Quorum Cyber

Service Description Brand and Credential Monitoring G Cloud 15

+44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Table of Contents

Service Overview

Background

Organisations are increasingly targeted beyond their traditional security perimeter. Cyber criminals actively trade stolen credentials, impersonate trusted brands, exploit exposed domains, and abuse social platforms to deceive customers and staff. These activities often take place on the dark web and closed communities, meaning organisations remain unaware until reputational damage, fraud, or a security incident has already occurred. Without continuous visibility of how a brand and its credentials are being abused, organisations are left reacting too late, increasing both cyber risk and business impact.

Phishing campaigns and exploitation of compromised credentials remain among the most common methods for threat actors to gain initial access to a victims' network. Gaining access to credentials of a user who already has access to data, applications, and infrastructure provides a way of reducing the visibility of an attack, enabling the threat actor to embed themselves in an environment to achieve their goals.

Quorum Cyber's Solution

Quorum Cyber's Brand and Credential Monitoring service provides continuous, intelligence-led monitoring of the open web, dark web, and underground cyber-criminal ecosystems. The service proactively identifies leaked credentials, brand impersonation, domain abuse, and malicious activity targeting the organisation, its people, and its consumers. By combining advanced technology, threat intelligence expertise, and defined response processes, Quorum Cyber delivers early warning and actionable insight that enables organisations to reduce risk before threats escalate into incidents.

Differentiators

- Threat-actor centric intelligence – Monitoring is focused on the platforms, forums, and communication channels actively used by cyber criminals, not just surface-level scanning.
- Human-led analysis – Findings are enriched and validated by experienced threat intelligence analysts, reducing noise and false positives.
- Depth of breach context – Advanced credential monitoring provides insight into how, when, and where data was first compromised and how it reappears over time, reducing the occurrence of credential stuffing impacting users.
- Integrated brand protection – Coverage extends beyond credentials to include domains, websites, social media, messaging platforms, and mobile applications.
- Actionable intelligence, not raw alerts – Outputs are designed to support real-world response actions such as account remediation, takedowns, and user awareness.

Service Features

Credential Leak Monitoring
Continuous monitoring of dark web marketplaces, forums, and underground channels for compromised credentials linked to the organisation's domains.

Brand and Domain Monitoring
Detection of brand and domain mentions indicating targeting, exploitation, or malicious interest by threat actors.

Typo-Squatting and Impersonation Detection
Identification of look-alike domains and counterfeit websites and apps designed to deceive users.

Advanced Credential Intelligence
Enrichment of leaked credential data, including breach origin, clear-text passwords (where available), and historical re-appearance tracking.

Dark Web and Instant Messaging Monitoring
Intelligence-led monitoring of the dark web, and platforms such as Telegram and Discord for malicious discussions related to the organisation or its staff.

Code and Session Data Leak Detection
Identification of exposed credentials, API keys, session tokens, and cookies from sources such as GitHub and underground markets.

Social Media and VIP Monitoring
Detection of fake social profiles impersonating the organisation or named executives to prevent fraud and reputational damage.

Service Benefits

- Protection of citizen trust and organisational reputation
- Early threat detection before attacks, fraud, or brand damage occur
- Reduced likelihood of account compromise through timely credential remediation
- Improved visibility of external cyber risk beyond the network
- Faster, more confident decision-making through analyst-validated intelligence
- Demonstrable risk reduction aligned to governance, risk, and compliance objectives