PROACT

Service Definition Document

Vulnerability Assessment as a Service

SDXVA-002 Published 09 October 2019

Public - Freely Distributable

Acknowledgements

Rapid7, NeXpose, Metasploit and SecurityStreet are registered trademarks of Rapid7 LLC.

ITIL® is a registered trademark of AXELOS Limited. All rights reserved

Linux ® is a registered trademark of Linus Torvalds administered by Linux Marks Foundation

Microsoft and Windows are registered trademarks of Microsoft Corporation

Any other brand or product trademarks (registered or otherwise) referenced within this document – but not explicitly acknowledged here – are the intellectual property of their respective holders and should be treated as such.

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

PROACT

Contents

Chapters

1 Service overview **1**
2 Service scope **3**
3 Available service levels **9**
4 Service deliverables **10**
5 Service transition **15**
6 Service charging policy **16**
7 Additional services **17**
8 Service demarcation **18**
Glossary **19**
Appendices ..... **I**
Appendix A: Technical Requirements II
Appendix B: Self-service support portal IV
Appendix C: Data retention, deletion and extraction V

Tables

Table 1: Available service level measures 9
Table 2: Service charging-model 16
Table 3: Service change options 17

Figures

Figure 1: VAaaS architecture schematic 2
Figure 2: Stage 0-6 transition model 15

1 Service overview

Proact's Vulnerability Assessment as a Service (*VAaaS*) solution provides a vulnerability analysis service that enhances traditional options with specialist security analysis, advice and remediation recommendations, and robust *ITIL* ® based support and service management processes.

This comprehensive managed vulnerability assessment service not only provides reports on detected vulnerabilities, but also advice and remediation options from our team of security specialists who understand today's threat landscape and enterprise security best practices.

Proact VAaaS is available in the following feature-sets:

- *Scanning - Internal* – Detection and assessment of vulnerabilities present on internal systems via private IP addresses
- *Scanning - External* – Detection and assessment of vulnerabilities present on systems with public IP addresses
- *Intelligence* – A custom feed of the latest vulnerability intelligence including advisories and press releases compiled by the Proact Security Team tailored for the customer's specific technology stack.

Secure

- Scan data held in a secure ISO 27001[1] certified Proact datacentre
- All data is encrypted in transit
- All data remains within the Proact datacentre's national boundary, assuring data sovereignty
- End of term data handback or deletion policy

Available

- Highly-available storage capacity
- 24x7x365 infrastructure support from Proact Service Desk located in an ISO 27001[1] certified Proact Network Operation Centre (*NOC*)
- 24x7x365 Proact Service Desk monitoring the platform.

Flexible

Service can be comprised of any combination of feature-sets allowing the Customer to tailor the service to their needs, scanning Internal or External hosts.
An additional feature set, Intelligence, can be taken standalone or in combination with the Scanning feature sets.

In all scanning feature-sets the solution:

- Scans customer assets for vulnerabilities
- Provides actionable remediation advice and vulnerability analysis
- Provides access to a support portal for tracking discovered vulnerabilities
- Notifies the customer according to criticality and defined groups of scan targets

Proact perform vulnerability scans as defined by the customer's requested scan schedule. Requests to alter scan scheduling can be submitted through the Self-service support portal or direct to the Proact Service Desk.

What is the charging policy?

Costs for the scanning feature-sets (Internal and External) are per targeted IP address.

Costs for the Intelligence feature-set are per type of device or application.

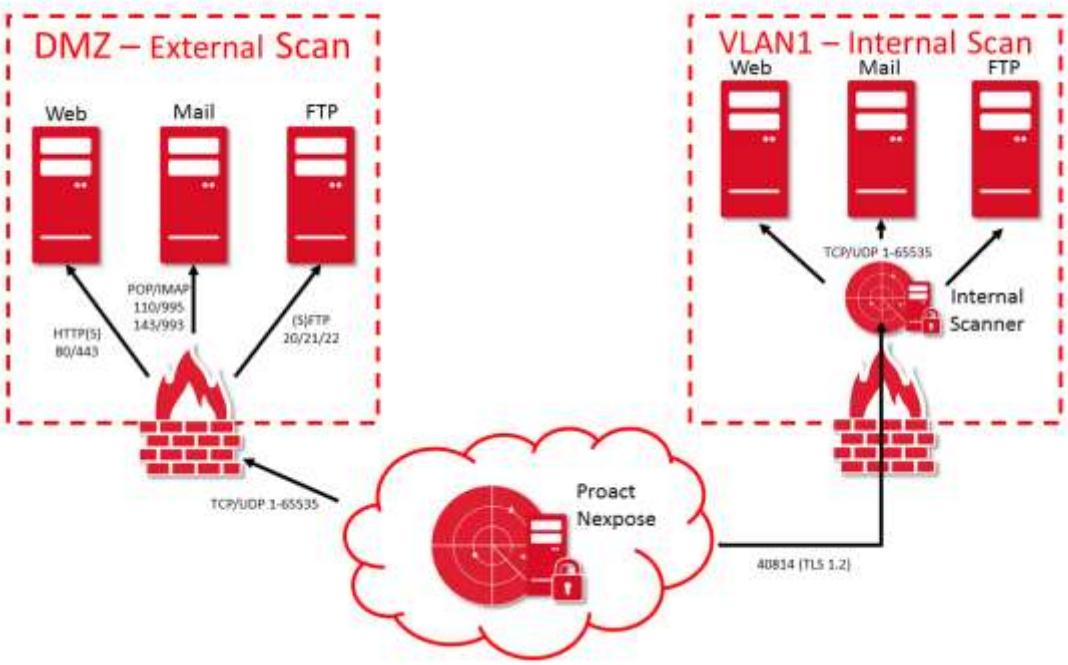
Vendor terms

This service is subject to vendor terms, which customers can view in full at these links:

http://www.proact.eu/terms/vendor

[1] ISO27001-certified Datacentres and *NOCs* are available in selected Proact delivery countries only

Figure 1: VAaaS architecture schematic



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
  - 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 10) for more detail on the components.

2.1 Service package

Objective	To provide a vulnerability assessment solution that enhances traditional options with inbuilt resilience and robust ITIL based support and management processes.
Hosted-in	A Proact datacentre on a secure multi-tenant platform. Proact's ISO 27001 certification assures security.
Supported vulnerability assessment targets	▪ Proact's vulnerability scanning service can target any internal or external system with a reachable IP address. This includes: ▪ Network devices ▪ Storage devices ▪ Physical or Virtual servers ▪ Hypervisors ▪ Web Applications
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 connectivity is by encrypted (TLS 1.2) public internet links using existing shared firewalls.
Engagement	▪ Use the Proact Self-service support portal to address detected vulnerabilities and enact remediation recommendations.
Complementary services	You can combine VAaaS with other Proact service offerings – Ch. 7 (on page 17) – such as Proact Security Information and Event Management as a Service (SIEMaaS) or Proact Infrastructure as a Service (IaaS)
	Service Feature Sets
Supported feature-sets	▪ Scanning – Internal ▪ Scanning – External ▪ Intelligence
Scanning feature-sets	▪ Scans customers assets for vulnerabilities ▪ Provides actionable remediation advice and vulnerability analysis
Scanning - Internal	▪ Vulnerability scans are performed from Scan Engine(s) hosted on the customer's internal network(s)
Scanning - External	▪ Vulnerability scans are performed from Scan Engine(s) hosted in Proact Datacentres as part of Proact's multi-tenant vulnerability assessment platform.
Intelligence	▪ Vulnerability advisories and vendor notifications are aggregated by Proact, and from this knowledge base Proact provides a bespoke vulnerability digest to the customer specifically tailored to the customer's requirements.
	Service capabilities

Scanning Schedule	▪ Proact offer flexible vulnerability scanning schedules, configurable per vulnerability scanning target, or groups of targets, to meet the customer's contracted requirements (within the operating parameters of the product). The default schedule is: ▪ Weekly Scan – a weekly full vulnerability scan.
Intelligence	▪ Proact provides bespoke vulnerability advisories to the customer specifically tailored to the customer's requirement. ▪ Vulnerability advisories and vendor notifications are aggregated by Proact, from this knowledge base Proact provides a bespoke vulnerability digest via the Self-service Support Portal to the customer specifically tailored to the customer's requirements.
Historic Scan Retention policy	▪ Proact configure and maintain a flexible retention policy configuration to meet the customer's contracted retention requirements (within the operating parameters of the product and consistent with the contract term). NOTE: The managed service contract only commits Proact to retaining vulnerability scan data in line with the policy configuration while the managed service contract is current and does not commit to retain the data after the contract ends. See also: Appendix C: Data retention, deletion and extraction (on page V) Exclusion 1: Retention of vulnerability scan data after the contract termination date

2.2 Service infrastructure

2.2.1 Service platform

Platform	▪ A secure multi-tenant platform ▪ Utilises proven Rapid7 Nexpose software
Compute	Compute resources are required in the form of: ▪ Local Scan Engine (Only where the *Scanning - Internal* feature-set is selected)
Software	▪ All vulnerability scanning operations are provided by the Rapid7 Nexpose software suite

2.2.2 Components

Local Scan Engine(s)	▪ Located on customer site running on a (usually virtual) server with the operating system provided and managed by the customer ▪ Only required if *Scanning – Internal* feature-set is selected. ▪ Contains local storage to run the required application software ▪ See: A.1: (on page II) for minimum specification
	Prerequisite 1: Provide Windows Server for Local Scan Engine Prerequisite 2: Deploy Local Scan Engine Software Responsibility 1: Maintain Operability of Local Scan Engine server(s) during contract
Remote Scan Engine(s)	▪ Performs scans of External assets. ▪ Located in a Proact datacentre
Nexpose MSSP Console Server	▪ Stores scan profiles, reports and templates ▪ Stores asset data, asset groups and scan schedules

2.2.3 Service connectivity

Connectivity options	▪ Scan data is transferred from the customer's site(s) to Proact datacentre(s) over encrypted (TLS 1.2) public internet links using Proact shared firewalls. ▪ Self-service support portal connections are over encrypted (TLS 1.2) public internet links.
Firewall	▪ All internet communication uses Proact's existing shared firewall infrastructure and either the customer's existing firewall or other shared or tenant firewall in a third-party or Public Cloud environment. ▪ For the *Internal* option TCP port 40814 out to Proact's Nexpose MSSP Console Server must be permitted from the Local Scan Engine. ▪ For the *External* option inbound traffic to external facing services to all assets in scope for external scanning must be allowed from Proact's Scan Engine(s)
	Prerequisite 3: Provide an administrator to assist with firewall configuration as necessary Prerequisite 4: Open required firewall ports Prerequisite 5: Notify Proact of the Local Scan Engine(s) Public IP address(es)
Bandwidth use	▪ Internet bandwidth is required for external scanning activities. This applies only where the *Scanning - External* feature-set is selected.
	NOTE: Proact endeavour to minimise potential monopolisation of bandwidth by spreading scanning activities and scheduled scans over customer-defined periods of time
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 6: Provide remote access for Proact configuration and support tasks Exclusion 2: All configuration shall be performed by Proact remotely Responsibility 2: 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 3: 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. ▪ Proact do not provide antivirus protection for the Local Scan Engine, and we recommend that the customer deploy their own antivirus protection to the local vault server where the *Scanning – Internal* feature-set is selected.
Patching	▪ Proact patch and update all infrastructure software, firmware and hardware under their management in order to minimise security vulnerabilities. ▪ The customer is responsible for patching the OS of Local Scan Engine(s) when the Scanning – Internal feature-set is selected.
	Responsibility 4: OS patching of Local Scan Engine(s)
Data storage	▪ Secure HTTPS/TLS encryption is applied to all data connections between Proact and their customers ▪ In all architecture models, scan data is stored in an access controlled database on our central vulnerability console, which is situated in a trusted internal network at a secure ISO 27001[2] certified Proact datacentre.
Audit capability	▪ Proact provide regular reports confirming the status of vulnerability scans, which together form an audit trail of job success or failure. ▪ The Rapid7 Nexpose software itself has an inventory of every asset scanned, which is accessible by Proact Security Team operatives.

2.2.5 Applications and licensing

Vulnerability Scanning Licensing	Proact provide all scan licenses for each host in scope. Proact provide licenses for all vulnerability scanning software.
Scan Engine Servers	The customer must provide appropriate operating system licensing for all Local Scan Engine servers (if the *Scanning – Internal* feature-set is selected).

[2] ISO27001-certified Datacentres and *NOCs* are available in selected Proact delivery countries only

2.3 Supporting services

Monitoring	▪ The *Proact Monitoring platform* monitors the service infrastructure and the status of Vulnerability Assessment related tasks. Its near-real-time monitoring raises alerts (for example on an unexpected service stop), which are forwarded to the Proact Service Desk. ▪ Monitored items include the Nexpose MSSP Console Server and Proact-hosted Scan Engines, to identify whether an issue requiring an alert has occurred. ▪ Proact monitor the scan targets (that is, the servers, and applications being scanned) ONLY where the customer has separately contracted cover e.g. through *Proact Premium Support Plus* or *Proact Service Management.*
Proact Service desk	▪ Provides support and management of the service and supporting infrastructure 24x7x365 – see Service infrastructure (Section 2.2, on page 5on 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 schedules).
Proact Self-service support portal	Proact provides customer-nominated administrators with access to a Self-service support portal through which they can: ▪ Request changes to scanned assets and scheduling ▪ 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.

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	▪ VAaaS

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 threshold 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 if assistance is required.
	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 issues.
	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 3: 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.

4.3 Operational Activities

Deliverable	Frequency	Description and content summary
Vulnerability Assessment Review	Weekly	Feature-set(s): All Scanning feature-sets Proact's security specialists review the vulnerability scan results (Mon-Fri, excl. bank holidays) and produce actionable remediation advice in the form of incidents on the Self-service support portal. The customer may select the minimum vulnerability score (CVSS) for which incidents created will trigger a notification to the defined customer contacts. Incidents created for vulnerabilities detected that are lower than this agreed threshold will be accessible via the self-service support portal but will not trigger notifications.
Vulnerability Intelligence Review	Daily	Feature-set(s): Intelligence Proact's security specialists conduct daily (Mon-Fri, excl. bank holidays) review of the latest vulnerability intelligence. Any new vulnerability intelligence applicable to the customer's selected items in the *Intelligence* feature-set is published in the Self-service support portal and notified to the customer by email.

Deliverable	Frequency	Description and content summary
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 5: Provide at least 24-hours' notice of planned maintenance
Change Management	Continuous	All changes to the customer's scanning profile or policy configuration are planned and implemented according to the Proact Change Management processes ▪ The customer may use the Self-service support portal to request changes to scan policy, timing, or targets.
Local Scan Engine Installation	As required	Proact perform the installation of Scan Engine(s) (where the *Scanning – Internal* feature-set is selected) remotely to ensure that they are configured correctly with the shared infrastructure. The customer will need to be available to provide a server account with elevated privileges as part of the installation. Proact will perform the client installation of new Scan Engine(s) remotely where: ▪ The software vendor supports remote deployment ▪ A working remote deployment method exists Responsibility 6: Assist in installation of Scan Engine(s) 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.

Deliverable	Frequency	Description and content summary
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.
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
Vulnerability Assessment And Intelligence Dashboard	Ongoing	The self-service portal will feature a dashboard in which the customer can view outstanding incidents relating to detected vulnerabilities that require resolution.
Service Review Report (SR)	Quarterly	A quarterly Service Review Report showing vulnerability statistics and information, where the relevant feature-sets have been selected, for example: ▪ Vulnerabilities by asset ▪ Vulnerability scan status ▪ Vulnerability scan detections and recommendations ▪ Incident response times ▪ Incident by category ▪ Incident logged by method ▪ Incident and change log **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 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. ▪ A review of system capacity growth, performance, risks and other technical observations and recommendations.
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 8 (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 applications or systems that utilise the infrastructure to be managed by Proact ▪ Technical owners for any supporting infrastructure needed to allow Proact to access and monitor the in-scope CIs (for example, network engineers, for creating VPNs and 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 7: Provide appropriate customer representation at transition workshops Responsibility 7: Provide appropriate representation at project closedown workshop
Data migration	Migration of workloads and datasets from legacy systems to systems under Proact service management is not included in this service – see Additional services (Ch. 7, on page 17)
	Exclusion 4: Data migration is excluded from the scope of service transition
Training sessions	▪ 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

Charging basis	▪ Set-up charge according to the types, sizes and configuration of the CIs selected by the customer to be protected.
	▪ Minimum commit and Flexible charge according to the types, sizes, configuration and location of the CIs selected by the customer to be protected. For example, the quantity of
	  ▪ Internal IP addresses
	  ▪ Internal Scan Engines to be deployed
	  ▪ External IP addresses
	  ▪ Device types or Applications

Minimum commitment	▪ Charge based on 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

7 Additional services

Customers should contact their Proact Account Manager to discuss the available options, some of which are shown Table 3 (below).

Table 3: Service change options

Service change	▪ Adding new features or services requires updating the service design and-or architecture, unless otherwise specified in this document. Proact can perform this on a separately chargeable consultancy basis.
Service upgrade	Service review upgrade – A quarterly remote service review meeting is included as standard. It can be upgraded to monthly and-or delivered onsite instead of via teleconference at additional cost.
Bespoke services	Proact Professional Services can be engaged to assist with a range of bespoke services including, but not limited to: ▪ Migration of workloads, datasets and monitoring and vulnerability scanning configurations from legacy systems to systems under Proact service management ▪ Out of scope support – Proact can provide support and professional services for out of scope equipment ▪ Service transfer and end-of-life – Any bespoke activities required by the customer outside of the ***Service Transfer Plan*** can be provided using Proact Professional Services – See also: ***Proact Service Transfer Policy***

Complementary services	Proact provides a range of services complementary to BaaS, including, but not limited to:
	▪ Monitoring, Support and Service management
	  ▪ Proact Premium Support Plus
	  ▪ Proact Service Management
	▪ A range of vSOC services to complement VAaaS including
	  ▪ SIEMaaS (Security Information and Event Management)
	  ▪ NLDaaS (Network Layer Defense)

8 Service demarcation

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

Prerequisites	Prerequisite 1: Provide Windows Server for Local Scan Engine .....5 Prerequisite 2: Deploy Local Scan Engine Software.....5 Prerequisite 3: Provide an administrator to assist with firewall configuration as necessary .....5 Prerequisite 4: Open required firewall ports.....5 Prerequisite 5: Notify Proact of the Local Scan Engine(s) Public IP address(es).....5 Prerequisite 6: Provide remote access for Proact configuration and support tasks ...5 Prerequisite 7: Provide appropriate customer representation at transition workshops 15
Responsibilities	Responsibility 1: Maintain Operability of Local Scan Engine server(s) during contract .....5 Responsibility 2: Maintain sufficient network capacity for service operation.....5 Responsibility 3: Maintain compatibility of interacting external systems or environments at all times.....6 Responsibility 4: OS patching of Local Scan Engine(s) .....7 Responsibility 5: Provide at least 24-hours' notice of planned maintenance.....12 Responsibility 6: Assist in installation of Scan Engine(s) by providing elevated privileges.....12 Responsibility 7: Provide appropriate representation at project closedown workshop 15
Exclusions	Exclusion 1: Retention of vulnerability scan data after the contract termination date.4 Exclusion 2: All configuration shall be performed by Proact remotely .....5 Exclusion 3: Unauthorised use of the Proact Self-service support portal and-or Service Desk.....11 Exclusion 4: Data migration is excluded from the scope of service transition .....15 Exclusion 5: Scan data is not retained beyond the contract end date V

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
Scan Engine		A component of the vulnerability scanning solution that conducts the vulnerability scans.

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.
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.
Vulnerability		A weakness which could allow an attacker to reduce the information assurance of a system

Appendices

Appendix A: Technical Requirements ..... **II**

Appendix B: Self-service support portal ..... **IV**

Appendix C: Data retention, deletion and extraction ..... **V**

Appendix A: Technical Requirements

A.1: Minimum server specifications

A.1.1: Local Scan Engine

For *Scanning - Internal* solutions, a dedicated server (preferably virtual) running Microsoft Windows Server is required to run each Local Scan Engine, which:

- Provides a point from which vulnerabilities scans can be carried out against internal assets
- Communicates scan results back to Proact's central VA platform

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:

- 4x (v)CPU
- 8GB RAM
- 1 x (v)NIC assigned a Static IP address
- Minimum 100GB Disk

The supported Operating Systems are as follows:

- Ubuntu 16.04 LTS (Recommended)
- Ubuntu 14.04 LTS
- Red Hat Enterprise Linux Server 6
- Red Hat Enterprise Linux Server 7
- Windows Server 2008 or later (full installation)

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 number of in-scope endpoints.

A.2: Firewall Ports

A.2.1: Ports required for Scanning

The following firewall rules must be implemented where in-scope endpoints reside in different security zones from the Local Scan Engine 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 Local Scan Engine without going through a firewall.

Client	Client Port	Server	Server Port(s)	Protocol	Communications
Local Scan Engine	Any	Local Vulnerability Scan Target	1-65535	TCP + UDP	Unidirectional

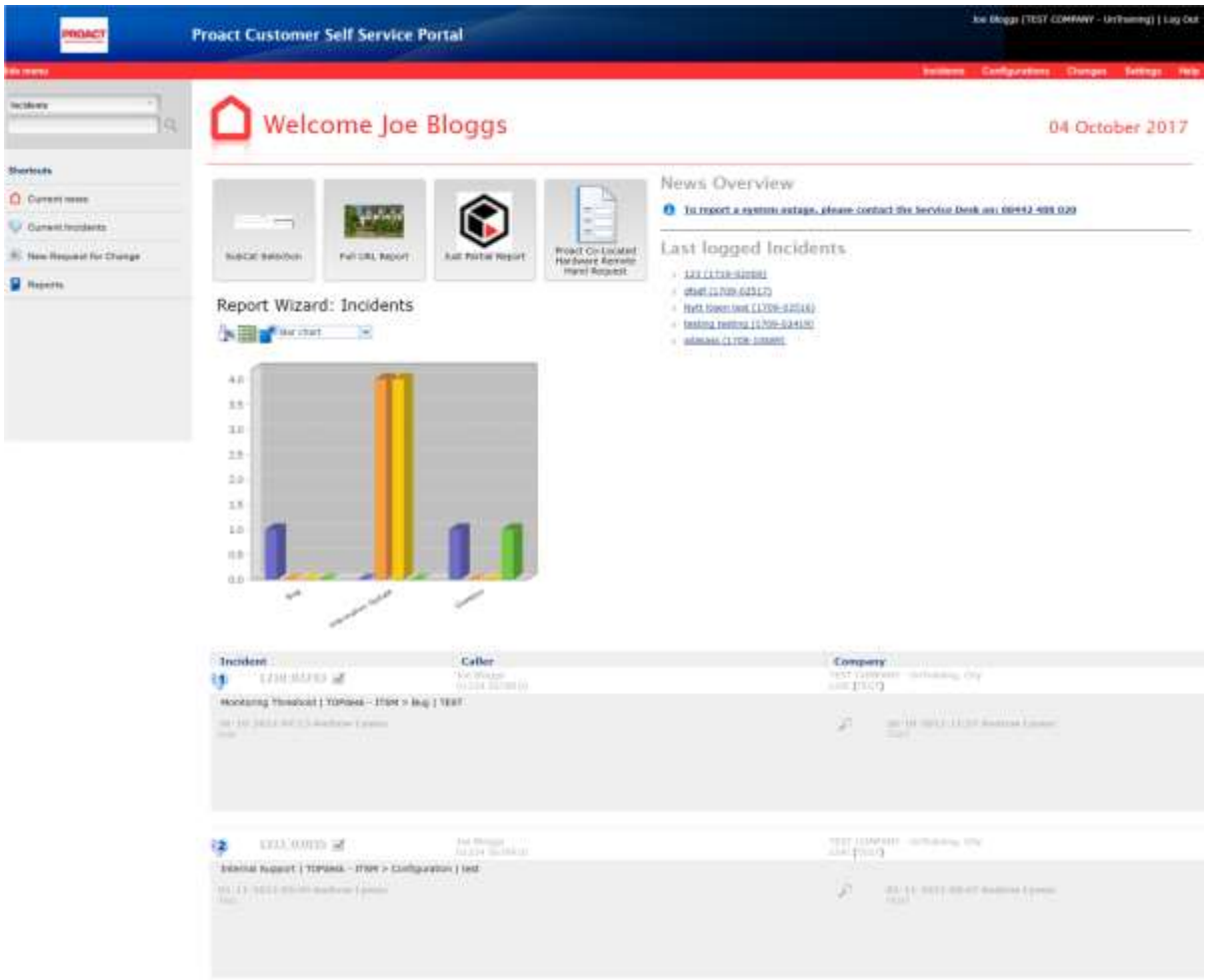
A.2.2: Ports required for VAaaS Master Service

Each Local Scan Engine will communicate with Proact's central VA platform. The following traffic must be allowed through Customer firewall(s) and the Customer must inform Proact of the source Public IP from which this traffic will originate:

Client	Client Port	Server	Server Port(s)	Protocol	Communications
Proact Central VA Platform	Random	Local Scan Engine	40814	TCP	Unidirectional

Appendix B: Self-service support portal

The service includes access to a self-service support portal that can be used to view vulnerability assessment incidents and intelligence knowledge base articles that have been raised in relation to the customer's assets.



The functionality of the portal includes:

- Case management
  - Incidents for vulnerabilities detected (where a *Scanning* feature-set is selected)
  - Incidents raised by the customer for advice in relation to intelligence advisories (where the *Intelligence* feature-set is selected)
- Reporting
  - Outstanding vulnerabilities (where a *Scanning* feature-set is selected)
  - Highest priority vulnerabilities (where a *Scanning* feature-set is selected)
  - Relevant intelligence advisories (where the *Intelligence* feature-set is selected)

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, with the operating parameters of the VAaaS product.

Proact's default policy is to retain all vulnerability scan data and only remove vulnerability scan data upon written customer request or following service termination; no automatic removal process is scheduled.

C.1.2: Data Deletion

Proact will only retain scan data in line with the agreed VAaaS configuration policy during the term of the 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 scan data from the VA platform, in which case Proact will:
  - Remove the customer silo to prevent additional scan data from being collected
  - Inform the customer that all the scan data has been deleted.
- Request that Proact extract and return vulnerability scan data from the VA platform storage (see Section C.1.3:)

By default, Proact will, irrespective of the retention policy, delete the vulnerability scan 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: Scan data is not retained beyond the contract end date

C.1.3: Data Extraction

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

- Export the vulnerability scan data into Nexpose backup format and provide it to the customer via email in an encrypted zip file.