Service Definition Document

Mangaged Security and Incident Event Management (SIEM)

G-Cloud 15 - Lot 3

+44 (0) 845 565 2097
info@celerity-uk.com
celerity-uk.com

Head Office:
11 St. George's Court
Kirkham, Preston
PR4 2EF

Crown Commercial Service Supplier

celerity

Contents

Crown Commercial Service Supplier

celerity

G-Cloud Service Reference Number

Celerity reference: GC 15 03 02

G-Cloud Lot/s

This service is offered under G-Cloud 15 Lot 3

Security Operations Centre (SOC): Service Description

It is a fact, that the quicker a cyber-attack is identified the more damage costs are reduced. With the average cyber-criminal now spending 197 days inside a network before being discovered, it is critical for organisations to detect cyber threats as soon as possible by using the core component of Celerity Managed Security Information Event Management (SIEM).

Managed Security Information Event Management allows you to achieve a real-time view of internal and external threats to your network through consolidated threat information and intelligence enabling identification of an attack. Not only does it detect an external attack on your organisation, but it also identifies internal threats to your business by addressing unauthorised or unsanctioned user behaviour. By helping you to gain better insight, it allows you to make better decisions and thus respond faster to advanced threats.

The service comprises:

- Manage the day-to-day operation of the SIEM platform
- 24/7 monitoring of logs from firewalls, servers, endpoints, databases, and cloud services
- Real-time threat detection and alerting
- Advanced analytics using AI/ML, collecting and analysing data from multiple sources to detect patterns and identify hidden threats
- Incident triage and escalation
- Monthly reporting and dashboards
- Compliance support (e.g., ISO 27001, PCI DSS, GDPR)
- Continuous tuning of detection rules and playbooks
- Incident reports provided with key findings and remediations to allow resolution by the Client
- Provide monthly service reviews
- Provide reports for management reporting and compliance requirements

Underlying Technology

Managed SIEM is based on industry-leading technology which helps security teams accurately detect and prioritize threats across the enterprise, and it provides intelligent insights that enable teams to respond quickly to reduce the impact of incidents. By consolidating log events and network flow data from thousands of devices, endpoints and applications distributed throughout your network, Managed SIEM correlates all this different information and aggregates related events into single alerts to accelerate incident analysis and remediation.

Key Features

- Ingests vast amounts of data from on-premise and cloud sources
- Applies built-in analytics to accurately detect threats
- Correlate related activities to prioritise incidents
- Automatically parses and normalises logs
- Threat intelligence and support for STIX/TAXII
- Integrates out-of-the-box with 450+ security solutions
- Highly scalable, self-tuning and self-managing database
- User Behaviour analytics analyses user activity to detect malicious insiders and determine if a user's credentials have been compromised.

The first step in security analytics is collecting the right data. To gain visibility into the different pillars of enterprise IT environments, Managed SIEM ingests data from a broad set of information sources. Most of these data sources are readily available, and each offers unique insight. For instance:

Network data produced by firewalls, gateways, routers or through sensors can deliver a broad view of communication flows inbound, outbound and within the enterprise environment. This data shows who is talking to whom, how and when.

Endpoint data is typically generated by operating systems and provides deep insights into individual system activity, processes, configuration changes, running applications and individual user interactions on a system. This information is excellent for monitoring, tracking and auditing system or user activity. It also allows security analysts to detect suspicious processes and execute deep forensics once a compromise has been discovered.

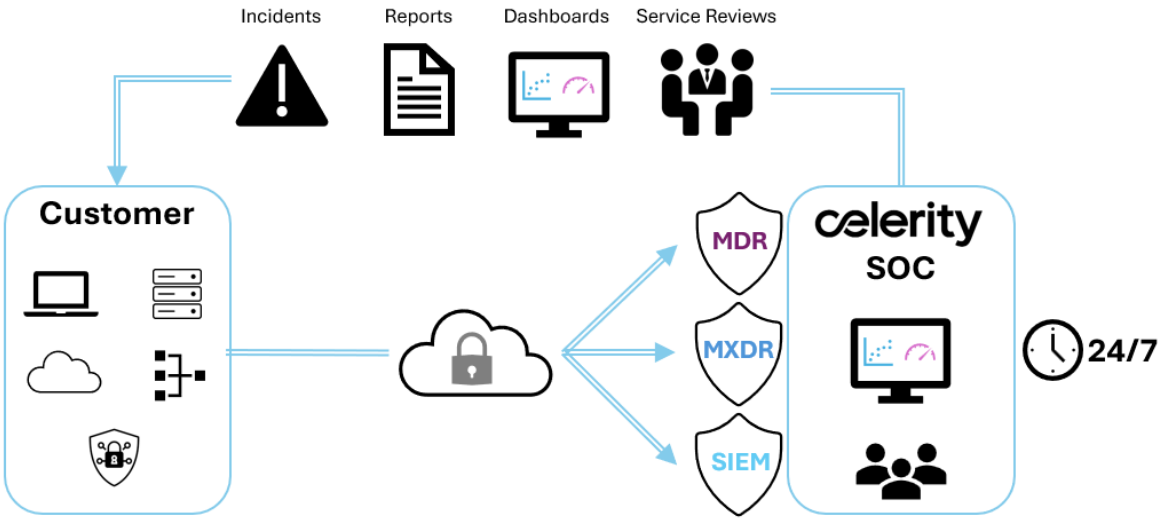
Cloud data produced by IaaS or SaaS providers allows security and cloud teams to monitor and retain all activity across their cloud infrastructures.

User and identity data ingested from Active Directory, LDAP or other identity and access management (IAM) solutions provide a contextual understanding of the person or resource behind a logon ID.

Application data can help expose fraud or advanced attacks by providing insights into what is happening on a system beyond access and authentication activity.

Security data typically originates from specific security controls such as antivirus tools, vulnerability scanners, intrusion detection systems, malware sandboxing solutions or data loss prevention systems. Output from these systems informs the security team when specific security policies have been violated, potentially indicating a threat is eminent.

Threat intelligence, often consumed by analysts through external feeds, offers insights into known threat actors, tactics, techniques and procedures (TTPs), malicious assets (IP, URL and FQDN) and even goals. These Indicators of Compromise (IOCs) help security analysts identify and understand their adversary so they can make more informed decisions and take quick, decisive action to better protect the organization.



Operational Support

The Celerity Service Desk (CSD) will be the customer's point of contact for all aspects of the service.

The CSD operates to ITIL3 standards and is managed by staff with extensive experience in delivering managed IT and data protection services.

Celerity utilises a modern IT Service Management System (ITSMS) which is at the centre of our Service Desk operations. The customer will be allocated accounts on our ITSMS portal. Via the portal users can:

1. Log service requests
2. View the status of service tickets
3. Run standard reports
4. Access contract / SLA information

You may also log service requests by telephone.

An escalation procedure will be incorporated into the SLA agreed between the customer and Celerity.

This will clearly state the contact points, names and positions of staff from both the customer and Celerity, and the points during an incident when they will be involved.

Customer Success Manager

The Customer Success Manager ensures that Celerity customers have a positive and fruitful experience with our products/services. They build a solid and trusting connection with our clients, knowing their goals, and helping them achieve them with our solutions.

They provide regular reporting to the specific needs and goals of each customer, acting as champions for customers within Celerity. They collect feedback and insights from

customers during monthly meetings and share this information with relevant internal teams to drive product enhancements and improvements that better meet our customer's needs. Overall, the role of a Customer Success Manager shows the company's devotion to the success and satisfaction of our customers, ultimately leading to mutual benefit and long-term partnerships.

Customer Account Manager

You will also have a Customer Account Manager who will help you take advantage of the services that Celerity provides. The CAM is the main contact person for the customer. They will collaborate with you to understand your business objectives, challenges, and IT requirements. This includes having regular consultations, gathering feedback, and staying updated with your evolving needs. The CAM works with the Customer Success Manager to evaluate how well the services are doing and to make sure your concerns and needs are addressed and managed. The CAM also collaborates with technical teams in Celerity to fix issues fast and to minimise any disruption to your workflow. They keep you informed regularly and maintain transparency throughout. The CAM's role is to be a trustworthy consultant, offering strategic advice and providing useful services that assist your business in reaching its objectives.

Reporting

Celerity considers detailed reporting as a crucial component of managed service contracts. The data gathered under such contracts is essential to our philosophy of ongoing enhancement and providing value through expert account management. We do this by taking a pro-active approach, and we follow the Kaizen methodology. Celerity will produce reports every month and review them with you.

Outline Implementation Plan

Service onboarding is an initial implementation meeting where Celerity will collate operational documentation which will be used to gather required information and ensure all parties clearly understands their roles and responsibilities. It ensures Celerity deliver the highest quality of service.

The key components are:

Onboarding	Description
Introductions	Initial meeting with customer & Introductions
Customer Information Gathering and documentation	Discussion with Customer to achieve a detailed understandin of their environment
User Details (Customer)	Customer provides details about uthorised users that can access the service
VPN Setup	VPN access is configured
Service Initialisation	The service is provisioned and configured

Network Configuration (Customer)	Customer configures any network requirements to support the service
Service Tuning	Service rules and logic are tuned
Test & Validate Environment	Testing and validation of the deployment before completing the onboarding process in agreement with the customer.
Onboarding Complete	Onboarding Complete

Service Level Agreement

Celerity Translated Priority Rating	Microsoft Sentinel Severity	Celerity QRadar Magnitude	Target MTTD*
P1	Critical	8-10	30 Mins
P2	High	5-7	1 Hour
P3	Medium	3-4	4 Hours
P4	Low	0-2	8 Hours

**MTTD: Mean time to Detect – time taken for Celerity SOC Analysts to react and start investigations upon incident identification.*

Service Availability

Service Desk:

Method	Service Hours	Contact Details
Web Portal	24x7x365	https://help.celerity-uk.com
Telephone	08:00-18:00hrs on Business Days (UK Time)	0191 4341060

Security Operations Centre (SOC):

Method	Service Hours	Contact Details
Customer specific, based on customer preferences (e.g. telephone call, WhatsApp, etc.)	24x7x365	Customer specific, a service phonebook will be established during onboarding outlining clear 24x7 escalation procedures supported by a primary and secondary on-call rota.

Dependencies

The customer must provide:

- a suitable hardware platform if hosted on a customer site
- remote access network capabilities (e.g. site-to-site VPN, Citrix, etc.)
- agreement to maintenance windows

- a dedicated technical contact to assist and co-ordinate activities related to service onboarding, maintenance, updates and enhancements that will performed on the customer network and infrastructure
- a customer on call rota for incident investigation out of hours, including escalation procedures

Pricing

Please refer to the separate pricing document for this service.

Why Celerity?

Celerity is an Enterprise IT Services Solutions provider and trusted advisor based in the UK, focused on Hybrid Cloud and Managed Services. Cross industry offerings include Cybersecurity, Disaster Recovery, and a range of Systems Management services such as monitoring, automation, and data protection supported by a 24x7 UK Service Desk.

We provide an innovative approach to supporting our enterprise clients and channel partners transitioning to an "as a service" model. Our skilled staff work with enterprise organisations, systems integrators, and public sector organisations, such as local government and healthcare, to design and implement services solutions that address real business needs.

Celerity builds trusted, commercial, and technical partnerships based on an understanding of our customers' requirements. Our experience in supplementing in-house skills, out-tasking processes and supporting our customers and partners in their digital transformation, is recognised informally through recommendations and formally through leading vendor and Industry awards.

Established in 2002 with consistent and sustained growth over many years, Celerity today manages and secures multi-petabytes of highly sensitive data for government, defence, health, financial and commercial organisations globally. We understand that change is constant in almost all businesses today as our clients embrace modernisation and digital transformation, demanding innovation, and creative open-minded thinking to meet the outcomes needed for a digital future.

Core capabilities of the Celerity organisation are:

1. Data Security & Management Services including Backup, Disaster Recovery, Cyber Security
2. Enterprise Compute, Storage, Backup & DR Infrastructure Integration
3. IT Technical Consultancy
4. Infrastructure Monitoring & Management
5. Private / Public / Hybrid Cloud Service Deployment & Management
6. Fully Managed IT Services

We have received a wealth of accolades and industry recognition for delivering exceptional results and service to our clients; providing benefit from collaborative relationships that have been developed over many years of success. Celerity bridges the gap between customer and IT vendors providing access to best-of-breed services via cloud, managed and traditional routes.

- ISO9001 Quality Management
- ISO27001 Information Security Management
- ISO14001 Environmental Management
- Cyber Essentials Plus

Crown Commercial Service Supplier

Celerity holds several accreditations and key skills with experience from a wide range of vendors including VMware, Cisco, Veeam, AWS, Azure, IBM Cloud, Cloudian, Red Hat, Microsoft, IBM, Oracle, Dell, Lenovo