PROACT

Service Definition Document

SIEM as a Service

SDXSIEM-003 Published 09 October 2019
Public - Freely Distributable

Acknowledgements

Phone: +46 (0)8 410 666 00
Fax: +46 (0)8 410 668 80
Email: info@proact.eu
www.proact.eu

Proact IT Group AB
Kistagången 2
Box 1205
SE-164 28 KISTA

Contents

Chapters

Tables

Figures

1 Service overview

Proact's SIEM as a Service (SIEMaaS) is a remote monitoring and security service offered to improve customers' security knowledge of their infrastructure and application environments.

SIEMaaS is designed to meet the customer's requirement to store, analyse and triage data from infrastructure, operating system and application logs, and for being alerted to potential threats.

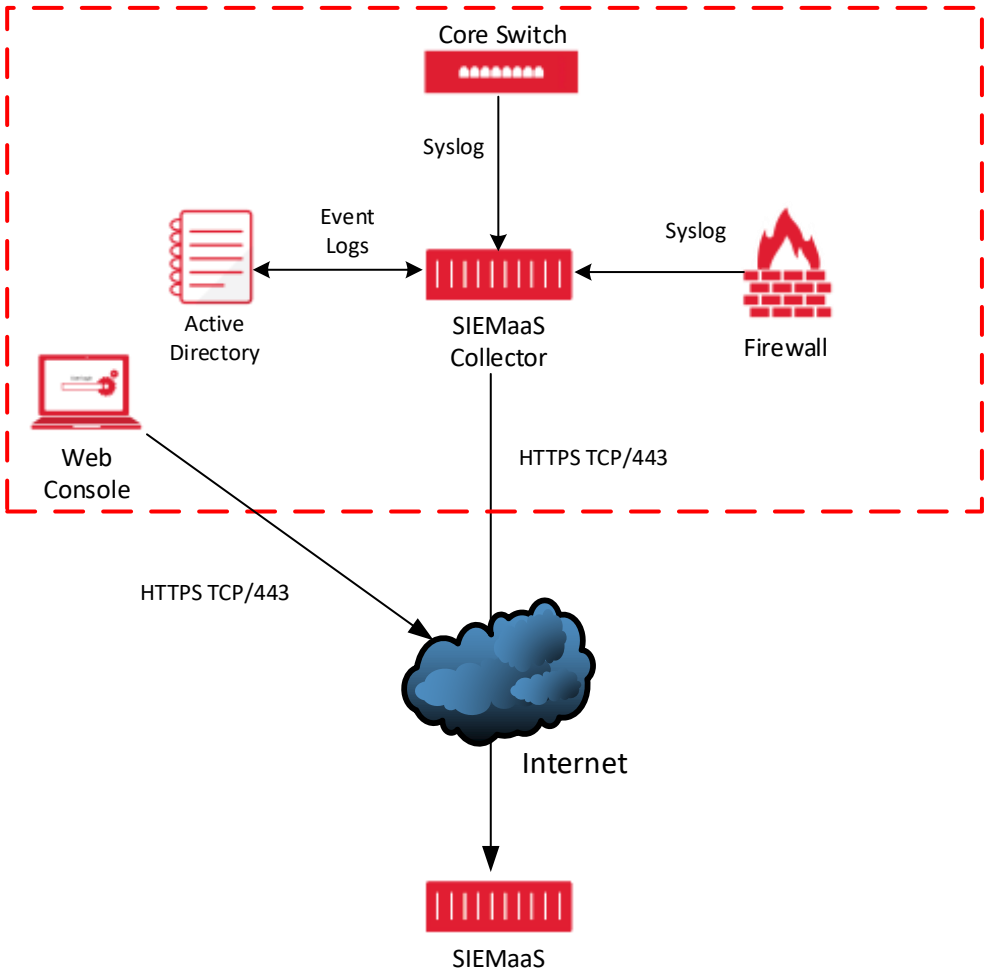
The solution provides for the remote collection and analysis of logs using an industry-standard Security Information and Event Management solution.

SIEM 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
- Security Operations team to produce historical reporting and perform log analysis.

This 24x7x365 service provides security guidance and advice to a customer's general IT team, whereby Proact's Security Operations Centre (SOC) to become a cost-effective virtual member of the customer's security team. This service package ensures that the customer's environment is analysed for suspect activity and advises the customer on appropriate steps to take to prevent suspect activity from escalating. The Managed service reduces the workload of the customer's Security Officer(s), by analysing and notifying them of high-risk events and continually tuning the alerting process, and ensuring that only abnormal events are escalated to the customer

Figure 1: SIEMaaS schematic diagram



2 Service scope

This chapter identifies and describes the high-level components that make-up the service, which comprise the:

- Service package – which defines the service, capabilities and options.
- Service platform infrastructure - which defines the service delivery mechanism, such as:
  - Service architecture
  - SIEM components
  - Connectivity
  - Applications and licensing
- Supporting services - any processes or resources that support the delivery of the service, such as the Self-service support portal, through which the customer's authorised users can log cases and change requests.

Further information …

See Service deliverables (Chapter 4 on page 11) for more detail on the components.

2.1 Service package

Objective	To provide the remote collection and analysis of logs using an industry-standard Security Information and Event Management solution.
Description	SIEMaaS simplifies the task of identifying, analysing and understanding security events by correlating the dispersed 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 an alerting facility for unexpected events detected in the environment ▪ Comprehensive and easily accessible data.
Hosted-in	A Proact datacentre on 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 SIEMaaS includes built-in log parsers for a wide range of industry-leading infrastructure components, operating systems and applications, providing out-of-the-box best-practice log classification. For systems that do not have built-in log parsers available, Proact's SOC will work with the Customer to define common log patterns that can be classified using Regular Expressions (RegEx).
Supported-from	All support and management is delivered remotely from a secure, accredited *Proact Network Operations Centre (NOC).*
Support level	Monitoring, support and service management of the infrastructure only.
Required connection types	All connections are encrypted over the public internet.
Engagement	▪ Use the Proact Self-service management portal – see Appendix B: (on page IV) – to monitor SIEM activity ▪ Use the Proact Self-service support portal to request additions of log sources

SIEMaaS Deliverables	▪ Usage reporting & billing ▪ Log data consolidation ▪ Log data classification ▪ Log data risk scoring ▪ Tuning activities ▪ Security risk notification (email, 24x7x365) ▪ Security specialist guidance & advice ▪ Access to assistance from Proact security team ▪ Review & recommendations for incidents logged ▪ Reporting engine for custom reports ▪ Regular summary report (SIEM statistics) ▪ Regular summary report (SIEM utilisation & tuning) ▪ SIEM self-service management portal
	Service capabilities
Log monitoring	▪ The Proact SIEMaaS platform monitors customer log sources 24x7x365
Log data consolidation	▪ Proact handle the consolidation and storage of all logs sent by items in the scope of the solution ▪ Logs are retained for the customer specified retention period ▪ Logs are viewable through a central point, the self-service management portal
Log data classification	All log messages are automatically classified in to categories such as: ▪ Access control ▪ Audit ▪ Security ▪ Error
Log risk scoring	▪ Each log message is assigned a risk score based on its type, contents and source
Log source alerts	▪ Proact raise alerts if a log source fails
Reporting engine	SIEMaaS provides a configurable reporting engine that customers can use to generate a wide array of reports. For example: ▪ List: Top 10 Log Sources over the period (by IP / hostname) ▪ List: Top 10 Log Sources generating suspicious log activity ▪ Pie Chart: Percentage of events logged in each criticality ▪ Pie Chart: Percentage of events logged by each device type ▪ Line Graph: Events per second daily average

Self-service management portal	▪ A Self-service management portal allows customers to monitor the status of their items covered by the SIEMaaS solution. Functionality includes:
	  ▪ View trends, reports, alerts, and a near-live log view
	  ▪ Perform searches and investigations
	  ▪ Create cases relating to the log data from the items monitored in the SIEMaaS solution scope.
	▪ Full details are provided in Appendix B: (on page IV).

Raise security risk alerts	Security risk alerts, identified by the Proact Security team, are sent by email to a nominated customer contact as defined in the customer's Service Operations Manual. Responsibility 1: Nominate contact point for security risk alerts

Access to security specialists	Proact security specialist are available, when necessary, to assist the customer to:
	▪ Investigate security risks on the customer's behalf
	  ▪ The Proact Security Team analyse and filter the events as they are logged
	▪ Provide detailed guidance and advice on dealing with security risks to customer representatives
	  ▪ The Proact Security Team provide recommendations (via email or support portal) in line with best practices.
	  ▪ The customer is responsible for implementing these recommendations.

	Responsibility 2: Implement Proact security recommendations as required
Recommend continuous improvement activities	Recommendation to help give the customer an increased view-of and control-over security incidents. For example, expanding the scope of SIEMaaS to include additional log sources, or enable verbose logging for increased visibility and more holistic security intelligence.
Tuning activities	Fine-tuning security measures ensures the customer maximises the value of their SIEMaaS solution. This can include, for example, turning off unnecessary log messages and automatically reviewing the noisiest log sources thereby increasing the efficiency of the solution.
	Service Options

Agents	Additional logging capability can be obtained from desktops and servers with the deployment of local agents providing:
	▪ Registry Monitoring
	▪ Independent process monitoring
	▪ Network connection monitoring
	▪ User activity monitoring
	▪ Data Copy Logging from local to removable storage devices
	▪ File integrity monitoring for desktops and servers
	  ▪ Detect reads, modifications, and deletions
	  ▪ Identify specific user or application
	  ▪ Support for policy layering
	
	Different agents are required for servers and desktops.

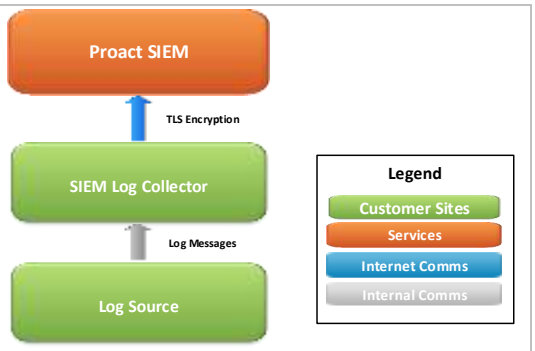
Log Retention	Log data is retained for 90 days by default. Extended retention beyond 90 days is available, up to the duration of the contact.

2.2 Service infrastructure

2.2.1 Service platform

Platform	▪ A securely-segmented multi-tenant platform within a Proact datacentre ▪ Each customer is provided a distinct collection entity, ensuring they can see only their own logs. ▪ Utilises proven industry-leading SIEM software
Storage	▪ Proact provides secure storage vault capacity to cater for the contracted volume of log data sent to the SIEMaaS platform. This capacity is used to hold the central log database for each customer, retaining data in line with the contracted retention period

2.2.2 Components

Component summary	Proact's SIEMaaS offering is based on Enterprise SIEM software and structured in a hub-spoke topology. It comprises four main components: ▪ Multiple SIEMaaS Log Collectors ▪ A SIEM master service ▪ A Self-service management portal 

Log Collector	▪ The SIEMaaS Log Collectors are installable software packages running on dedicated Microsoft Windows Server operating systems on the customer's site(s).
	  ▪ The Customer must provide a Windows Server for each Log Collector (see Appendix A.1.1: on page II)
	▪ Each SIEMaaS Log Collector collects logs from the devices in its local security zone, they:
	  ▪ Act as receivers for log messages sent to them (for example, by syslog) from monitored items in the customer's environment
	  ▪ Perform log collection by remotely logging on to machines in their respective network segments and collecting flat log files from, for example, hardware devices, operating systems, and applications, using the appropriate collection methods, which include (non-exhaustive):
	  ▪ IETF Syslog (client-initiated, unauthenticated)
	  ▪ SNMP Trap (client-initiated, unauthenticated)
	  ▪ NetFlow (client-initiated, unauthenticated)
	  ▪ Microsoft Windows Server Event Logs (collector-initiated, authenticated by Active Directory)
	  ▪ Encrypt the raw log information obtained from the LAN
	  ▪ Pass the information to the SIEMaaS Master service
	▪ Typically one SIEMaaS Log Collector per monitored network segment or vLAN is required.
	▪ The customer is responsible for determining the level of logging on their devices, and the intelligence gathered from the logs will be restricted by the verbosity of the log content

	Prerequisite 1: Provide Windows Server for SIEMaaS Log Collector Prerequisite 2: Deploy SIEMaaS Log Collector software Responsibility 3: Maintain operability of SIEMaaS Log Collector server(s) during contract
Master Service	▪ The resilient central SIEM master service is located in a Proact's datacentre ▪ Receives consolidated log data from SIEM Log Collectors and SIEMaaS Mediator Proxies.
Monitoring	The *Proact SIEMaaS platform* monitors the customer environment, monitored items include: ▪ SIEMaaS platform ▪ SIEMaaS log monitoring software ▪ SIEMaaS storage systems ▪ SIEMaaS hypervisors ▪ Log sources

Endpoint configuration	The Customer should: ▪ Create a read-only Active Directory service account to be used by the SIEMaaS Log Collector to connect to in-scope Windows Server endpoints to collect Event Logs ▪ Configure syslog or SNMP Trap on each endpoint (appropriate to capability) to point to the IP address of the server running the SIEMaaS Log Collector Prerequisite 3: Configure active directory account for remote Windows Event Log collection Prerequisite 4: Configure syslog on each endpoint for SIEMaaS Log Collector server IP

2.2.3 Service connectivity

Connectivity options	▪ All communication between the customer's site(s) and Proact datacentre(s) is over encrypted (HTTPS/SSL/TLS) public internet link; there is no requirement for a site-site VPN or other dedicated communications channel ▪ For security purposes all SIEMaaS data, in flight or at rest, is encrypted
Firewall	▪ 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) ▪ The open port requirements are documented in Appendix A.2: on page II ▪ During the initial setup phase, and throughout the term of the contract, a customer representative must be available to assist with configuring their firewall(s) and other security devices to allow new log sources to contact Log Collectors, and to allow new Log Collectors to contact the central SIEMaaS platform in Proact's datacentre **Note**: Where log traffic between in-scope devices and the SIEMaaS Log Collector must traverse a firewall additional rules must be configured (see *Appendix A.2.1: on page II*) **Note**: A separate internet connection and firewall is required for each site location unless the site(s) are connected through an internal WAN. **Note**: The customer must notify Proact of the public IP address(es) the logs will be sent from, to allow the IP to be whitelisted Prerequisite 5: Provide an administrator to assist with firewall configuration as necessary Prerequisite 6: Open firewall ports as required Prerequisite 7: Notify Proact of the Public IP Address from which logs will be sent
Bandwidth use	SIEMaaS communications bandwidth is sized based on the following assumptions: ▪ Average size of an encrypted log message sent by SIEMaaS: 500 Bytes ▪ Average number of log messages sent by items in the SIEMaaS scope: 3 per second ▪ The minimum bandwidth required is 1Mbps The above is based on an average environment which may vary based on the types of items managed by individual SIEMaaS deployments and the number of messages generated.
Connectivity for self-service management portal	▪ The self-service management portal provides secure access using HTTPS (TCP port 443). ▪ Secure access to the service is maximised by restricting it to whitelisted IP addresses. This requires the customer provide Proact with a list of the IP addresses requiring portal access. Prerequisite 8: Identify IPs requiring self-service management portal access

Connectivity for transition	Proact undertake all Service configuration in-scope remotely, and therefore the customer should provide resource for this remote access. The customer must also ensure that their network environment has sufficient capacity, ports and configuration to support on-going service operation.
	Prerequisite 9: Provide remote access for Proact configuration and support tasks Exclusion 1: All configuration shall be performed by Proact remotely Responsibility 4: Maintain sufficient network capacity for service operation
Interoperability with Customer-managed systems	Where this service interacts with any system, application or environment not managed by Proact, it is the customer's responsibility to ensure that it remains compatible with any Proact-managed systems/applications at the hardware, firmware, *OS*, and application version levels – as recommended by Proact or its vendors as best practice.
	Responsibility 5: Maintain compatibility of interacting external systems or environments at all times

2.2.4 Service security

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

See also …

Further details are available in the technical white paper Proact Managed Service Security Policy.

Anti-virus protection	Proact's infrastructure incorporates enterprise level antivirus protection.
Patching	Proact and the customer will manage patching according to the following responsibilities. ▪ SIEMaaS platform patching – Proact are responsible for patching and updating all the infrastructure software and hardware under their management ▪ Operating system patching – It is assumed that customers will maintain and patch the servers on their premises running SIEM Log Collector.
	Responsibility 6: Patch guest OS for Log Collector
Data encryption	▪ Secure HTTPS/SSL/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 ▪ 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 limited log of all actions undertaken on the platform. 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. These audit logs are available to Proact's security team only.

2.2.5 Applications and licensing

SIEM Licensing	Proact provide all licensing for SIEM Log Collectors and for the processing of log messages through the SIEM Master server
Log Collector servers	The Customer must provide appropriate operating system licensing for all Log collectors

2.3 Supporting services

<table>
<tr>
<td>Proact Service desk</td>
<td>

Provides 24x7x365 support and management of the service and supporting infrastructure – see

<table>
<tr><th colspan="2">Service Options</th></tr>
<tr><td>Agents</td><td>Additional logging capability can be obtained from desktops and servers with the deployment of local agents providing:
Registry Monitoring
Independent process monitoring
Network connection monitoring
User activity monitoring
Data Copy Logging from local to removable storage devices
File integrity monitoring for desktops and servers
Detect reads, modifications, and deletions
Identify specific user or application
Support for policy layering
Different agents are required for servers and desktops.</td></tr>
<tr><td>Log Retention</td><td>Log data is retained for 90 days by default. Extended retention beyond 90 days is available, up to the duration of the contact.</td></tr>
</table>

Service infrastructure (Section 0, on page 5)
Handles events, requests, queries and incidents raised by authorised users only, whether by phone, e-mail or self-service support portal
Handles Change Requests (CR) in accordance with Proact’s Change Management process.
Resolves problems with, applies changes to and maintains the patch state of, the service platform in accordance with Proact's change management process
Makes configuration changes on request (for example, changes to log feeds).

</td>
</tr>
<tr>
<td>Proact Self-service support portal</td>
<td>Proact provides customer-nominated administrators with access to a Self-service support portal through which they can:

Request additional log sources to be configured
Create new and update existing incidents for investigation
Create new and update existing changes from a change catalogue

The credentials assigned to users are for their sole use. Shared accounts are not available.
</td>
</tr>
</table>

3 Available service levels

This chapter identifies the service level measures applicable to the service – see Table 1 (below)

You should consider these measures in the context of the general terms and conditions described in full in the ***Proact Service Level Agreement*** document, which customers may view at this web address: http://www.proact.eu/terms.

Table 1: Available service level measures

Availability	▪ SIEMaaS

Response time	▪ Incidents
	  ▪ P1
	  ▪ P2
	  ▪ P3
	▪ Changes
	  ▪ Standard
	  ▪ Normal
	  ▪ Emergency

4 Service deliverables

This chapter provides more detail about the deliverables that make up the Service package described in *Section 2.1 (on page 3)*.

4.1 ITIL processes

Proact monitor, support and manage the service infrastructure using processes aligned with the ITIL framework for IT Service Management.

This section summarises the processes' key capabilities and deliverables.

> The Proact Customer Service Operations Guide provides full detail on how Proact deliver and operate these processes.

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 take whatever action is required to restore operation and-or to minimise any service down time. ▪ 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 Resources

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 do 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. Prerequisite 10: Provide appropriate browser for Self-service management portal
Proact Self-service monitoring portal	Continuous	Proact provide the customer with access to the Proact Self-service monitoring portal, showing monitoring metrics for in-scope systems, to allow customer administrators to view trends and manage infrastructure resources.

4.3 Operational Activities

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.
Log classification	Continuous	▪ The Proact SIEMaaS platform automatically classifies all logs sent to it. Categories include, for example, as access control, audit and security.
Risk scoring	Continuous	▪ The Proact SIEMaaS platform automatically risk scores all logs sent to it. Scoring is based on message type, message content and log source.

Deliverable	Frequency	Description and content summary
Alert handling	Per Event	▪ Where Proact detect an unusual event or an alert threshold is breached the Proact Service Desk deal with the alert directly, generating a support case, investigating the issue and taking appropriate action as required.
Alert notification	Per Event	▪ Proact will send email notification whenever they detect an unusual event or an alert occurs.

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 by the change control process
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 to sites, networks or other devices that may affect the availability, communicability, performance or integrity of any system monitored or managed by Proact **See also**: Proact's Customer Service Operations Guide, where this requirement is described further Responsibility 7: Provide at least 24-hours' notice of planned maintenance
Change Management	Continuous	All changes to the customer's log sources or policy configuration are planned and implemented according to the Proact Change Management processes

Deliverable	Frequency	Description and content summary
Platform Monitoring	Continuous	▪ Proact continuously monitor the availability of the SIEMaaS platform. ▪ The service is deemed available if the SIEMaaS 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 Log Collectors. Upon detection of interruption of log feeds, Proact will alert the customer and recommend action to remediate, such as: ▪ Reboot a Log Collector ▪ Reboot a log source ▪ Amend the firewall configuration. Exclusion 3: The solution does not support monitoring of customer applications or appliances
Storage Capacity Management	As required	Proact extend storage capacity in line with contractual limits where storage volumes reach certain thresholds to ensure that they do not run out of space.
Log Collector Installation	As required	Proact will assist the customer with the installation of additional Log Collectors as required. The customer must complete the documented pre-requisites for additional Log Collectors and Mediator Proxies, and provide an administrator with elevated privileges to work with Proact engineers on the installation. Responsibility 8: Assist in installation of Log Collectors and Mediator Proxies by providing elevated privileges

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	A schedule of the customer's contracted services and associated charges.
Service Level Agreements	Contract	Proact's standard Service Level Agreements.
Terms and conditions	Contract	Proact's terms and conditions for all services.
Managed Service Transition Guide	Start-up	How customer 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.

Deliverable	Frequency	Description and content summary
Service Operations Manual	Ongoing	Proact produce and maintain a *SOM* document, which details the scope of the services provided including: ▪ Services and service levels ▪ Customer contacts ▪ Locations and environments ▪ CIs ▪ Change management contacts and classifications ▪ Incident management processes and contacts ▪ *Monitoring Thresholds* and defined event response actions ▪ Regular scheduled operational activities
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 With the **Managed** service-package, Proact will also include the following in the Service Review Report: ▪ SIEM incident review & recommendations ▪ SIEM utilisation & tuning advice, including: ▪ Identification of unnecessary log messages ▪ Recommendations for re-classification of logs, where appropriate **Note**: This is an example report. Technical content is subject to change
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-contract.
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***.

4.5 Meetings

The following meetings are held between the customer and Proact as part of this service:

Deliverable	Frequency	Description and content summary
Service Review Meeting	Quarterly	A Service Review teleconference meeting is held between the customer, their assigned SDM and Account Manager, and a security specialist from Proact's SOC, to discuss the performance and use of the service, and identify any future requirements for expansion, integration or additional services. This meeting takes place following delivery, by email, of each period's Service Review report and covers the following agenda items at a minimum: ▪ Review of Proact's performance against SLAs ▪ Review of any high-impact Incidents or Problems from the reporting period ▪ Review of capacity (where relevant) ▪ Recommendations by Proact for any non-essential remedial work or upgrades that should be considered ▪ Review new Proact technologies / services as appropriate ▪ Overview from the customer of any relevant forthcoming projects and plans that may require assistance from Proact ▪ Overview from the customer of key priorities for the next period ▪ Review usage and consumption of licence entitlements where relevant ▪ Review of the SOM, and any other service-specific documentation that requires regular customer review. ▪ Review of system capacity growth, performance, risks and other technical observations and recommendations. ▪ Provision of guidance on inclusion of additional monitored devices or on configuration changes for increased visibility and security intelligence.
Service Improvement Plan Meeting	Weekly, Fortnightly or Monthly, as preferred by the customer	▪ Proact hold a teleconference meeting to review the SIP with the customer ▪ The frequency of this meeting is jointly agreed between Proact and the customer, and may be varied throughout the term of the contract as required.
Other Meetings by Request	Upon Request	Proact join teleconference meetings and, according to availability, any other meetings requested by the customer. Meetings may involve third parties of either Proact or the customer, but there must always be a representative of both Proact and the customer in attendance.

5 Service transition

Proact use a standard methodology for transitioning the customer's services into live operation.

This methodology is described in full in the ***Proact Managed Service Transition Guide***.

Transition prerequisites
▪ General prerequisites are detailed in the ***Proact Customer Prerequisites Guide***
▪ Service-specific *prerequisites* are summarised in Chapter 7 (Service demarcation) of this document.

Proact follow a Stage 0-6 model for all Service Transitions (Figure 2 below).

Figure 2: Stage 0-6 transition model

Meetings	**Service transition workshop** The Customer is required to attend a Service Transition workshop and any further workshops required to complete the detailed service and technical design, and make available appropriate service and technical personnel with suitable skill sets at these meetings. ▪ Service owners and-or technical owners for any log sources to be collected by Proact ▪ Technical owners for any supporting infrastructure needed to allow Proact to collect and transmit logs (for example, network engineers, for creating firewall rules) ▪ Project manager, if the customer has chosen to use one. **Project Closedown** The Customer is required to attend a Project Closedown meeting to formally close projects for transitioning new services into operation.
	Prerequisite 11: Provide appropriate customer representation at transition workshops Responsibility 9: Provide appropriate representation at project closedown workshop
Data migration	Migration of log history from legacy SIEM systems to Proact's SIEMaaS platform is not included in this service.
	Exclusion 4: Data migration is excluded from the scope of service transition
Training sessions	▪ Using the Proact Self-service management portal A Proact engineer will provide a single remote web-based training session to the customer's administrator(s) covering the access and use of Proact's Self-service management portal for SIEMaaS, which will include: ▪ How to view backup job statuses ▪ How to initiate restore operations ▪ Using the Proact Self-service support portal Proact provide, on request, a single remote web-based training session to the customer's administrator(s) covering the access and use of Proact's Proact Self-service support portal, to supplement the instructions provided in the ***Proact Customer Service Operations Guide***

6 Service charging policy

Proact's monthly invoicing and flexible usage models free the customer's capital budgets.

Self-service portals and intrinsic infrastructure support minimise mundane operational tasks, freeing the customer's focus for strategic business projects.

Proact base the charges for the solution on usage information provided and on assumptions made on the basis of that information, all of which forms part of the contractual agreement. Any prolonged and significant variation in usage may require a reassessment of the charges.

Table 2: Service charging-model

Item	Allocation model
Contract term	12 – 60 months
Professional Services Charges	Calculated based on: ▪ Number of log collectors ▪ Number of log sources ▪ Type of log sources ▪ Number of log sources requiring custom SIEM log parsers
Charging metrics	▪ Minimum rate of Messages per Second (MPS) ▪ Overage charges for oversubscribed months ▪ Number of Server Agents and Desktop Agents ▪ Log Retention period (GB)
Oversubscribed Months	Any month where the average MPS rate over the month is greater by 10% than the Minimum MPS monthly rate
Messages Per Second (MPS) Measurement	The Minimum MPS rate is 250. A larger initial Minimum MPS rate can be defined in the Customer Service Specification. MPS is measured on a rolling 24-hour average of messages per second, received by the SIEM Master Service whereby "message" means an individual log or system event. If there are 2 consecutive Oversubscribed Months during the contract term, the customer will pay additional charges in arrears at the flexible MPS rate defined in the Customer Service Specification, for both such months and for the remainder of the contract term. The new Minimum MPS rate will be measured by the peak 72-hour average MPS quantity during the prior 2 months.
Agent Measurement	▪ The number of deployed Desktop based agents ▪ The number of deployed Server based agents Add-on orders for Agents after commencement of the service will be co-termed with the current contract term
Storage Measurement	Storage usage of total compressed archive data size on disk in GB measured as an average over the month.
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 additional charges and the additional MPS rate for the period, beginning on the first day of the month in which the report is provided.

Item	Allocation model
Termination Notice Period	Notwithstanding the operation of clause 33 of the Standard Terms and Conditions or any clause dealing with termination of any services within the Contract, the SIEMaaS services to which this document relate shall automatically renew for successive 12 month periods unless either party provides written notice of termination at least 90 days before the expiration of the then current Minimum Service Term. For the avoidance of doubt, the Minimum Service Term as it relates to any other Managed Services shall be unaffected

7 Service demarcation

This chapter identifies the prerequisites, responsibilities and exclusions upon which the delivery of the service defined in this document depends.

Prerequisites	
Responsibilities	
Exclusions	

Glossary

Term		Definition
Availability SLA		Availability service level agreements, typically defined in terms of service up-time, are particularly applicable for infrastructure and service provision arrangement where a continuous IT service is provided.
Change advisory board	CAB	Delivers support to a change management team by approving requested changes and assisting in the assessment and prioritisation of changes.
Change request	CR	A document requesting a change to an item within the scope of the contracted service, or to the service itself
Configuration item	CI	A hardware, firmware, software or other item monitored, supported and-or managed by Proact. That is, it is included in the agreed list of in-scope items as an item covered by the selected service
Configuration management database	CMDB	A repository for information technology installations. It holds data relating to a collection of IT assets
Contract change note	CCN	Contract change notes are used to legally document amendments to contractual commitments during the contract term
Contractual SLA		A Contractual service level agreement defines the boundaries of responsibility between customer and supplier, sets standards of performance and defines the measurement of service performance. It commits the supplier to delivering to required service levels and identifies the consequences of failure, usually in the form of service credits or other compensation.
Customer service operations guide	CSOG	The Proact Customer Service Operations Guide. A guide to how Proact operate customer service, how to communicate with Proact and how to best use the service.
Customer service specification		Defines the service configuration to be deployed for a specific customer
Customer-site	Site	Customer-site refers to a geographically-local collection of in-scope customer networks, devices or resources, whether they are physically located on customer premises, in a Proact or third-party provider datacentre, or in a Proact or third-party public or private cloud.
Dashboard		A view presented via a Proact Portal or application that shows the current service status and a summary of performance and usage.
Datacentre	DC	A data centre is a facility used to house computer systems and associated components, such as telecommunications and storage systems
Disaster recovery	DR	The process of restoring and assuring the continuation of essential IT services in the event of a disaster disrupting normal operation/
Exclusion		Exclusions are, for the purposes of this document, items outside of the scope of this service contract for which Proact are not liable.

Term		Definition
ITIL	Information Technology Infrastructure Library	A set of practices for IT service management that focuses on aligning IT services with the needs of business.
ITSM	IT Service Management system	The system used by the Proact Service desk to manage events, incidents, problems and changes
Log Collector		The (virtual) machine that is used to collect logs from configured log sources.
Major incident		The parties and process for declaring an incident a major incident are agreed during service transition. Whilst no formal ITIL definition exists these are typically incidents with significant corporate impact over and above a P1 incident, which do not require invocation of disaster recovery.
Major incident report	MIR	Major incident reports identify incident timeline, root cause, workarounds and-or remedial actions and lessons learned
Monitoring threshold		The monitoring threshold is the trigger value beyond which an alert will be raised. See also – threshold breach
Network operations centre	NOC	A location from which Proact deliver their monitoring, support and or management services.
Near-real-time		Near real-time (in telecommunications and computing) refers to the time delay introduced by automated data processing or network transmission between the occurrence of an event and the use of the processed data (for example, for display or feedback & control purposes).
Operating System	OS	The program which, after initially loading, manages the other programs in a (virtual) machine. The installed applications make use of the operating system. For example, Microsoft ® Windows ®, Windows Server ® and Linux ®
Prerequisite		Prerequisites are, for the purposes of this document, tangible resources, actions or commitments without which the service cannot be initiated and whose provision and maintenance (where applicable) is the responsibility of the customer for the duration of the contract.
Proact Premium Support	PS	Proact Premium Support is Proact's proven break-fix support solution
Proact Premium Support Plus	PSP	Proact Premium Support Plus is Proact's proven monitoring solution
Public IP Address		IP address that can be accessed from the public internet.
Remote desktop protocol	RDP	Remote desktop protocol provides remote display and input capabilities over network connections for Windows-based applications running on a server.
Regular Expression	RegEx	A sequence of characters that define a search pattern
Response-time SLA		Response time service level agreements define the time taken to respond to a reported event.
Responsibility		Responsibilities are, for the purposes of this document, ongoing actions or commitments necessary to sustain service delivery, which must be maintained for the duration of the contract

Term		Definition
Service delivery manager	SDM	Proact service delivery managers oversee the delivery of a service or service technology to the customer. The SDM establishes policies designed to ensure consistently high service performance, monitors the delivery and responds to customer feedback to develop quality improvement processes.
Service improvement plan	SIP	The Proact maintained service improvement plan logs and tracks the status of any technical or service issues highlighted by the customer or by Proact in relation to the service provided
Service operations manual	SOM	The Service operations manual details the scope of the services provided.
Service transition		The process of transitioning a contracted service from planning through to a live delivery state.
Security Information and Event Monitoring	SIEM	A software toolset that Software tools that collates, manages, analyses and correlates multiple sources of security information and log files in a network
Service level agreement	SLA	An official commitment to the level of service provision that prevails between a service provider and their customer
Security Operations Centre	SOC	Proact's security monitoring and management function, and its associated analysts
SNMP traps		Alert messages sent from remote devices to a central collector
Syslog		A logging standard that allows event messages to be sent from network devices to a logging server
Threshold breach		In the context of the Proact Monitoring Platform a threshold breach occurs when an event on a monitored item exceeds a pre-set threshold. For services that include monitoring, Proact define these thresholds and agree them with the customer during the service transition stage, they are maintained throughout the contract term. See also – Monitoring thresholds
Trend analysis		Analysis of data to identify patterns. Trend analysis is used in problem management to identify common points of failure or fragile configuration items.
User		A user is a customer defined entity that allows an administrator to login to Proact's Self-Service Portals.
Virtual Servers		A Virtual Server, or Virtual Machine, is an Operating System which runs in a container within a hypervisor host, and imitates a hardware server.

Appendices

Appendix A: Technical Requirements

A.1: Minimum server specifications

A.1.1: Log Collector

A dedicated server (preferably virtual) running Microsoft Windows Server is required to run each Log Collector. The network location of these servers will be agreed between Proact and the Customer during Service Transition.

The minimum requirements for each server are as follows:

- Windows Server 2008 or later (full installation)
- 2 x (v)CPU
- 4GB (v)RAM
- 1 x (v)NIC
- Minimum 65GB Disk

The above minimum specification is for basic operation - resource requirements may be higher (and therefore may need to be amended by the Customer during the term of the contract) depending on the log volume generated from of the in-scope endpoints.

A.2: Firewall Ports

A.2.1: Ports required for Log Collection

The following firewall rules must be implemented where devices sending logs to / having logs collected by the Log Collector are located in different security zones from the collector and the traffic must therefore traverse a firewall.

NOTE: These rules are not required for any systems in scope that can communicate directly with the SIEM Log Collector without going through a firewall.

Component Interaction					
Client	**Client Port**	**Server**	**Server Port**	**Protocol**	**Communications**
Devices Sending Logs					
UDP Syslog Device	Random	SIEM Collector	514	UDP	Unidirectional
TCP Syslog Device	Random	SIEM Collector	514	TCP	Unidirectional
NetFlow v1, v5 or v9 Device	Configurable	SIEM Collector	5500	UDP	Unidirectional
J-Flow Device	Configurable	SIEM Collector	5500	UDP	Unidirectional
sFlow Device	Configurable	SIEM Collector	6343	UDP	Unidirectional
SNMP Trap Device	Configurable	SIEM Collector	161	UDP	Unidirectional
Remote Log Collection					
SIEM Collector	Random	Windows Host (Windows Event Logs)	135, 137, 138, 139,445	TCP/RPC	Bidirectional, Client Initiated
SIEM Collector	Random	Database Server (UDLA)	DB Server dependent*	TCP/ODBC	Bidirectional, Client Initiated
SIEM Collector	Random	Check Point Firewall	18184	TCP/OPSEC LEA	Bidirectional, Client Initiated
SIEM Collector	Random	Cisco IDS (SDEE)	443	TCP/HTTPS	Bidirectional, Client Initiated
SIEM Collector	Random	Nessus Server	8834	TCP/HTTPS	Bidirectional, Client Initiated

SIEM Collector	Random	Qualys Server	443	TCP/HTTPS	Bidirectional, Client Initiated
SIEM Collector	Random	Metasploit Server	3790	TCP/HTTPS	Bidirectional, Client Initiated
SIEM Collector	Random	Nexpose Server	3780	TCP/HTTPS	Bidirectional, Client Initiated
SIEM Collector	Random	Retina Server	1433	TCP/ODBC	Bidirectional, Client Initiated
SIEM Collector	Random	eStreamer Server	4444	TCP/HTTPS	Bidirectional, Client Initiated

* The server port for UDLA collection will vary based on the database server being queried.
(SQL Server default = TCP 1433; MySQL default 3306; Oracle default = TCP 1521; DB2 default = TCP 50000)

A.2.2: Ports required for SIEM Master Service

The following rules are required to allow Log Collector(s) to communicate directly with Proact's central SIEM platform:

Client	Client Port	Server	Server Port	Protocol	Communications
SIEM Log Collector(s)	3333	Proact Master SIEM Service	443	TCP	Unidirectional

Appendix B: Self-service management portal functionality

The service includes a configurable Self-Service Management Portal engine that can be used to generate a wide array of reports, and allows multiple focussed dashboards to be created for a variety of audiences (e.g. technical, security, executive).

The functionality of the Portal includes:

- Searching
  - Usernames
  - IP Addresses
  - Hostnames
  - Geographic Location
  - Log Classification
  - Create, store and rerun searches
- Create Cases
  - Add selected logs
  - Share case with collaborators
  - Audit trail for each case
- Dashboards (Trends)
  - Top X information
  - Double click drill down functionality
  - Internal/External flow of events
- Analyse
  - Detailed look in to log data
  - Correlate activities
  - Extract raw log data

Appendix C: Data retention, deletion and extraction

C.1.1: 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 product.

Proact's default policy is to retain log data for 90 days on the platform for operational purposes. Where log retention for archiving purposes is required the customer may request separately to have them retained for up to the duration of contract.

Archived logs can be retrieved by the customer via a change request submitted to Proact through the portal.

C.1.2: Data Deletion

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

At the end of the contract term the customer can choose to either:

- Renew the contract, if both parties agree new terms
- Request that Proact delete logs from the SIEM 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 SIEM platform storage (see Section C.1.3:)

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.

Exclusion 5: Log data is not retained beyond the contract end date

C.1.3: Data Extraction

If the customer requests that Proact extract and return logs at the end of the contract term, Proact will:

- Export the log message data into native format (flat files) on customer provided hardware (servers and-or storage as appropriate) so that it can be accessed by the customer as required.
- The customer's participation in the process is necessary to agree the logistics around the extraction and to organise for any resources required.

Note: This is not a part of Proact's standard managed service offering. The required work is undertaken as a standalone project, scoped and costed on receipt of the customer's notification of its intent to recover the data. Log data is stored in a proprietary format for the SIEM software platform and will exported as such.