Cyber Security Operations Centre

Service Definition Document

Cyber Security Operations Centre (CSOC)

1 WHAT THE SERVICE IS

Leidos has created a UK Sovereign Cyber Security Operations Centre, leveraging the 2,900 Cyber Security professionals within the US and bringing to bear their Federal Government experience to provide UK Government customers with the best possible service. Leidos ensures an adaptive defence strategy and sustainable threat protection to outpace adversaries.

FEATURES

- Innovation.
- Outpacing adversaries by using high quality data.
- Exploiting Cyber Threat Intelligence.
- Proactive Threat Hunting.
- Effective technology driving customer objectives.
- Optimised tooling.
- Experienced CSOC Analysts applying consistent processes.
- Leveraging technology as a force multiplier for our CSOC Analysts.
- 24x7 detection and response.

BENEFITS

- Enhanced decision making.
- Enhanced situational awareness.
- Predict and prevent Cyber Threats before they happen.
- Mission intelligence.
- Reduced Mean Time to Detect.
- Reduced Mean Time to Respond.
- Reduced Dwell Time.
- Reduced false positive reporting.

OVERVIEW

Leidos UK Cyber Security is on mission with its customers. Cyber Security is more important and more complex than ever before, especially for Government Agencies and Critical National Infrastructure. Cyber Security is vital to ensuring the continuity of Agency functions. In an ever changing Threat Landscape, Cyber Security goes hand in hand with innovation, if you have the right partner with the right approach. Leidos has 30+ years of experience defending Global Cyber Interests and protecting some of the world's most valuable assets.

Service Components

The Leidos UK CSOC is a Defensive Cyber Security capability. Its purpose is to support its customers Cyber Resilience and protect them from the threat of Cyber Attack, providing a 24x7 threat detection and response service. The CSOC services are separated into the following:

CSOC Onboarding

This is the activity for the CSOC Analysts to become familiar with the new environment, tooling, rules, Incident Response Process, how to raise a ticket etc.

CSOC Management

CSOC Management is responsible for ensuring the CSOC is adequately resourced, operating effectively and Incidents are responded to promptly and managed correctly.

Cyber Security Monitoring

Cyber Security Monitoring is used to automatically identify and alert on malicious or suspicious activity according to predefined rules and criteria, enabling Leidos to better detect and respond to Cyber Attacks. Log data collected from multiple sensors and sources and other detective and preventative Cyber Security controls allow visibility into network, server and application activity that might indicate a Cyber Attack.

Cyber Security Alert Investigation

Cyber Security Alert Investigation is the analysis and closure of alerts or offences produced as a result of the rules triggered in the Cyber Security Monitoring. It may result in false positives or true positives, leading to Cyber Security Incident Response.

Cyber Security Incident Response (CSIR)

CSIR is a collection of technology, processes and people. It defines a structured framework to consistently follow in response to a Security Incident and is based on NIST SP 800-61. It follows six phases: Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned.

Root Cause Analysis

Root Cause Analysis is the systematic process to identify the source of a threat, Cyber Attack or compromise and the evidence needed to support that conclusion.

Threat Hunting

Threat Hunting is the proactive process of searching for previously undetected malware and attackers that may reside in an environment. It can result in the detection of suspicious abnormalities that might be an active indicator of un-detected threat activity.

Vulnerability Management

Vulnerability Management promptly detects Vulnerabilities affecting products and technologies, which affect the solutions Leidos delivers to our customers. It is responsible for publishing Vulnerability Assessments indicating what is affected, what the impact could be, and what the mitigation is. Vulnerability Management constitutes the prioritisation, planning and remediation activities through to closure and effectiveness testing.

Cyber Threat Intelligence

Leidos exploit Cyber Threat Intelligence (CTI) to proactively defend against Cyber Threats. It does this by collecting and acting upon Open Source Intelligence on Threats Groups and Threats to enhance situational awareness and inform decision making. Leveraging CTI enables Leidos to reduce attack surface, detect vulnerabilities early before they are exploited, identify and apply IOC's (Indicators of Compromise) and learn from the TTP's (Tactics Techniques and Procedures) used by Adversaries.

SIEM (Security Information Event Monitoring) Content Development

SIEM Content Development is responsible for ensuring the SIEM is effectively configured to detect suspicious activity, threats, IOC's and Cyber Attacks. It is responsible for the following: Developing content based on CTI, developing rules and queries, developing dashboards, Alert management and configuration, defining how logs should be parsed, coordinating event and log, collection and management, and the development of SIEM capabilities based on use cases transforming them into actionable alerts that can be triaged.

CSOC MI Reporting

A Cyber Management Information (MI) report delivers a comprehensive analysis of your organisation's current threat landscape, providing vital insights into the various cyber threats and vulnerabilities specific to your IT environment. Tailored to the business context, the report compiles data from multiple sources, including security devices, system logs, and cyber threat intelligence, to offer a detailed and actionable overview of potential security risks. By highlighting trends, patterns, and emerging threats, the MI report allows the organisation to make informed decisions on security strategies, prioritise risk mitigation efforts, and enhance overall cybersecurity posture. This proactive approach ensures that the business is well-prepared to protect against both known and emerging cyber threats, effectively safeguarding any critical data and systems from potential breaches.

CSOC Escalation

Analysts in the CSOC on shift can escalate for advice, support, guidance and recommendations up to a Level 2 Analyst, who can then escalate to a level 3 Analyst, who can then escalate to the CSOC Manager.

2 ANY ONBOARDING AND OFFBOARDING SUPPORT YOU PROVIDE

Where relevant, Leidos will adopt a consultative approach with customers to define and validate their requirements in order to determine how best to engage with the services. The onboarding and offboarding process is dependent on the specific requirements of the solution, and the delivery methodology agreed upon.

3 PRICING

Please refer to the associated Pricing Document relevant to this Service.

4 TERMS AND CONDITIONS

Please refer to the associated Terms and Conditions Document relevant for our Service Offerings.

5 FURTHER INFORMATION

Please send your requirement to publicsector@uk.leidos.com. Alternatively, if you wish to discuss your requirements in more detail, please send us the following information and we will be happy to contact you:

1. Your organisation name.
2. The name of this service.
3. Your name and contact details.
4. A brief description of your business situation.
5. Your preferred timescales for starting the work.

ABOUT LEIDOS

Leidos is a leading partner to the UK government and the Scottish government as well as having key client partners in transportation and energy. Leidos employs 1300 people across the UK supporting technology and business process transformation programmes for clients such as the Home Office, the Ministry of Defence, the Metropolitan Police Service and NATS.

The success of this work in the UK and beyond shows that we are a trusted partner in the region and that our people can deliver innovative solutions to solve the most challenging problems.

LEVERAGING OUR CORE CAPABILITIES

Our technical core capabilities define the areas in which technical excellence is critical, not only for our business, but in the work we do daily to help customers achieve the important missions on the frontlines of their industry. Explore our core capabilities here.

INCLUSION AND DIVERSITY IN LEIDOS UNITED KINGDOM

Leidos is committed to creating a diverse and inclusive workplace, where every colleague has the opportunity to contribute, share their unique ideas and talents, and be supported in their career. Explore Inclusion and Diversity in the UK here.

SOCIAL VALUE

We're committed to supporting sustainability initiatives, tackling workforce inequality and STEM education by enriching the communities to our operations. Learn more about Social Value in the UK here.