PROACT

G-Cloud 15

Proact Storage Detection and Response Service Definition

PROACT

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
04/12/2025	Colin Abram	V1	Document Upload

Proact Storage Detection and Response Service Definition

Proact's Storage Detection and Response (SDR) is a service designed to enhance Customers' security awareness and improve their protection, detection, and response capabilities by analysing, triaging and responding to alarms and actions executed by the NetApp Autonomous Ransomware Protection (ARP).

- Management and monitoring of the NetApp Autonomous Ransomware Protection (ARP) feature
- Incident handling and reporting of the ARP alarms, response and remediation to blocking or locking actions
- 24x7x365 Response by Proact's Security Operations Centre
- Routine tabletop testing to rehearse and prepare for cyber attacks
- Change and configuration management.

This document contains the following appendix detailing the service definition for Storage Detection and Response (SDR):

PROACT

Appendix 1 – Storage Detection and Response Service Definition

1.1 - Service Overview

Proact's Storage Detection and Response (SDR) is a service designed to enhance Customers' security awareness and improve their; protection, detection, and response capabilities by analysing, triaging and responding to alarms and actions executed by the NetApp ARP (Autonomous Ransomware Protection).

General Service Deliverables
Proact shall: • Provide a service desk and customer support portal to report and update incidents, change requests and escalations. • Provide a Service Platform. • Provide service delivery management. • Maintain documentation of the service configuration. • Maintain a CMDB listing for all CIs. • Respond to Service Platform alerts and events and notify the Customer of relevant incidents. • Coordinate any product vendor involvement necessary. • Take appropriate action to restore operation of the Service Platform in case of outage. • Provide a major incident report, where required. • 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. • Respond to reasonable service requests for relevant information and advice. • 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.
The following elements are out of scope of the service: • Upgrades or enabling of new features on the Service Platform. Proact may upgrade the platform at its sole discretion.

Storage Detection & Response
Proact shall: • Provide the SIEM platform within Proact's datacentres. • Take appropriate action to restore operation of the SIEM platform in case of outage. • Provide a tenancy within the platform, dedicated to the Customer. • Keep a short-term audit log of administration actions undertaken on the platform. • Provide all SIEM agent software and licenses required to monitor the CIs in scope. • Encrypt SIEM data both at-rest and in-flight. • Provide access to the service via the internet, through a secure firewall. • Provide internet bandwidth for the transfer of service traffic. • Attend a consultative technical security review with the Customer on a quarterly basis. • If requested, assist the Customer with an annual tabletop exercise simulating a security incident.
The Customer shall: • Nominate security contact(s) and contact details to be informed when handling incidents. • Provide service accounts and passwords/keys with privileges to allow log data collection. • Provide and manage servers/cloud instances required to host agent software.

• Deploy agent software at Proact's request. • Open internal firewall ports to allow access to the CIs/agent software in scope. • Provide sufficient internet bandwidth for the transfer of service traffic. • Provide a network administrator to configure and troubleshoot service traffic. • Provide and manage servers/cloud instances required to host agent software. • Provide sufficient compute, network and storage resource to allow for efficient data collection. • Inform Proact of planned maintenance or other operations that may impact the service.
The following elements are out of scope of the service: • Upgrades or enabling of new features on the SIEM platform. Proact may upgrade the platform at its sole discretion.

Array
Proact shall: • Manage the ARP feature on the Customer's NAS Controller and receive telemetry and log data from CIs. • Configure ARP and commence monitoring on the required CIFS volumes. • Work with the Customer to agree pre-defined 'playbook' actions to apply during ARP generated incidents. • Respond to and investigate alerts/incidents issued by ARP to triage risk exposure.
The Customer shall: • Ensure that all NetApp CIs in scope support the ARP functionality. • Inform Proact of changes to NetApp CIs that require protection. • Define the CIFS volumes that ARP should consider 'in-scope' or 'excluded'. • Work with Proact to agree pre-defined 'playbook' actions to apply during ARP generated incidents.
The following elements are out of scope of the service: • ARP protection on non-CIFS volumes or file systems presented to a hypervisor.

Domain Controller
Proact shall: • Provide near real time monitoring and SIEM data for the CIs in scope. • Utilise common data connectors for SIEM data collection, where required. • Where ARP identifies suspicious activity, execute workflows to disable suspected users in the AD environment. • Inform the Customer of user accounts that are disabled due to suspicious activity. • Where appropriate, the SOC will raise a security incident and provide guidance on resolution and future prevention. • Tune alerts received to minimise the number of false positives.
The Customer shall: • Nominate security contact(s) to be informed when handling incidents. • Ensure NAS controllers are limited to AD DCs that are both CIs and local to their respective controllers. • Work with Proact to tune alerts and settings to minimise false positives. • Investigate disabled user accounts suspected of malicious activity. • Act upon Proact's advice/guidance regarding alert/incident prevention.

1.2 - Service Level Agreement

1.2.1 - 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.

1.3 - 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/.

Vendor Name
NetApp

1.4 - Glossary

Glossary Term	Definition
Configuration Item (CI)	A term used for a component which is within the scope of the Contract and stored within the Configuration Management Database (CMDB). The CIs will be NAS Controllers and AD Domain Controllers monitored by the service, as set out in the Contract.
Service Platform	Depending on the service, Proact will provide monitoring and/or management platforms to enable delivery of the service. These Service Platforms are managed by Proact.
Autonomous Ransomware Protection (ARP)	NetApp's Autonomous Ransomware Protection (ARP) is an AI-powered storage feature that detects and mitigates ransomware attacks by identifying suspicious file activity, creating recovery snapshots, and triggering alerts.