Online Exposure Monitoring (OXM)

Service Summary

NCC Group's Online Exposure Monitoring (OXM) Service offers organisations a robust service for continuously tracking and managing their digital footprint, ensuring their online presence is both secure and compliant. This service empowers clients to proactively identify and mitigate risks associated with unauthorised data exposure, reputation damage, and compliance breaches.

Designed for security and compliance professionals, the service provides actionable insights from diverse data sources, including web crawlers, social media platforms, and dark web monitoring. Our comprehensive monitoring equips clients with the knowledge necessary to safeguard their brand, protect sensitive information, and maintain regulatory compliance.

The Online Exposure Monitoring (OXM) Service offers ongoing surveillance and analysis of an organisation's digital presence. By utilising advanced monitoring technologies and expert analysis, the service helps organisations understand their online exposure via a 24/7 platform and take corrective actions to mitigate potential risks, allowing them to maintain a robust and secure online presence in an ever-evolving digital landscape.

The OXM Service includes a pool of retained Threat Intelligence Analyst Support Tokens, which can be utilised for both proactive and reactive taskings. This may include tailored intelligence reports, in-depth incident analysis, or advisory support for emerging threats and strategic planning.

Service Overview

The Online Exposure Monitoring (OXM) Service provides clients with a comprehensive framework to effectively manage their online exposure, keeping them informed, prepared, and capable of responding to digital threats. NCC Group offer two tiers of services, Assisted and Supported. Both provide:

- Continuous monitoring of online platforms to detect data leaks, unauthorised content, and potential compliance issues.
- Alerts regarding significant exposure incidents and vulnerabilities.
- Access to expert analysts for consultation and deeper investigations into exposure incidents.
- Proactive recommendations to enhance online security and reduce the risk of reputational damage.

Currently the source list utilised to create this Online Exposure Monitoring (OXM) Service are:

Dark Web Traffic
Inbound and outbound tor traffic with the associated service and port.

Breached Websites
Leaked organisational data

Social Chats
Telegram discussions, organisational mentions, sale of data.

Code Repositories
API keys, configs, credentials, organisation mentions

Domain Intelligence
Typo-squatted domains, phishing, Domain and SSL expiries

Dark Web Marketplace, Forums, and Onion sites
Discussions about an organisation, network attribute mentions, leaked data market listings, sale of organisation data, leaked credentials, discussions of attack.

Paste Sites
Credentials (username:password), leaked data, organisation PII, network attributes.

VirusTotal
Private documents and emails, private organisational data, classified documents.

Infrastructure Intelligence
Open ports, CVEs, open-cloud buckets, DMARC & DNSSEC, DNS Zone Transfer, SPF.

Online Exposure Monitoring (OXM)

For more information from NCC Group on our G-Cloud 15 service, please contact:

+44 (0)161 209 5200

bidteam@nccgroup.com