

PROACT

G-Cloud 15

Vulnerability Assessment and
Intelligence Services as a
Service (VAaaS)

Document control

Document type	Public - Freely Distributable		
Company	Proact IT UK		
Address	Proact IT UK Grayson House, Venture Way, Chesterfield, Derbyshire, S41 8NE		
Telephone	01246 266 300		
Primary contact	bids@proact.oc.uk	Role	N/A

Revision history

Issue date	Author	Version	Revision description
08/12/2025	Colin Abram	V1	Document Upload



Vulnerability Assessment and Intelligence Services as a Service (VAaaS)

Proact's Vulnerability Assessment as a Service (VAaaS) 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.

The deliverables of the VAaaS service are as follows:

- 24x7 virtual SOC capability via Proact's cyber security analysts
- Provision of Vulnerability Assessment software from Proact's data centre including the infrastructure and management of the underlying platform
- Confidentiality of data through encrypted TLS 1.2 connection
- Detailed monthly and quarterly reports ensuring easy forensic analysis
- Dedicated security operations staff
- Investigation and advise with identified vulnerabilities
- Self-service support and management portals
- A named Service delivery manager to co-ordinate delivery and provide regular customer reports

This document contains the following appendix detailing the service definitions for Proact Vulnerability Assessment as a Service (VAaaS):

- [Appendix 1 – Vulnerability Assessment as a Service](#)



Appendix 1 - Vulnerability Assessment as a Service – Service Definition

1.1 - Service Overview

Proact's Vulnerability as a Service solution provides a vulnerability analysis service to improve customers' security awareness around their infrastructure and application environments.

This service provides reports on detected vulnerabilities, and advice and remediation options from our team of security specialists.

Proact perform vulnerability scans as defined by the customer's requested scan schedule.

Proact VAaaS supports scanning of the following systems:

- *Internal* IP addresses - Detection and assessment of vulnerabilities on internal systems via private IP addresses
- *External* IP addresses - Detection and assessment of vulnerabilities public/Internet facing IP addresses

The service provides the following deliverables:

- Scans customer IP assets for vulnerabilities
- Provides actionable remediation advice and vulnerability analysis

See the glossary for the definition of acronyms used.

General Service Deliverables

Proact shall:

- Provide a service desk and customer support portal to report and update incidents, change requests and escalations.
- Provide service delivery management.
- Maintain documentation of the service configuration.
- Maintain a CMDB listing for all CIs.
- Coordinate any product vendor involvement necessary.
- Respond to reasonable service requests for relevant information and advice.
- Provide a change advisory board to review normal, standard, and emergency change requests.
- Subject to agreement, join the Customer's change advisory board, for relevant changes.
- Implement agreed changes to CIs.
- Provide reasonable problem management.
- Provide incident trend analysis.

The Customer shall:

- Maintain compatibility with Proact-managed systems/applications at the hardware, OS, and application level.
- Log incidents via the portal, telephone, or email. Priority one incidents must be logged by telephone.
- Assist with any systems or applications not under Proact's management.
- Respond to requests for information/actions within five working days. Inactive incidents may be closed.
- Resolve health issues on customer-managed systems.
- Nominate named individuals to engage with Proact on the approval and timing of changes

Vulnerability Assessment as a Service

Proact shall:

- Provide the VAaaS platform including licensing
- Manage the VAaaS platform and receive scan data from CIs based on Proact defined schedule.
- Provide on demand scanning when requested
- Interact with the VAaaS platform via the provided portals and APIs.
- Provide near real time monitoring of the scan data through the VAaaS platform and report on identified CI vulnerabilities.
- Utilise provided scan engines for VAaaS platform data scanning, where required.

- Update provided scan engines on a schedule defined by Proact.
- Respond to and investigate alerts/incidents issued by the VAaaS platform.
- Where appropriate, the Proact SOC will raise a security incident and provide guidance on resolution and future prevention.
- Issue a P1 security incident where there is an immediate and uncontained threat. Assign an Incident Manager to direct activity and communicate with key Customer stake holders.
- Issue a P2 security incident where there is a severe threat to business data. Proact's security team will contact the Customer's security contact(s) with incident details and advice on resolution.
- Issue a P3 security incident where access to business data is potentially at risk. Proact's security team will contact the Customer's security contact(s) with incident details and advice on resolution.
- Provide a service review report.
- Organise a quarterly service review meeting.

The Customer shall:

- Open internal firewall ports to allow access to VAaaS platform.
- Deploy scan engines at Proact's request including providing sufficient server resources.
- Provide and manage servers required to host the scan engines.
- Ensure the scan engines are available.
- Request on demand scanning.
- Provide 'Service Accounts' and passwords/keys with privileges to allow scanning.
- Provide sufficient compute, network, and storage resource to allow for efficient data collection.
- Provide sufficient network bandwidth between the CIs and the VAaaS platform.
- Implement Proact's recommendations to vulnerabilities.
- Be responsible for any public cloud egress charges for scan and data transfer tasks.
- Define their minimum vulnerability score which will determine the threshold for which Proact will vulnerability notifications.
- Nominate security contact(s) and contact details to be informed when handling incidents.
- Act upon Proact's advice/guidance regarding alert/incident prevention.

1.1 - Service Level Agreement

1.1.1 - Response Time Service Levels

Response	Proact is deemed to have 'responded' when a case is created in Proact's customer support portal and a case number is allocated.
Initiation	A change is initiated at the point at which (as recorded in the support system) Proact commences implementation of the change.
Response Time SLA - P1 Incident	Proact will use its reasonable endeavours to respond to priority 1 (P1) incidents within 30 minutes. A P1 incident is: (i) a reasonable request by the Customer, which will be logged by phone (not email), for support or information in connection with the services, in circumstances in which the service(s) are completely unavailable or are imminently expected to be completely unavailable; or (ii) an alert received by Proact directly from its monitoring platform in connection with the services, that the service(s) are completely unavailable or are imminently expected to be completely unavailable; or have breached defined critical monitoring thresholds; or (iii) an incident logged by Proact in relation to an imminent and serious threat to the service(s). If Proact fails to respond to a P1 incident within 30 minutes the Customer will be entitled to a Service Credit of 15% of the monthly minimum service Charges.

Response Time SLA - P2 Incident	Proact will use its reasonable endeavours to respond to priority 2 (P2) incidents within 1 working hour. A P2 incident is a reasonable request by the Customer for support or information, or an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning such that the service is significantly impacted but remains operational or have breached defined major monitoring thresholds. If Proact fails to respond to a P2 incident within 1 working hour the Customer will be entitled to a Service Credit of 5% of the monthly minimum service Charges.
Response Time SLO - P3 Incident	Proact will use its reasonable endeavours to respond to priority 3 (P3) incidents within 4 working hours. A P3 incident is a reasonable request by the Customer for support or information, or an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning but with no significant impact on service or have breached defined minor monitoring thresholds.
Response Time SLO - P4 Incident	Proact will use its reasonable endeavours to respond to priority 4 (P4) incidents within 8 working hours. A P4 incident is a reasonable request by the Customer for support or information, in connection with the services, in circumstances in which there is no specific malfunction.
Service Credit Limits	A Service Credit is not a refund, cannot be exchanged into a cash amount and is capped at a maximum of 50% of the monthly minimum charges for the relevant service. A Service Credit is the sole and exclusive remedy for any failure by Proact to meet its obligations under the SLA.
Response Time SLO – Standard Change Request	Proact will use its reasonable endeavours to initiate standard changes within 8 working hours from when authorised. A ‘Standard’ change is any pre-authorised change that is low risk, relatively common and follows a predefined procedure or work instruction. Proact’s change advisory board (CAB) is not required to approve ‘Standard’ changes prior to implementation.
Response Time SLO – Normal Change Request	Proact will use its reasonable endeavours to initiate normal changes within 8 working hours from when authorised. A ‘Normal’ change is any change that is not a ‘Standard’ change according to the above definition and is not an emergency. An agreed ad-hoc change to the configuration of the services. The CAB must authorise ‘Normal’ changes and approve an implementation plan.
Response Time SLA – Emergency Change Request	Proact will use its reasonable endeavours to initiate required emergency changes within 4 hours from when authorised. An ‘Emergency’ change is any ‘Normal’ change that requires an expedited timeframe to resolve a P1 incident causing significant impact to the services in scope, and which cannot wait for review and approval from the CAB. Where there is not an active P1 incident, the change shall not be classified as ‘Emergency’. Proact’s Emergency Change Advisory Board (E-CAB) must authorise ‘Emergency’ changes and approve an implementation plan. If Proact fails to respond to an Emergency Change Request within 4 hours, then the Customer will be entitled to a Service Credit of 15% of the monthly minimum service Charges.
Response Time SLO – Service Request	Proact will use its reasonable endeavours to initiate service requests within 8 working hours.



	A 'Service request' is a reasonable request by the Customer for activity or information, in connection with the services, that is neither an incident nor a change and follows a predefined procedure or work instruction. A common example of a Service Request is a password reset.
Working hours for Changes	All Standard changes and Normal changes shall be scheduled by Proact and will be carried out during local business hours except where a change is requested by Proact and is expected by Proact (upon evaluation by the Proact CAB) to have a significant impact on availability or performance of the services in scope. The Customer may request that any particular change is implemented at a specific time, including outside local business hours, but, if such request is accepted by Proact, additional charges shall apply as agreed in advance between Proact and the Customer. 'Emergency' changes are implemented 24/7 and are not subject to additional charges.

1.2 - Vendor Terms

In addition to the terms and conditions set out in this Managed Service Agreement the Customer shall be subject to the relevant vendor terms set out at <https://www.proact.eu/en/about-us/terms-and-conditions/vendor-terms/>.

Outpost 24

1.3 - Glossary

Term	Definition
Configuration Item (CI)	A term used for a component which is within the scope of the Contract. The CIs will be the <define what the CIs are in this service> set out in the Contract.
VAaaS Application	A public cloud hosted secure multi-tenant vulnerability testing platform hosted, for the scanning and consolidation of vulnerability data. Scans performed by the platform will be analysed and reported.