that can help solve main standards and regulations management and Security requirements. The list of standards available includes the following:

- ISO 27002
- BASEL II
- EU 8th directive
- FISMA
- GIODO
- GLBA
- HIPAA
- NERC
- PCI
- SOX

The Customer and Atos shall comply with the responsibilities, as set out in the following table.

Table 14 Compliancy Pack Responsibility Matrix

No.	Task	Atos	Customer
1.	Implement compliancy pack.	X	
2.	Provision relevant log information and the list of controls, reports and dashboards to be considered.		X

1.1.18 Security Monitoring

The Customer and Atos shall comply with the responsibilities, as set out in the following table.

Table 15 Security Monitoring Responsibility Matrix

No.	Task	Atos	Customer
1.	Monitor the APS SIEM system for abnormal behavior or patterns.	X	
2.	Monitor Security log data from the Customer's IT Assets, searching for the signs of the Customer-specific Security scenarios, Incidents, and generic Security threats.	X	
3.	Perform the Incident response procedure by informing the Customer's designated Service contact about the Incident.	X	
4.	Provide a designated Service contact.		X

1.1.19 Periodic Fine Tuning

As the Customer's business objectives and priorities and IT landscapes change or new versions are implemented within the Network, APS SIEM configuration must be changed.

The Customer and Atos shall comply with the responsibilities, as set out in the following table.

Table 16 Periodic Fine Tuning Responsibility Matrix

No.	Task	Atos	Customer
1.	Order the periodic fine-tuning module for Silver.		X
2.	Keep the APS SIEM configuration in sync with reality by performing analysis and configuration change.	X	

1.1.20 Security Incident Response

The Customer and Atos shall comply with the responsibilities, as set out in the following table.

Table 17 Security Incident Response Responsibility Matrix

No.	Task	Atos	Customer
1.	Align containment processes to the Customer's specific Incident response policy and service scope of APS SIEM variant.	X	
2.	Provide Atos with the specific Incident response policy.		X
3.	Perform the Incident response procedure by informing the Customer's designated Service contact about the Incident.	X	

1.1.21 Optional - Risk Analysis and Monitoring on IT assets

The Customer and Atos shall comply with the responsibilities, as set out in the following table.

Table 18 Risk Analysis and Monitoring on IT assets Responsibility Matrix

No.	Task	Atos	Customer
1.	Provide sufficient information regarding the Business Applications and IT assets supporting them in scope to identify which are the main Applications/components to be assessed.		X
2.	Assess the likelihood and impact in case of materialization of main security threats for each component in scope.	X	X
3.	Conduct Risk Assessment for identified components and threads	X	
4.	Define the list of main Risk and Risk Scenarios to be implemented using the SIEM service	X	X
5.	Transfer the customized list of Risks/Risk Scenarios to routine operation.	X	

1.1.22 Additional Responsibilities

The following lists additional Atos and Customer responsibilities in relation to this service:

Table 19 Additional Responsibilities

Scope / Context	Atos	Customer
The Customer Premises Equipment (CPE) provides a platform upon which the Atos Prescriptive Security resides. This is typically a virtualization host to where the Atos software image may be loaded to, and operated from.		✓
To provide to Atos the appropriate ranges of IP addresses for their chosen network connection.		✓
To provide connectivity to the Atos Prescriptive Security service within a remote consumer network.		✓
Installation and management of the Event Receiver / Log Collector Manager services.	✓	
Configuration and management of virtual or physical device profiler functionality in the Event Recivers.	✓	
Depending upon the design of customers' networks, multiple Event Receivers / Log Collectors may be required to cater for volume, resilience and/or customer's LAN/WAN topologies. The customer must provide details of their anticipated number of devices, event volumes and locations.		✓
The Event Receiver / Log Collector is configured to client specific requirements. Atos assumes the presence of knowledgeable client staff regarding log collection, network design, security policy of the devices the client wants to monitor. If additional help is required in determining log collection requirements, configuration and data capture, Atos can assist via our Atos Prescriptive Security advisory service.	✓	✓
Customer to provide a rich event log file containing a wide variety of events that are to be monitored per device, or detailed log format specification.		✓
Customer Premise Equipment Provisioning: ► Installation of the Event Receiver / Log Manager software on the customer premises	✓	✓

Scope / Context	Atos	Customer
► Installation of the Virtual or Physical Device Profiler on the customer premises ► Maintenance of the APS software installed to the CPE ► Installation of the required collectors ► Installation of the required connectors ► Logically attaching required log data sources The role of other ICT service providers, a customer's own support staff, location and the number of CPE Event Receivers is assessed with a customer before the delivery model and pricing is confirmed.		
Initial Tuning ► Installation of the baseline filter set (generic) ► Optional Workshop with consumers' key business and IT personnel to identify high impact related risks and convert them into incident cases ► Optional analysis of the identified incident/risk cases and definition of the incident response policy including containment plan per case ► Optional development and setup of custom correlation rules ► Optional development and setup of the custom workflows	✓	✓
The customer must configure their event sources to generate log data in a format that is compatible with the Atos Prescriptive Security service		✓
Enhanced APS Report: ► The report will be dependent upon the data received by the APS service from the customer configured sources and log content.	✓	✓

2 Service Levels

2.1 Atos Prescriptive Security SIEM Service Levels

The standard measurement period for when Service Levels begin is 30 days after the “Go-live” Transition / Implementation Project milestone.

- The “Go-live” project milestone is an agreement between Atos and the customer with an agreed upon User Acceptance Test (UAT) defined in the initial planning stage of the Implementation Project.
- This period coincides with when Atos can begin billing the client for services.

2.1.1 Service Availability

The following Service Availability will be provided with this Service.

Table 20 Service Availability

Value		Object or Service Availability
		Service
Service Availability Window	7 days, 24 hours (all days) 24 hours a day	99.8%
	Within Business Critical Service Window [1]	
Maintenance Window	Saturday, 08:00 - Sunday, 12:00, once a month Central United States Time Zone	X

2.1.2 Support Availability

The following Support Availability will be provided with this Service.

The following table shows the support availability of the Atos Prescriptive Security (APS) SIEM operation. This means that e.g. the priorities relate to APS SIEM and not to e.g. Security Incidents that might be created by APS SIEM.

Table 21 Support Availability

Value	Silver	Gold
Support availability Window		
5 days, 9 hours (Business Days) 08:30–17:30	X	
7 days, 24 hours (all days) 24 hours a day		X
Within Business Critical Service Window [2]		
APS SIEM Infrastructure Incident handling Window		
Priority 1, 2: 7 days, 24 hours: All days, 24 hours a day Priority 3, 4: 5 days, 9 hours: Business Days, 08:30 – 17:30 h	X	X

[1] The Business Critical Service Window is optional and has to be agreed service-specific if applicable.

[2] The Business Critical Service Window is optional and has to be agreed service-specific if applicable.

Value	Silver	Gold
Within Business Critical Service Window [3]		
Standard Change handling Window		
5 days, 10 hours: Business Days, 08:00 – 18:00 h	X	X
Within Business Critical Service Window [4]		
Support language		
English	X	X

2.1.3 Additional Service Levels/KPIs

The following Additional Service Levels and KPIs will be provided with this Service.

No reports are provided for the mentioned KPIs.

Table 22 Additional Service Levels/KPIs

Name	Description	Level/Value
Security Event/Incident detection time	Maximum time that is required to detect a security event/incident. Security events have to be classified as Security Incidents during the implementation or fine tuning to be handled as a Security Incident. Time starts when the log information hits the CDPC and ends with sending an email to predefined address (Silver) or the Incident reaction performed by Atos (Gold). For Security Incidents that are classified as “medium” or “low”, Atos provides a daily report in Service class Gold and weekly report for Service class Silver. The Incidents will be closed afterward.	Silver: 15 minutes Gold: 15 minutes
Security Incident reaction time	Maximum time until the first reaction after a Security Incident classified as “high” or “critical” is detected. Time starts with end of “Security Incident detection time” and ends with start of incident reaction agreed with customer (sending email notification/making a phone call/generating a report etc.). During this phase, Atos personnel validate the Incident and try to avoid “false positives”.	Gold: 1 hour
Security Incident reminder time	For Security Incidents classified as “high” or “critical”, Atos expects a reaction (acknowledge) from the Customer within one (1) hour after first email is sent. In case Atos receives no reaction from the Customer, a reminder email will be sent for Security Incidents with classification “high”. All defined communication channels (e.g. mail, SMS, phone call) will be used for incidents with the classification “critical” once. Incidents that are classified as “high” will be closed.	Gold: 1 hour
Second security Incident reminder time	For Security Incidents that classified as “critical”, Atos will again remind the Customer via defined communication channels (e.g. mail, SMS, phone call) once. The Incident will be closed.	Gold: 1 hour

[3] The Business Critical Service Window is optional and has to be agreed service-specific if applicable.

[4] The Business Critical Service Window is optional and has to be agreed service-specific if applicable.

2.1.4 Standard Reports

The following Standard Reports will be provided with this Service.

Table 23 Standard Reports

Report Name	Description	Level / Value	Reporting Period
Availability	Availability of the ELM and CDPC Infrastructure. (CPE infrastructure and link to CPE is excluded.)	99.8%	Monthly
Service specific reports	Reports provided from APS SIEM. Required reports are identified during Service implementation or as a change during Service operation and provided electronically. Up to five (5) reports are included.		Weekly (Gold and Silver) Monthly (Bronze)
Security incident report	A report that describes the number and classification of occurred security incidents.		Weekly (Gold and Silver) (Not available for Bronze)

2.1.5 Standard Service Requests

The following Standard Service Requests will be provided with this Service.

Table 24 Standard Service Requests

Service Request Name	Description
Create correlation rule	Create a correlation rule.
Modify correlation rule	Modifying a correlation rule.
Delete correlation rule	Delete a correlation rule
Generate report	Generate an “Adhoc report” which was defined before in the Service Scope document, The report is filled in with data from required timeframe (less than a month).
Create Data source	Creating a Data source that has been previously configured properly on customer side.
Modify Data source	Modifying a Data source that has been previously configured properly on customer side.
Delete Data source	Removal of a Data source.
Export raw data	Export log raw data for single event source for a given period of time.
Create user account	Create APS customers WEB UI access to use APS. Only possible on dedicated infrastructure
Delete user account	Delete APS customers WEB UI access to use AHPS. Only possible on dedicated infrastructure
Reset User Password	Reset the password of an APS Web GUI user

Service Request Name	Description
Create parser	Create a new parser

Additionally to the above mentioned Standard Service Requests, customer might ask for the following changes on a regularly basis. Due to the dependencies from customer specific requirements and environment, it is not possible to standardize them on the same level. Therefore APS offers the below mentioned changes as small projects.

Change	Description
Add/modify a report template	Adding or modifying a report based on standard templates provided by the product vendor.
Delete a report template	Deletion of a report

3 Appendix A: Volumes and Assumptions

3.1 Minimum volumes

The following table lists the Managed Security Services minimum volumes for Events Per Second (EPS) required to obtain the published pricing.

Table 27 - Minimum Volumes

Quantity	Resource Unit
1,000 EPS	Security Monitoring, Log Management, and Analysis

3.2 Assumptions

- Customer and Atos will build very clear and precise Project Scope, with all captured customer requirements, site locations, log sources, etc., before final SOW signing, final pricing, or project start.
- Customers must provide very clear list of log sources with associated IP address, access credentials, and compatible log file formats.
- The customer agrees to all conditions as defined within this SOW document, including all appendices
    - That the customer will abide by all responsibilities assigned to them within this Statement of Work.

4 Appendix C

4.1 Base Line Volumes of Customer Event Sources

The Supplier design criteria is affected by many factors, such as time on task, the type of resource required, the speed in which responses are provided, and the complexity of the work. Changes to these factors may have a significant effect on the cost of delivery or the ability to meet certain performance goals.

The following table lists the baseline volume requirements of log sources and associated criteria for the solution.

Quantity	Description	Associated Service Criteria
	PRIVILEGED_USERS (admin user names)	Group: Domain Admins Group: Administrators All user accounts starting with “ADMIN’ Winvulnscan SIEM_LOG Executive Accounts
	DNS Servers	IP Addresses
	DHCP Servers	
	FTP Servers	IP Addresses
	Terminal Servers	IP Addresses
	Vulnerability Scanners	IP Addresses
	NetScalers	IP Addresses
	Telnet Servers	IP Addresses
	eMail servers	IP Addresses
	eMail Content Filtering /SPAM Filtering Servers	
	Load Balancers	IP Addresses
	HTTP Servers / Web Servers	IP Addresses
	SMTP Relay Servers	IP Addresses
	Database Servers Oracle MSSQL DB2 My SQL Etc.	IP Addresses
	Anti-Virus Endpoints	IP Addresses
	Database Monitoring Applications	
	Application Servers	IP Addresses
	Wireless Access Points	IP Addresses
	Wireless Controllers	
	Firewall(s) / UTMs	IP Addresses

Quantity	Description	Associated Service Criteria
	► Perimeter ► Internal ► Regional ► Branch / Small Office	
	WAN Accelerators	
	IDS / IPS	
	VPN Concentrators	
	Device control systems	
	Windows Domain Controllers Corporate Regional Office	
	Windows Servers	
	Windows Servers – High Activity	
	Database monitoring servers	
	Routers	
	Switches	
	Netflows – devices generating flows	
	Web Application Firewall Application	
	Host Intrusion Prevention - Endpoints	
	Network Access Control Appliances	
	Mainframe Servers / iSeries	
	Unix / Linux Servers – High activity	
	Unix / Linux Servers – Average activity	
	WEB Proxy / Content Filtering Appliances	
	Workstations	
	Data Loss Prevention Endpoints	
	Data Loss Prevention Servers	
	Network Access Control Servers	
	Additional systems and or applications that may have been missed.	