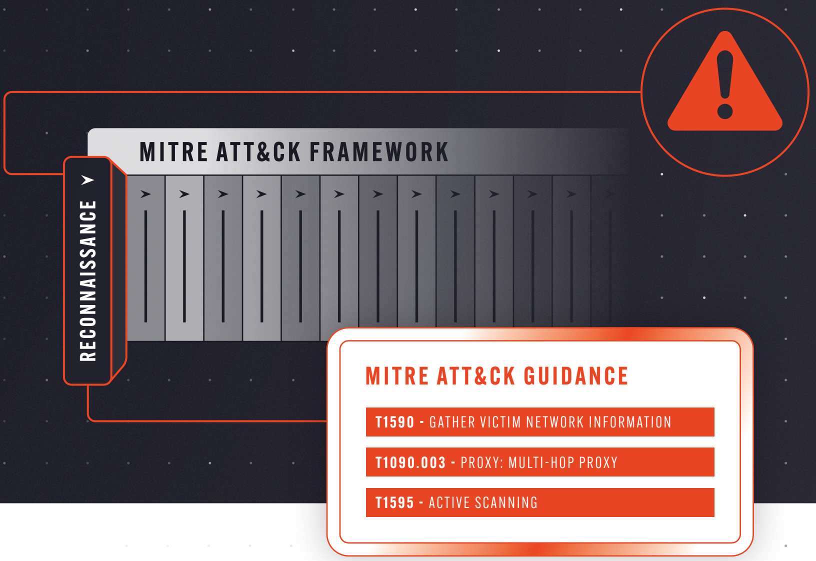
SEARCHLIGHT CYBER

DarkIQ

FOR GOVERNMENT



MITRE ATT&CK FRAMEWORK

RECONNAISSANCE

MITRE ATT&CK GUIDANCE

- T1590 - GATHER VICTIM NETWORK INFORMATION
- T1090.003 - PROXY: MULTI-HOP PROXY
- T1595 - ACTIVE SCANNING

MONITOR THE DARK WEB FOR THREATS TO YOUR AGENCY AND STAFF

Gain continuous, real-time visibility into adversaries targeting your personnel, sensitive data, and critical infrastructure on the dark web. DarkIQ automatically identifies threats to your agency and its supply chain, with actionable dark web alerts – before your data or systems become compromised.

> *We were blown away by the robustness of the platform and its features [...] Searchlight has saved us a lot of time and resources – approximately 32-40 hours a month!*

UNCOVER HIDDEN THREATS WITH CONTEXT-RICH ALERTS

DarkIQ's advanced engine automatically indexes, translates, and enriches dark web data– filtering out the noise so you can quickly identify and act on the earliest signs of an attack.

INSTANTLY IDENTIFY DARK WEB THREATS TO YOUR ORGANIZATION

Our browser-based tools allow government security teams to instantly identify threats to their organization's digital assets by simply entering IP addresses and domains.

DETECT PRE-ATTACK SIGNALS NO OTHER VENDOR CAN SEE

Gain visibility into Tor traffic to and from your network, enabling the detection of insider threat, data exfiltration attempts, and potential malware command-and-control activity.

PART OF SEARCHLIGHT'S ALL-IN-ONE EXTERNAL CYBER RISK MANAGEMENT SOLUTION

ASSETNOTE

Attack Surface Management

- Hourly scans across your entire environment
- Alerts on verified exposures, with POC's for every finding
- Zero-day alerts from our research team in product

DARKIQ

Dark Web Monitoring

- Continuous dark web scanning
- Get prioritized alerts focused on your specific attack surface
- Resolve threats quicker with out MITRE ATT&CK® mapping

CERBERUS

Dark Web Investigations

- Identiy, preserve, and share dark web evidence with ease
- Securely access Tor and I2P services with our virtual machine
- Set alerts to monitor keywords and actors across the dark web

Stop cyber attacks before they happen

CONTINUOUSLY MONITOR THE DARK WEB FOR SIGNS THAT YOU ARE BEING TARGETED. DETECT LEAKED EMPLOYEE CREDENTIALS, PHISHING INFRASTRUCTURE, AND DARK WEB CHATTER - LONG BEFORE CRIMINALS HAVE A CHANCE TO HIT YOUR NETWORK.

KEY FEATURES

Tailored Alerts From Closed-Source Intel

Continuously monitor for mentions of your organization across underground forums, marketplaces, and encrypted Telegram and Discord chats.

Dark Web Traffic Monitoring

Advanced network traffic analysis provides visibility into all incoming and outgoing dark web traffic to any IP address, CIDR, or domain using our proprietary technology.

Integrated MITRE ATT&CK® Mapping

Rapidly respond to threats with context-rich alerts mapped to the relevant MITRE ATT&CK® techniques and their recommended mitigations.

AI-Powered Translation

Understand what criminals are saying using our AI-Powered Translation, optimized for dark web content.

Law Enforcement Grade Data

Automatically scans your organization's attributes, against +475 billion recaptured data points from the dark, deep, and clear web.

Company Health Dashboard & Reporting

Monitor your agency's open actions and health report and easily create one-click reports to prove your team's impact.

TRUSTED BY GOVERNMENT AGENCIES AND LEADING COMPANIES WORLDWIDE

QANTAS · Linktree* · Canva · IMMUTABLE · afterpay · YUGALABS

TWILIO Segment · OAKWOOD BANK · utmb Health · nccgroup · Vitality · CHECK POINT

PROTECT YOUR DATA AND INFRASTRUCTURE. **LEARN HOW AT SLCYBER.IO/DARKIQ**

SEARCHLIGHT. CYBER

SLCYBER.IO
SALES@SLCYBER.IO

UK HEADQUARTERS
Suite 63, Pure Offices, 1 Port Way,
Port Solent, Portsmouth PO6 4TY
+44 (0)345 862 2925

USA HEADQUARTERS
44 Merrimac Street,
Newburyport, MA 01950
+1 (202) 684 7516

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM · CYBER ESSENTIALS · AICPA SOC · Crown Commercial Service Supplier