CyberOne

Dark Web Monitoring

G-Cloud 15

Service Description

Service Description
Dark Web Monitoring

This Schedule forms part of Schedule 3 to the Agreement between Customer and Provider and sets out a description of the Services and Service Levels in relation to Dark Web Monitoring as given on a Service Order.

1. Additional Definitions

The following definitions apply in this Schedule

Dark Web Monitoring is the process of actively searching for and tracking an organisation's or individual's sensitive information, such as compromised credentials, intellectual property, or other data, on the dark web.

Brand Protection in the context of Dark Web Monitoring, Brand Protection refers to the detection, analysis, and reporting of information on the dark web that could damage the organisation's reputation, compromise its assets, or be used for malicious purposes.

This includes monitoring for:

- Unauthorised use of the organisation's name, trademarks, or domains.
- Counterfeit products or fraudulent websites impersonating the brand.
- Leaked corporate credentials, customer data, or intellectual property associated with the brand.
- Discussions or listings that could indicate planned attacks or exploitation targeting the organisation.

The objective of Brand Protection is to provide early warning of potential threats so that appropriate mitigation actions can be taken before reputational or financial harm occurs.

Takedown Services is the process of requesting and coordinating the removal of malicious or unauthorised online content — such as phishing sites, counterfeit domains, or leaked data — from the internet. This is typically done by working with hosting providers, domain registrars, social media platforms, or law enforcement to disable or delete the offending material.

3rd Party Risk Monitoring the ongoing process of assessing and managing the risks associated with an organisation's relationships with external entities, such as vendors, suppliers, and service providers.

Company Attributes refers to customer specific domains, subdomains, network addresses, project names, file names, code repositories, keywords, password policies

Major Change to Attributes are any updates that may significantly impact the scope or effectiveness of the monitoring activities. These include addition of new attributes, removal of existing attributes, changes to keyword sets and technology stack modifications

Event refers to a detected occurrence or change in the threat landscape that may indicate a potential risk to the Customer's information security

Request an actionable item arising from the detection of relevant activity or content (e.g., malicious domain, phishing site, data leak) that requires review, escalation, or remediation in line with the agreed runbook.

Alert a notification automatically generated by the Dark Web Monitoring tool when activity, content, or data matching predefined criteria is detected.

2. Additional Commercial Terms Relating To The Dark Web Monitoring Service

Takedown service credits purchased as an addition cost to this service

3. Additional Customer Obligations Relating To The Dark Web Monitoring Service

3.1 The Customer shall advise the Provider of the Company Attributes at the commencement of the Service and of any Major Change to Attributes.

3.2 It is a pre-requisite of the Dark Web Monitoring Service that the Customer has a live MXDR Service with the Provider.

4. Dark Web Monitoring Service

4.1 The Provider will monitor and analyse output from Dark Web Monitoring tools, triaging identified threats and, where applicable, initiating an appropriate response. Findings will be assessed to determine the potential risk to the customer's organisation.

4.2 This service delivers:
4.2.1 **Customer visibility** – Insight into the organisation's exposure on the dark web
4.2.2 **Proactive threat response** – Action taken before potential threats impact the customer's business
4.2.3 **Early warning alerts** – Notification of emerging risks and vulnerabilities
4.2.4 **Third-party monitoring** – Visibility into the dark web exposure of critical suppliers and partners
4.2.5 **Supply chain risk assessment** – Identification of threats that could affect the customer through their supply chain

4.2 **Onboarding Process:**
The onboarding process for the Dark Web Monitoring Service consists of the following key steps:
4.2.1 **Attribute definition** – completion of the form defining the Company Attributes, followed by a collaborative onboarding workshop to validate and finalise the scope of monitored attributes.
4.2.2 **Runbook development** – development of response-specific runbooks and playbooks in coordination with the Security Operations Centre (SOC) to be utilised in the event of threats to the Company Attributes being identified by the Service]. These documents will cover response activities related to brand protection and takedown services.
4.2.3 Configuration of alert handling and ticketing workflows within the Providers ITSM platform to support ongoing monitoring and incident tracking.
4.2.4 Capture and validation of Customer escalation contacts, including primary and secondary points of contact for Event notifications
4.2.5 The Service will be considered live once all attributes are defined and the first business scan has been completed

4.3 Ongoing Service
4.3.1 **Standalone** – Monitoring Only Service
4.3.1.124x7 Dark Web monitoring of the Customers Company Attributes using the Providers Dark Web Monitoring platform
4.3.1.2Automatic assessment of all Alerts as they are received by the platform and initial allocation of priority level
4.3.1.3 Respond to the Alert in accordance with the Response Time SLA.
4.3.1.4 Conduct initial triage of each alert to assess whether the information is credible and warrants actions to identify potential Incidents and Events
4.3.1.5 In the event of a Request being identified the Request will be escalated and/or managed in accordance with run book agreed with Customer.
4.3.1.6 Business Hours support for general Customer enquiries.

4.3.2 **Integrated – Monitoring +**
4.3.2.1 Requests investigated and enriched with information from the SIEM platform
4.3.2.2Mitigation response actions in line with pre-defined playbooks
Investigation and reporting of Requests up to 3 hours per month in total (any unused hours may not be rolled over to future months). Additional investigation and reporting work will be charged as professional services. Additional hours may be purchased as additional consulting hours or using hours purchased as part of the Digital Forensics Incident Response (DFIR) Service

5. Exclusions

5.1 Incident Response services are not included as part of this service
5.2 The Provider will not perform manual searches of the dark web to validate, verify, or locate additional information beyond what is detected and reported by the Dark Web Monitoring tool.
5.3 Dark Web access won't be provided to the Customer
5.4 Dark Web service will only be facilitated via the Dark Web Monitoring Platform
5.5 The Provider will not undertake any direct engagement with the threat actor; this will be actioned via the Dark Web Monitoring platform.
5.6 Any Customer Attributes not defined will not be included as part of the Dark Web monitoring Service.
5.7 Only the activities, deliverables, and responsibilities expressly detailed within this Service Description are included. Any service elements not specifically stated are excluded from the scope unless agreed in writing by both parties.

6. Dark Web Monitoring Service Levels

Response Time (mean time to action) - Standalone – Monitoring Service Only

The Provider will respond to an alert reported by the Dark Web monitoring solution, log it into the agreed ticketing solution, and initiate Triage. This is to confirm to the client that the Alert has been recorded in the system by the Provider via the agreed method, and to acknowledge the initiation of Alert analysis.

	Priority Level	Expected Level	Expected Performance
Enhanced Hours 24x7x365	P1 – Critical	15 Mins	90%
	P2 – Major	30 Mins	90%
Standard Business Hours	P3 – Moderate	1 Hour	90%
	P4 – Minor	2 Hour	90%

Monthly SLA Target is calculated as follows:
For each Severity Level: (number of Alerts responded within SLA Target / number of Alerts recorded in total) * 100

Priority	Definition	Example
P1	Indicate severe threats or confirmed malicious activity	• High impact on business operations or data confidentiality. • High likelihood of exploitation. • Involves critical assets or sensitive data. • Often mapped to CVSS scores of 8.0–10.0 or equivalent.
P2	Potential threats or suspicious behavior that may require investigation	• Moderate impact or likelihood. • May affect non-critical systems. • Requires correlation with other events to confirm severity.
P3	Informational or low-risk events.	• Low impact and low likelihood of exploitation. • Often used for trend analysis or baseline behavior tracking.

7. Service Credits

Service Credits are not applicable as part of this Service.

CyberOne

Dark Web Monitoring

Proactively Identify Threats & Reduce Risk from the Dark Web

Illuminate the Dark Web – Stay Ahead of Cyber Threats

Cybercriminals operate in the shadows, using the dark web to trade stolen credentials, plan ransomware attacks and exploit vulnerabilities. CyberOne's Dark Web Monitoring, powered by Searchlight Cyber, provides unmatched visibility into underground cybercriminal activity.

Unlike basic monitoring services, which rely on outdated breach data, CyberOne delivers real-time intelligence, proactive risk assessment and rapid mitigation - empowering your organisation to detect and stop threats before they escalate.

The Power of Pre-Attack Intelligence

How We Keep You Secure

CyberOne's Dark Web Monitoring provides continuous visibility into hidden cyber threats, enabling proactive detection and response to protect your organisation.

Comprehensive Dark Web Coverage
Monitors forums, marketplaces, ransomware groups and invite-only encrypted channels, providing insights into criminal activity before it becomes a direct threat.

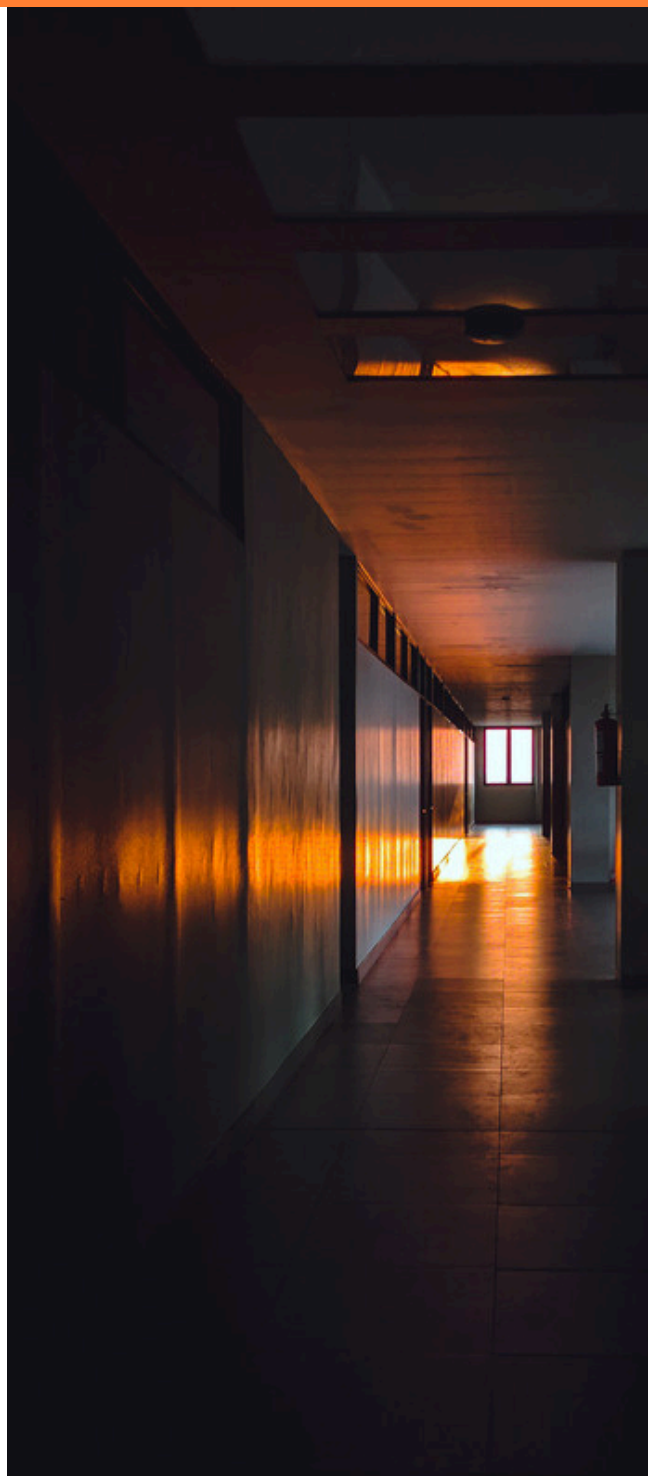
Threat Actor Profiling & Risk Assessment
Tracks cybercriminal discussions related to your organisation, delivering context-rich intelligence for early threat mitigation.

Real-Time Alerts & Automated Response
Unlike periodic scans, our real-time monitoring instantly flags compromised credentials and infrastructure risks. Microsoft Sentinel integration automates responses, ensuring rapid containment.

AI-Powered Dark Web Traffic Insights & Analysis
Uses AI-driven detection and automated correlation to identify malicious activity on your network and dark web forums—enhancing your defensive posture.

Takedown & Remediation Services
Goes beyond alerts by working with hosting providers, law enforcement and security teams to remove leaked data and disrupt cybercriminal operations.

Integrated with MXDR & SOC for 24x7 Protection
Feeds threat intelligence into CyberOne's Managed eXtended Detection & Response (MXDR) and SOC services, ensuring a continuous feedback loop between detection, investigation and response.



Why Choose CyberOne's Dark Web Monitoring?

Unlike basic solutions, we deliver real-time intelligence, deeper dark web access and proactive threat mitigation.

Unmatched Visibility & Deep Intelligence

Scans Beyond Credential Leaks - Detects fraud discussions, IP leaks and ransomware negotiations.

Provides Exclusive Access - Invite-only criminal networks, uncover threats missed by basic tools.

Engages Directly With Threat Actors - Gathers intelligence on cybercrime operations.

Proactive Protection Not Just Alerts

Delivers Real-Time Breach Detection - Instead of relying on outdated breach databases.

Automates Mitigation With Microsoft Sentinel - SIEM/SOAR platforms for faster response.

Tracks Credential & Infrastructure Exposure - Ensures stolen data is addressed immediately.

Complete Risk Management & Compliance Support

Ensures Compliance - GDPR, NIS2 and ISO 27001 through proactive dark web monitoring and reporting.

Provides Executive-Level Reports - Including actionable insights for CISOs and security leaders.

Correlates Threat Intelligence - Aligns with security events to prioritise real risks over alert noise.

Why Choose CyberOne?

Combining top talent and advanced technologies to secure your mission-critical services, CyberOne's MXDR and SOC Services offer comprehensive protection and resilience, empowering organisations to operate securely and confidently.

1. Global Expertise

CyberOne's CREST-accredited SOC professionals bring extensive experience, ensuring robust protection across complex environments.

2. Microsoft Sentinel Expertise

CyberOne's Microsoft-certified experts optimise Sentinel's capabilities for your environment to maximise protection.

3. Proven Threat Detection Standards

Microsoft Advanced Specialisation in Threat Protection, CyberOne applies rigorous standards to ensure continuous protection of your critical assets.

4. 24x7 Threat Monitoring

Around-the-clock monitoring and alerting empower your organisation to stay ahead of threats and maintain operational continuity.

5. Maximised Microsoft ROI

Optimise your Sentinel and wider Microsoft ecosystem investment with our certified-experts, boosting efficiency and reducing costs across your organisation.

6. Insightful Reporting & Analytics

CyberOne's real-time insights empower your organisation with detailed reporting to inform strategy and meet audit requirements.

7. Proactive Risk Management

CyberOne's threat hunting and risk analysis tools actively identify and address vulnerabilities, minimising risks before they can impact your business operations.

8. Tailored Incident Response

Our NCSC Cyber Incident Response Level 2 accreditation demonstrates our capability to handle and remediate complex incidents

About CyberOne

CyberOne is a Microsoft Security Solution Partner and member of the Microsoft Intelligent Security Association (MISA). We deliver one of the UK's most advanced AI-augmented Managed eXtended Detection & Response (MXDR) services, recognised with Microsoft-verified Managed XDR solution status, enabling organisations to move with confidence from risk to resilience. Powered by Microsoft's market-leading security technologies and realised by CyberOne's accredited experts, we help businesses anticipate and contain modern threats so they can thrive.

With 24x7x365 Global SOC coverage, NCSC accredited Cyber Incident Response, CREST SOC and Penetration Testing accreditations and guaranteed SLAs, CyberOne combines Microsoft Security with expert consulting, professional and managed services to protect operations, achieve compliance and build lasting resilience.

Accreditations & Certifications

CyberOne's services are backed by the world's leading standards bodies including NCSC, CREST and ISO as well as our key technology partners, whilst our experts are backed by industry-leading certifications, cementing our role as leaders in cyber security.

CyberOne

hello@cyberone.security

+44 (0) 3452 757575

cyberone.security