PROACT

SIEM as a Service Enterprise

Service Definition Document

SDXSIEM-E-001 Published 09 October 2019

Public - Freely Distributable

PROACT

Table of Contents

1 Service Overview

Proact's SIEM-as-a-Service Enterprise (SIEMaa-E) is a remote logging security service offered to improve Customers' security awareness of their infrastructure and application environments.

SIEMaaS-E is designed to meet the Customer's requirement to store, analyse and triage data from infrastructure, operating system, application logs, end point devices and cloud platforms.

This Managed Service provides for the remote collection and analysis of logs, using an industry-leading Security Information and Event Management solution (SIEM) and can additionally include User Entity Behaviour Analytics (UEBA) functionality.

The service simplifies the correlation, consolidation and comprehension of events recorded in transient, disparate and widely dispersed system logs to deliver:

- Alerts for unexpected events
- Extended storage of usually transient log data
- Prioritisation of logs by risk scoring
- Online access to real-time information surrounding log data and events
- Historical reporting and performance log analysis produced by the Security Operations team
- UEBA activity monitoring and user risk profiling against unusual or suspicious activity.

The 24x7x365 Managed Service provides security guidance and advice to the Customer's IT team and/or other nominated representatives. Proact's Security Operations Centre (SOC) becomes a cost-effective virtual member of the Customer's security team, reducing the workload of the Customer's security officer(s), by notifying of high-risk events.

The environment in scope is analysed for suspect activity and abnormal events. Proact then advises the Customer on appropriate steps to be taken to prevent suspect activities from escalating.

1.1 Service Scope

Objective	▪ To provide the remote collection and analysis of logs using Security Information and Event Management (SIEM) and User Entity Behaviour Analytics (UEBA)
Description	▪ The service simplifies the task of identifying, analysing and understanding security events by correlating the disparate and often transient logs generated by IT elements (for example, operating systems, applications, firewalls and switches etc.), to provide: ▪ Persistent logs, stored for a minimum of 90 days (extended retention periods are available) ▪ Prioritised logs and alerting facility for unexpected events detected in the environment ▪ Comprehensive and easily accessible data. ▪ Risk based scoring of user and network activity.
Hosted-in	▪ A securely segmented multi-tenant platform.

Supported log sources	▪ Logs can be collected from any device that supports one of the following protocols
	  ▪ Syslog
	  ▪ SNMP Trap
	  ▪ Microsoft Windows Event Log formats
	  ▪ Restful API integration
	  ▪ Flat file collection
	▪ Includes built-in log parsers for a wide range of industry-leading infrastructure component vendors, operating systems and applications, providing out-of-the-box best-practice log classification and correlation functionality.
	
	A list of available supported vendor log sources is available on request.

Unsupported Log Sources	▪ For systems that do not have built-in log parsers available, Proact may, on request from the Customer, work with the Customer to define common log patterns that can be classified using Regular Expressions (RegEx). Any such Proact assistance requested by the Customer will be charged at Proact's standard professional services rate and will be subject to the availability of Proact resources.
Supported-from	▪ All support and management is delivered remotely from a secure, accredited *Proact Network Operations Centre).*
Support level	▪ Monitoring, support and service management of the platform.
Service Deliverables	▪ Usage reporting & billing ▪ Log data consolidation ▪ Log data classification ▪ Log data risk scoring ▪ User Behaviour Risk Profiling ▪ Advanced threat detection through data correlation. ▪ Tuning activities NOTE: The scope of tuning is refined to the Proact platform to ensure the correct logs are parsed and processed. Proact will, where possible, provide tuning recommendations to be applied to the log sources by the Customer IT personnel, to improve the quality of the service and reduce unnecessary log processing. ▪ Security risk notification based on event categorisation and priority. ▪ Security specialist advisory guidance. ▪ Response and guidance from the Proact security team in relation to the containment and remediation of security incidents. ▪ Reporting engine for custom reports ▪ Quarterly Service Review report (SIEM metrics, utilisation & tuning) ▪ Access to the security platform web interface for data searching and customisable dashboards. ▪ Self-service portal access for incident raising, tracking and reporting.

1.2 Service Capabilities

Log monitoring	▪ The Proact platform monitors Customer log sources 24x7x365
Log data consolidation	▪ Proact handle the consolidation and storage of all logs sent by the items in the scope of the Managed Service. ▪ Logs are retained for the Customers specified retention period ▪ Logs and events can be made directly visible to the Customer via a web interface
Log data classification	▪ All log messages are automatically classified into categories to identify the associated impact based on threat models and policies built into the platform.
Entity and Log risk scoring	▪ As log messages are processed into the platform they are automatically associated with an 'entity'. This can be a user, device or application. The entity is continuously assigned a risk score based on the type of log messages
Log source alerts	▪ Proact will raise an alert if a log source fails and will contact the Customer to undertake a local investigation. If the issue is related to the configuration of the remote collection agent software, Proact will troubleshoot the issue over a remote connection. The Customer remains responsible for troubleshooting any issues not relating directly to the log collection software.
User Risk Profiling	▪ Proact shall notify the Customer of suspicious user activity based on a risk scoring mechanism. Risk scoring is based on deviations from previous learned user activity in comparison to peer group activity and activity related to known insider threat vectors.
Self-service management portal	▪ The Self-service management portal allows the Customer to monitor the status of their items covered by the service. Functionality includes: ▪ Trends, reports, alerts, and a near-real-time log view ▪ Perform searches and the creation of custom reports ▪ Raise issues relating to the log data from the in-scope items monitored.
Raise security risk alerts	▪ Security risk alerts, identified by the Proact security team, are sent to a nominated Customer contact using the chosen communications mechanism defined in the Customer's Service Operations Manual. *Responsibility 1: Nominate contact point for security risk alerts.*

Log monitoring	▪ The Proact platform monitors Customer log sources 24x7x365

Access to security specialists	▪ Proact security specialists are available to provide advice to the Customer under the following circumstances.
	
	▪ The Investigation of security incidents:
	  ▪ The Proact security team analyse and filter the events as they are logged into the platform through correlation rules and threat hunting activities, to highlight suspicious or anomalous activity leading to the raising of a security incident investigation
	
	▪ The remediation and containment of security incidents:
	  ▪ The Proact security team will provide recommendations to contain and remediate security incidents, in line with best practices provided by the associated technology vendor, relating to the application of patches, configuration changes, or other updates, required to remediate the issue and reduce any further exposure.
	
	  ▪ The Customer is responsible for implementing recommendations provided by Proact.
	
	Responsibility 2: Implement Proact security recommendations as required

Recommend continuous improvement activities	▪ Recommendations to help give the Customer an increased view-of and control-over security incidents. For example: Expanding the scope of the service to include additional log sources, or review and tune log sources for greater security awareness.
Tuning activities	▪ Proact will assist the Customer to reduce the EPS log count by providing tuning recommendations for the relevant log sources in scope. This may include reviewing the highest reporting log sources and identifying unnecessary log messages that could be suppressed by the Customer reconfiguring those log sources, thereby increasing the efficiency of the Managed Service. The Customer may implement the tuning recommendations recommended by Proact at their discretion.

1.3 Service Options

	Service Options
Cloud Integration	▪ SIEMaaS-E has an additional option to take the logs from Cloud based IaaS and SaaS platforms. Cloud specific correlation are applied to this data for additional advanced threat detection capability for cloud platforms. Cloud integration is a chargeable feature.
Log Retention	▪ Proact's default policy is to retain log data for 90 days on the platform for operational purposes after which all logs will be deleted. Where log retention for archiving purposes is required the Customer may request separately to have them retained for up to the duration of Contract.

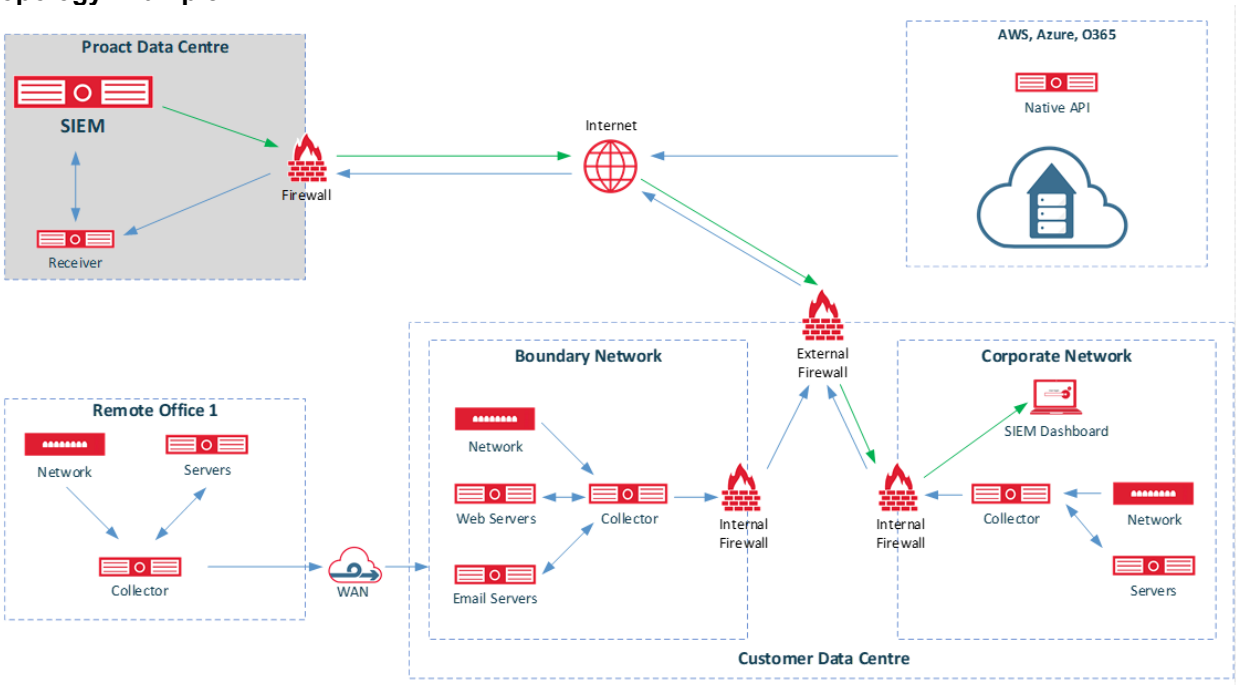
2 Service Configuration

2.1 Topology

One or more locally installed collection agents (also referred to as Remote Ingestion Node) collect logs from the Customer datacentre and forward them to the central platform managed by Proact.

The following diagram demonstrates a high-level overview of the topology. For security purposes all log data obtained by the collection agents and forwarded to the platform, is encrypted in transit using the TLS (Transport Layer Security) protocol. The data is then further encrypted at rest using AES encryption on the storage platform.

Topology Example:



2.1.1 Collection Agents

Log Collectors are installable software packages running on dedicated Linux CentOS or Red Hat Server operating systems on the Customer's site(s). The Customer must provision and build a virtual or physical server for each log collector to be deployed, and the Customer is responsible for all management of each server and its operating system. Proact will provide the minimum requirements for the server in a pre-requisites document during service transition or on request from the Customer.

Proact will install and configure the agent software remotely using a web-based administration session hosted by the Customer.

The number of collection agents required will be determined by the topology of the Customer systems that are in scope of the service. A design workshop is undertaken with the Customer at the beginning of the service transition to determine the appropriate number of collection agents and where they should sit within the Customer network, taking into account the number of locations and internet breakout configuration.

Prerequisite 1: Provide a server for each SIEMaaS-E log collection agent
Prerequisite 2: Notify Proact of the Public IP Address from which logs will be sent
Responsibility 3: Maintain operability of SIEMaaS-E Log Collector server(s) during contract term

2.1.2 Active Directory Integration

The log collection agent must interface with Active Directory (AD) to register LDAP information surrounding user identities within the Customer environment.

The Customer is responsible for creating an appropriate account in active directory for this purpose and to ensure the log collection agent can interface with Active Directory over the local network.

NOTE: The account is a standard AD user with no specific membership requirements.

Prerequisite 3: Provision Active Directory user account for the SIEMaaS-E platform to utilise.

2.1.3 Windows Events

Where the required scope of the is to capture event data from multiple windows operating systems, a central Windows Event Collector (WEC) server is required. This will receive all the logs from the Windows hosts that are in scope and forward onto the SIEM agent for collection and processing.

The Customer is responsible for providing a windows server and installing the windows event collector. Proact will provide the minimum requirements for the server in a pre-requisites document during service transition or on request from the Customer.

Proact will assist with the configuration of the WEC and provide guidance to the Customer on its integration into Active Directory Group Policy.

Prerequisite 4: Configure a Windows server for Windows Event Collector service

2.1.4 Log Collection Methods

The log collection agent collects or receives logs from the devices in scope by undertaking the following:

- Perform log collection by remotely logging on to machines to collect flat log files.
- Receive forwarded syslog message over TCP or UDP
- SNMP Traps
- Integrate with API (Application Programmable Interfaces)
- Manual import of specific data sources.

To ensure the confidentially and integrity of log data, the log collection agent shall:

- Encrypt the raw log information obtained from the LAN
- Pass the information to the Proact service over a TLS encrypted connection.

The Customer is responsible for the configuration of the devices, or systems, in the scope of the service, by applying the relevant logging configuration settings where applicable. If logs are to be obtained via an API (For example: Cloud SaaS platforms) the Customer is responsible for providing access to the log collection agent and the relevant credentials.

Prerequisite 5: Configure logging settings on in scope infrastructure.
Prerequisite 6: Provide API access and user credentials for Cloud platforms or other API integrated components.

2.2 Network Connectivity

All communication between the collection agents on the Customer's site(s) and Proact datacentre(s) is over encrypted (HTTPS//TLS) public internet link; there is no requirement for a site-site VPN or other dedicated communications channel.

All internet communication uses Proact's existing shared firewall infrastructure and either the Customer's existing firewall, or the firewall in the public cloud data centre (as required). Proact will provide the requirements for open ports / firewall rules in a pre-requisites document during service transition or on request from the Customer.

During service transition and throughout the term of the Contract, a customer administrator must be available to configure the Customer's infrastructure to allow new log sources to contact the log collector agents and to allow additional log collection agents to contact the central platform in Proact's datacentre.

NOTE: Where log traffic between in-scope devices and the SIEMaaS-E log collection agents must traverse a firewall, additional rules must be configured (provided by Proact during service transition or on request). A separate internet connection and firewall is required for each site location, unless the site(s) are connected through an internal Wide Area Network (WAN).

Responsibility 4: Provide administrator to configure Customer infrastructure
Prerequisite 7: Open firewall ports as required

2.3 Bandwidth Requirements

Communication bandwidth is sized based on the following assumptions:

- Average size of an encrypted log message sent: 600 Bytes
- Average number of log messages sent by items in the scope of devices.
- The minimum bandwidth required can be calculated as number of monitored user identities multiplied by 2 x the average log message size. **For example, 1000 Users = 9.6Mbit internet connection.*

* This is an example based on an average environment, that may vary based on the types of items managed by individual SIEMaaS-E deployments and the number of messages generated. It should be noted that times of peak activity, such as the start of the working day, typically generate more events and additional bandwidth may be required, or the logs will be queued on the collector.

The Customer must ensure there is sufficient egress bandwidth available for log messaging to be sent from the log collection agent to the Proact platform.

Responsibility 5: Maintain sufficient network capacity for service operation

2.4 Self-Service SIEM/UEBA Web Portal Access

As part of the service Proact provide Customers with a self-service web portal.

- The self-service management portal provides secure access using HTTPS (TCP port 443) and is available from any location in the UK and the EEA (European Economic Area) with Internet access.
- Access to the self-service portal is through account credentials provided by Proact that use additional multi-factor authentication. Role Based Access Control is used to provide granular access policies for Customer users depending on their individual requirements.

NOTE: The "Gemalto SafeNet MobilePass" application will need to be downloaded and installed by each user on their chosen device type of Laptop or Smart Phone.

- The Customer will provide Proact with a list of users whom require access to the platform and the levels of information they wish for each user to see. Additional users can be added during the lifecycle of the platform by logging requests through the Proact support portal.

Prerequisite 8: Download and install the Gemalto SafeNet MobilePass application
Prerequisite 9: Provide usernames, email addresses and role requirements for Portal users.

2.5 Remote Configuration and Interaction

- During the service transition period, Proact will undertake the configurations of the Managed Service which is in-scope of the Contract. This will be done automatically and therefore the Customer should provide resource for this remote access during this period. The Customer must also ensure that their network environment has sufficient capacity, ports and configuration to support on-going service operation.
  - In particular, the Customer is responsible for ensuring that they have adequate Internet bandwidth to support the transmission of collected logs to Proact's SIEMaaS platform. The calculation for the expected bandwidth requirement is detailed in Section 2.3: Bandwidth Requirements.

Prerequisite 10: Provide remote access for Proact configuration and support tasks
Exclusion 1: All configuration shall be performed by Proact remotely

2.6 Systems Interoperability

- Where this Managed Service interacts with any system, application or environment which is not managed by Proact, it is the Customer's responsibility to ensure that it remains compatible with any infrastructure, systems/applications managed by Proact or the hardware, firmware, operating system and application version levels which are recommended by Proact or its vendors as best practice.

Responsibility 6: Maintain compatibility of interacting external systems or environments at all times

2.7 Service security

The security of the Customer's data assets is paramount, and Proact endeavour to maintain its approach to security across all services in line with established industry standard practice.

Anti-virus protection	▪ Proact's infrastructure incorporates enterprise level antivirus protection. Anti-v protection is applied to all servers running the service and any end points used to access the platform by Proact operators. ▪ The Customer is responsible for and required to install and maintain anti-virus software on the log collector servers.
Patching	▪ Proact and the Customer will manage patching according to the following responsibilities. ▪ SIEMaaS-E platform patching – Proact are responsible for patching and updating all the infrastructure software and hardware under their management. This includes the log collection agent software running on the Customer site. ▪ Operating system patching – The Customer will maintain and patch the servers on their premises running the collection agents or Windows log collectors. *Responsibility 7: Patch guest OS for Log Collector and install Anti-Virus*
Data encryption	▪ Secure TLS encryption is applied to all data connections between Proact and their Customers ▪ All transmitted log messages are protected by a hashing algorithm, which calculates the message hash and stores it in the database to guard against potential tampering during transmission. The hashed message is then encrypted before transmission. ▪ In all architecture models, data is stored in an encrypted format to ensure its security, whether at rest or inflight.
Audit capability	▪ Proact keeps a log of all actions undertaken on the platform for continuous monitoring and audit purposes, within the retention policy defined in Section 7.1: Data Retention. ▪ This can be helpful in detecting attempts, whether successful or not, to gain illegitimate access to the system, probe its information, or disrupt its operation. Knowing an attack is attempted and the details of the attempt can help in mitigating the damage and preventing future attacks.
Administration	▪ All administration interfaces to the platform are accessed only over secure protocols. (TLS and SSH). ▪ Administration of the platform is accessible only from a secure network only available within the Proact Network Operations Centre facilities.

2.8 Applications and licensing

SIEM Licensing	▪ Proact will provide all licensing for the log collection agents and for the processing of log messages through the platform.
Log Collection Agents	▪ Proact recommend the use of CentOS for Log Collection Agents, which is a freely available distribution and does not require a license. ▪ Where the Customer elects to use Red Hat instead of the default CentOS, the Customer must provide appropriate Red Hat operating system licensing.
Windows Event Collector	▪ The Customer must provide appropriate operating system licensing for the server acting as the WEC.

2.9 Data Privacy

General Data Protection Regulation (GDPR)	▪ The Customer is the Data Controller and controls the ways and means of processing of Customer Data. Proact is the Data Processor and will process data under the instructions of the Customer as detailed within the relevant Contract. ▪ The Customer warrants that is has the appropriate authority and all relevant consents in accordance with the applicable law in connection with all Customer Data including any Personal Data to permit the Customer to transfer the same to Proact to process for all purposes set out in the Contract.

3 Support Structure

3.1 Proact Service Desk

Deliverable	Frequency	Description and content summary
Service Desk – contact number	Continuous	▪ Proact provide the Customer with a 24x7x365 service desk telephone number for the purpose of reporting incidents and raising Change Requests (CRs) for Configuration Items (CIs) ▪ Calls are logged on receipt, and will be acted upon within the Customer's contractual service window ▪ The Proact Service Desk and Proact self-service support portal are accessible to named individuals only; not to the Customer's users in general. Proact does not offer *end-user* support. *Exclusion 2: Unauthorised use of the Proact Self-service support portal and-or Service Desk*
Proact Self-service support portal	Continuous	▪ The Customer is provided with access to the *Proact Self-service support portal* via the internet. Using the portal, the Customer can: ▪ Create new and update existing incidents for investigation ▪ Create new and update existing CRs from a change catalogue ▪ View their CIs on the CMDB ▪ Proact provide each named individual with an account for their sole use, with their username being their email address. No shared accounts are provided.
Proact Self-service management portal	Continuous	▪ Proact provide login credentials for named authorised Customer representatives, assigning each a unique username and password. ▪ Access to the portal requires one of: Google Chrome; Internet Explorer 11; Mozilla Firefox; Safari.

3.2 Service Monitoring

Deliverable	Description and content summary
Monitoring Platform	▪ Proact will monitor the service infrastructure in near-real-time and raise alerts to the Proact Service Desk.
Monitored Items	▪ Proact will monitor all Proact infrastructure used for the delivery of the service ▪ The scope of monitoring will include the log collector agents in the Customer environment to determine if logs are being received into the Proact platform. The Customer will be responsible for ensuring these devices remain available and that log sources are transmitting logs to the collector agents. ▪ Proact will monitor the log collection agents for: ▪ Log sources no longer being received to the collection agents ▪ Log collection agents being offline

3.3 Connectivity for Troubleshooting

If a routine change is required or an issue occurs, it is the responsibility for Proact to remediate. The case owner will request assisted remote access to connect to the Customer's environment.

4 Activities

4.1 ITIL processes

Proact monitor, support and manage the service infrastructure using processes aligned with the ITIL framework for IT Service Management. Proact will provide the Customer with a Customer Service Operations Guide containing full detail on how Proact deliver and operate these processes. These guides may change from time to time. This section summarises the processes' key capabilities and deliverables.

Event management	**Near real-time monitoring**	▪ The Proact monitoring platform continuously monitors the service infrastructure to: ▪ Deliver near-real-time device monitoring ▪ Collect metrics for analysis ▪ Identify alert conditions and thresholds breaches ▪ Send triggered alarms to the Service Desk
	Alert notifications	▪ The Proact Service Desk responds to triggered alarms, analysing, investigating and taking appropriate remedial action.
	Event handling	▪ Proact process all alerts (not just critical alerts), taking the appropriate action to resolve the issue (if required.
Incident Management	**Service desk**	▪ The Proact Service Desk provides an escalation path for the Customer's administrators when assistance is required with software issues, firmware issues and hardware faults on CIs.
	Incident Response	▪ Proact Service Desk escalates alerts to its technical teams for resolution as appropriate ▪ Proact Service Desk inform the Customer's nominated contact of any service impacting alerts and the resolution timeframe ▪ For incidents categorised as P1, Proact will take appropriate action to restore operation and-or to minimise any service down time for the platform components managed and operated by Proact. ▪ Proact co-ordinate any product vendor involvement necessary to achieve resolution of an issue.
Change Management	**Controls**	▪ All changes to the service infrastructure are performed under the Proact change management process ▪ Proact perform changes to the service infrastructure only when authorised to do so by a CAB approved Change Request (CR)
	Tools	▪ Proact use orchestration appliances to perform changes where compatible and appropriate.
Problem Management	**Pre-emptive maintenance**	▪ Proact's proactive problem management processes help avoid recurring issues. ▪ Proact applying patches, bug-fixes and upgrades to the service infrastructure in line with best practice. ▪ Proact maintain problem records in the CMDB to aid identification and prompt resolution of issue.
	Trend analysis	▪ Proact perform regular incident *trend analysis* to proactively identify any reoccurring service infrastructure problems and their root causes.
Capacity management	▪ Proact monitor and respond to service infrastructure threshold breaches and growth forecasts to maintain agreed performance levels and adequate capacity for growth.	
Service reporting	▪ Proact provide quarterly service review reports through their service delivery team	
Continual Service Improvement	▪ Proact manage service improvement plans which track recommendations for changes to improve service provision.	

Configuration & Knowledge Management	▪ Proact maintain a definitive record of the service infrastructure in a CMDB ▪ Proact maintain a knowledge database to allow support teams to efficiently resolve known issues and find supporting information.

4.2 Operational Activities

The following table outlines the operational activities undertaken by Proact as part of SIEMaaS-E:

Deliverable	Frequency	Description and content summary
Log handling	Continuous	▪ Proact consolidate and store all logs sent from the Customer site in a central database for the contracted retention period.
Risk scoring	Continuous	▪ The Proact SIEMaaS-E platform automatically applies threat models and policies across all logs sent to it. Scoring is then applied based on these threat models to provide an aggregated risk score accordingly.
User risk scoring	Continuous	▪ The Proact SIEMaaS-E platform automatically risk scores user activity using behaviourally based machine learning algorithms and peer group analysis to identify potentially anomalous or suspicious user activity that could indicate a malicious or compromised internal user. By combining data across the whole platform each individual user is given a unique risk score.
Alert handling	Per Event	▪ The Proact security team will investigate events to ascertain the risk exposure to the Customer and, where necessary will raise an incident, assign a priority and contact the Customer. The investigation and notification processes are detailed in Section 4.3: *Alert Handling*.

Provision of advice and guidance	As required	▪ The Proact security team:
		  ▪ Analyse and filter events as they are logged
		  ▪ Provide the Customer with recommendations in line with best practices using email or the self-service support portal. The Customer is responsible for implementing this guidance.
		▪ Review significant incidents, providing recommendations for:
		  ▪ Preventing or dealing with similar incidents in the future
		  ▪ Improving the Customer's security posture.

Maintain platform infrastructure resources	Continuous	▪ Proact maintain the infrastructure to a standard that enables its availability to at least match the agreed service level ▪ Proact provide planning and implementation of upgrades and-or patches to software and firmware on the underlying platform infrastructure ▪ Proact make configuration changes to Customer IP addressing, certificate changes and IP routing on Proact communication devices located in a Proact datacentre, when requested via the change control process

Deliverable	Frequency	Description and content summary
Planned maintenance	As required	▪ Proact endeavour to provide, by email, advanced notification of any planned maintenance activities, either by Proact or by its third-party providers, at least five working days in advance of the maintenance commencement ▪ Where maintenance is required more urgently, to prevent a longer outage or a security incident, or due to third-party provider timescales, Proact may give less notice than five working days ▪ The Customer must inform Proact whenever they intend to perform any maintenance, penetration, vulnerability or security testing to sites, networks or other devices that may affect the availability, communicability, performance or integrity of any system monitored or managed by Proact *Responsibility 8: Provide at least 24-hours' notice of planned maintenance*
Change Management	Continuous	▪ All changes to the Customer's log source or policy configuration are planned and implemented according to Proact change management processes

Platform Monitoring	Continuous	▪ Proact continuously monitor the availability of the SIEMaaS-E platform.
		  ▪ The service is deemed available if the SIEMaaS-E log monitoring software's incoming message queue responds to the platform's software probe.
		▪ Proact Service Desk monitor the continuity of log feeds from Customer's log sources and SIEMaaS-E log Collection agents. Upon detection of interruption of log feeds, Proact will alert the Customer and recommend action to remediate, such as:
		  ▪ Reboot a log collection agent
		  ▪ Investigate a failed log source
		  ▪ Amend a firewall configuration.
		Exclusion 3: The solution does not support monitoring of Customer applications or appliances

Log Collector Installation	As required	▪ Proact will assist the Customer with the installation of additional log collection agents as required. The Customer must complete the documented pre-requisites for additional log collection agents and provide an administrator with elevated privileges to work with Proact engineers on the installation. *Responsibility 9: Assist in installation of log collection agents by providing elevated privileges*

4.3 Alert Handling

4.3.1 Triage and Notification

The Proact security team will raise an incident upon the investigation of an event to ascertain the risk exposure to the Customer and assign a priority. In this context, an event refers to any notification resulting from the following mechanisms:

- The threat modelling and behavioural intelligence functionality of the service.
- Triaging and correlation activities by the Proact security team

Where events are determined by Proact's security team to require communication to the Customer, incidents will be created and prioritised accordingly, and the Customer shall be contacted via the chosen notification mechanism and provided with actionable intelligence and advice on how to appropriately respond.

During the investigation process Proact will always contact the nominated Customer personnel as agreed and recorded in the Service Operations Manual. According to the nature and priority of the incident, communication may be as a notification only, or may be direct contact from Proact's security team to the Customer in order to obtain any locally significant context such as expected changes in user or system behaviour patterns planned maintenance.

- **P1 Incidents**

Where the investigation of an event by the Proact security team concludes that there is an immediate and uncontained threat to the Customer the incident may be assigned or upgraded to P1 (Priority), and Proact will assign a named Incident Manager to direct Proact activity and communications with key Customer stakeholders until the priority is reduced.

- **P2/P3 incidents**

The following table demonstrates the process of interaction with the Customer stakeholders for P2/P3 priorities. These processes will be reflected in the Service Operations Manual.

Priority	External Threat	Incident Notification	Interaction
SIEM / Threat Modelling and Correlation			
P2	▪ Account Compromised ▪ External Attack	Proact security team will contact the Customer directly	Full incident detail in Proact portal
P3	▪ Informational / Configuration / Vulnerability or other remediation guidance.	An incident will be created, and the Customer will be notified by email	
User Behaviour			
P2	▪ Likely Compromised User ▪ Malicious insider activity	Proact security team will contact the Customer directly	Self-Service SIEM/UEBA dashboard.
P3	▪ Flight Risk ▪ Inappropriate Access ▪ Deviation from behavioural baseline	An incident will be created, and the Customer will be notified by email	

In all cases, incidents raised that are dormant for 7 days without Customer input or further request for assistance shall be closed

4.3.2 UEBA Alert Content

Proact are aware of the sensitive nature of logging and alerting on user behaviour activity in regard to both user privacy and how the governance of the Customer's organisation may vary in how this should be dealt with, and the visibility of such activity. The Customer is responsible for investigating the behaviour of individual users and determining the internal actions to be taken. The Customer is also responsible for ensuring that they have the appropriate internal authorisation to process such data, and that they comply with all organisational policies and legal requirements regarding those processing activities.

Proact provide a self-service SIEMaaS-E interface via a UEBA (User Entity Behaviour Analytics) web portal that can be used by relevant authorised stakeholders in the organisation (HR officer / senior management / privacy officer) to understand and review user behaviour. This portal will continuously list live information showing the top risk users within the organisation based on the behaviour profiling.

Where there is a need or requirement for local IT staff to view general information in the self-service SIEMaaS-E portal, but the staff should not have detailed views of employee activity due to data privacy concerns, Proact can enable the following features in the self-service portal.

- RBAC (Role Based Access Control) to prevent these staff members from viewing information surrounding user activity.
- Data Masking/Obfuscation of sensitive Personal Identifiable Information such as the users full name, department or job role

When responding to and dealing with user behaviour risk alerts The Proact security team will perform an initial investigation to ascertain:

- The nature of the activity and whether it appears related to insider threat of a deliberately malicious nature; a compromised user account or behaviour that may be considered unacceptable to the organisation.
- The immediate threat to the organisation that the behaviour is potentially deemed to present.

4.4 Service Guides, Documents and Reports

Proact provide and maintain as required throughout the contract term the following service guides, operational documents and reports:

Deliverable	Frequency	Description and content summary
Service Specification/Contract	Contract	▪ A schedule of the Customer's contracted services and associated charges.
Service Level Agreements	Contract	▪ Proact's standard Service Level Agreements.
Standard Terms and conditions	Contract	▪ Proact's Standard Terms and Conditions which governs the services.
Managed Service Transition Guide	Start-up	▪ How services are transitioned into live operation.
Customer Prerequisites Guide	Start-up	▪ The activities the Customer must perform before the service can be commissioned.
Customer Service Operations Guide	Ongoing	▪ A guide to how Proact operate Customer service, how to communicate with Proact and how to best use the service.
Service Operations Manual	Ongoing	▪ Proact produce and maintain a *Service Operation Manual* document, which details the scope of the services provided including: ▪ Services and Service Levels Agreements ▪ Customer contacts ▪ Locations and environments ▪ Customer configuration items (Log Collectors) ▪ Change management contacts and classifications ▪ Incident management processes and contacts ▪ Regular scheduled operational activities

Deliverable	Frequency	Description and content summary
Service Review Report (SR)	Quarterly	▪ A quarterly Service Review Report showing service performance statistics, for example: ▪ Incident & change statistics ▪ Incident response times ▪ Incident by category ▪ Incident logged by method ▪ Incident and change log ▪ SIEM storage capacity and log volume reports ▪ SIEM statistics report, including: ▪ Most Impacted Log Sources ▪ Most Common Events ▪ Most Impacted Applications in the Customer's environment. ▪ Number of Log Messages processed in period ▪ Busiest Log Sources ▪ Average Messages Per Second ▪ SIEM incident review & recommendations ▪ SIEM utilisation & tuning advice, including: ▪ Identification of unnecessary log messages ▪ Recommendations for re-classification of logs, where appropriate
Major Incident Report	Per Major Incident	▪ In the event that a major incident occurs, for which Proact are responsible, Proact provide a *MIR* detailing the following: ▪ Timeline of the incident ▪ Root cause analysis ▪ Workarounds employed ▪ Remedial actions ▪ Lessons learned ▪ SLA status ▪ Proact aim to complete the MIR and deliver it to the Customer within ten working days of the resolution of the incident.
Service Transfer Policy	Contract	▪ Proact's policy for handling data and asset returns at end-of-C.
Service Transfer Plan	End of contract	▪ A plan for handling data and asset returns for the Customer, in accordance with the ***Proact Service Transfer Policy***.

5 Service Charging Policy

Item	Allocation model
Contract term	▪ 12 – 36 months
Professional Services Charges	▪ Calculated based on: ▪ Number of collection agents ▪ Number of log sources to configure ▪ Type of log sources ▪ Number of log sources requiring bespoke configuration or log sources not on the supported list of devices
Charging metrics	▪ Minimum commit and Flexible charge for the quantity of: ▪ Number of registered user identities ▪ Additional EPS consumption beyond usage allowed per user (*see **EPS Charges**, below)* ▪ Additional Log Retention period (GB) ▪ 2FA tokens for self-service management portal access ▪ A dedicated customer web console
User Identities	▪ SIEMaaS-E is charged using a user identity model. A user identity is defined as an 'Active' account within an Active Directory domain that is registered in the SIEMaaS-E platform. Active accounts can be users, administrator users or service accounts on the system. ▪ The SIEMaaS-E connection to Active Directory is made at the root of the domain(s) and therefore encompasses all active user accounts in the environment. ▪ The base monthly charge for the platform is defined by the minimum commitment of the contract for the predicted number of monitored user accounts. ▪ Flexible charges are applied on a monthly basis for each user account that is registered during that month into the SIEMaaS-E platform over the minimum commitment.
Storage Measurement	▪ Storage usage of total compressed archive data size on disk in GB measured as an average over the month.
EPS charges	▪ Each registered user identity in the platform is allowed to consume an average of 1.5 EPS (Events Per Second). EPS usage is calculated over a monthly average. ▪ Where monthly EPS usage totals greater than the number of user identities x 1.5, an additional flexible charge is applied for each EPS above this figure.
Billing profile	▪ Milestones or Time & Materials for Set-up charges ▪ Monthly or quarterly in advance for Minimum commit charges ▪ Monthly or quarterly in arrears for Flexible charges The Customer shall be invoiced for any additional user identities for the period, beginning on the first day of the month in which the report is provided.

6 Prerequisites, Responsibilities and Exclusions

The following table details:

- The following are the prerequisites that must be provided or completed by the Customer prior to Service Commencement
- The following are the responsibilities of the Customer in throughout the life of this service.
- The following are exclusions to the service provided by Proact

Prerequisites	Prerequisite 1: Provide a server for each SIEMaaS-E log collection agent ..... 8 Prerequisite 2: Notify Proact of the Public IP Address from which logs will be sent ..... 8 Prerequisite 3: Provision Active Directory user account for the SIEMaaS-E platform to utilise. . 9 Prerequisite 4: Configure a Windows server for Windows Event Collector service ..... 9 Prerequisite 5: Configure logging settings on in scope infrastructure. ..... 10 Prerequisite 6: Provide API access and user credentials for Cloud platforms or other API integrated components. ..... 10 Prerequisite 7: Open firewall ports as required ..... 11 Prerequisite 8: Download and install the Gemalto SafeNet MobilePass application ..... 12 Prerequisite 9: Provide usernames, email addresses and role requirements for Portal users. 12 Prerequisite 10: Provide remote access for Proact configuration and support tasks 12
Responsibilities	Responsibility 1: Nominate contact point for security risk alerts ..... 5 Responsibility 2: Implement Proact security recommendations as required ..... 6 Responsibility 3: Maintain operability of SIEMaaS-E Log Collector server(s) during contract term ..... 8 Responsibility 4: Provide administrator to configure Customer infrastructure ..... 11 Responsibility 5: Maintain sufficient network capacity for service operation ..... 11 Responsibility 6: Maintain compatibility of interacting external systems or environments at all times ..... 12 Responsibility 7: Patch guest OS for Log Collector and install Anti-Virus ..... 13 Responsibility 8: Provide at least 24-hours' notice of planned maintenance ..... 18 Responsibility 9: Assist in installation of log collection agents by providing elevated privileges 18
Exclusions	Exclusion 1: All configuration shall be performed by Proact remotely ..... 12 Exclusion 2: Unauthorised use of the Proact Self-service support portal and-or Service Desk 15 Exclusion 3: The solution does not support monitoring of Customer applications or appliances 18

7 Data Retention and Deletion

7.1 Data Retention

During transition, Proact and the Customer agree on a policy configuration that meets the Customer's retention requirements, within the operating parameters of the SIEMaaS-E product.

Proact's default policy is to retain log data for 90 days throughout the Contract period after which all logs will be deleted.

7.2 Data Deletion

Proact will only retain logs in line with the agreed SIEMaaS-E retention policy during the term of the SIEMaaS-E contract. It is not obligated to retain the data beyond the contract end date.

Following termination of contract the Customer can choose to either:

- Renew the Contract, if both parties agree new terms
- Request that Proact delete logs from the SIEMaaS-E platform, in which case Proact will:
  - Remove the Customer entity to prevent additional log messages from being collected.
  - Delete the Customer's archived logs once any log messages in the database have been flushed to the archive,
  - Advise the Customer that all the log messages have been deleted.
- Request that Proact extract and return logs from SIEMaaS-E platform storage (see Section **Error! Reference source not found.**: **Error! Reference source not found.**)

By default, Proact will, irrespective of the retention policy, delete the log message data unless written confirmation of the Customer's request for it to be extracted and returned is received within 30 days of the Contract termination date.

8 Vendor Terms

The following terms are applicable where SIEMaaS-E is delivered by Proact through the use of software provided by 'Securonix'.

MINIMUM TERMS FOR CUSTOMER AGREEMENT

Participant agrees to incorporate these minimum terms (the "**Minimum Terms**") in each Customer Agreement, and to cause these Minimum Terms to apply to each Customer, and each Customer's employees and individual consultants. Any capitalized terms used herein and not otherwise defined have the same meaning as given to such term in the Agreement.

1. Customer may access and use the Securonix Products solely in connection with the Service Provider Services provided by Participant and in accordance with any written or electronic documentation and any license restrictions set forth in the applicable License Agreement for such Securonix Product. Customer's consultants may access and use the Securonix Products solely on behalf of Customer for Customer's benefit in connection with Customer's receipt of Service Provider Services, provided that Customer shall remain liable for any non-compliance by its contractors with these Minimum Terms.

2. Customer shall not, and shall not permit its employees or consultants to, (a) license, sell, rent, lease, transfer, assign, distribute, host, outsource, disclose or otherwise commercially exploit the Securonix Software or Securonix Cloud offerings or make the Securonix Software or Securonix Cloud offerings available to any third party except that Customer may permit its affiliates or individual consultants to access and use the Securonix Software and Securonix Cloud offerings to the extent expressly permitted by Participant in accordance with Section 1 above; (b) modify, make derivative works of, disassemble, reverse compile or reverse engineer any part of the Securonix Software and/or Securonix Cloud offerings; (c) access the Securonix Software and/or Securonix Cloud offerings in order to build a similar or competitive software or service; (d) copy, reproduce, distribute, republish, download, display, post or transmit the Securonix Software or Securonix Cloud offerings in any form or by any means, including electronic, mechanical, photocopying, recording or other means. Customer acknowledges that Customer shall be fully responsible for all liabilities incurred through its use, or any of its employees or consultants use, of the Securonix Software and/or Securonix Cloud offerings.

3. Customer acknowledges and agrees that the Securonix Software may contain Open Source Software that is subject to the General Purpose License "GPL" or other open source licenses and Customer's acceptance of the Customer Agreement constitutes Customer's acceptance of additional terms, if any, included in the GPL with respect to such Open Source Software.

4. In the event Customer, or any of its employees or consultants, are in violation of the Customer Agreement, Participant and Securonix reserve the right to temporarily suspend, indefinitely suspend, or terminate a Customer's account or access to the Securonix Products. If Customer materially breaches any Customer Agreement relating to Securonix Products, Participant will notify Securonix of such breach.

5. Securonix has no obligation or responsibility whatsoever to provide support and maintenance services to Customer for any purpose.

6. Customer disclaims all representations and warranties by Securonix and Customer acknowledges that Securonix will have no liability to Customer, or any of its employees or consultants, and that Customer's and its employees' and consultants', sole and exclusive remedy for any claim arising under, or in connection with, the Customer Agreement shall be against Participant.