Managed Detection and Response (MDR 24/7)

TorchLight leverages Cisco to create an around the clock, complete MDR solution.

Overview

Through its MDR cybersecurity service packages, TorchLight helps clients protect their data and assets from real threats that elude common organizational security controls—so they can spend less time chasing down false positives and more time on their core business.

MDR clients also benefit from flexible Security Orchestration Automation & Response (SOAR) implementation options, tailored to meet each client's specific business needs. This flexibility enables either turnkey solutions—which include TorchLight-provided "Cisco-as-a-Service" Security Hardware and Software (SHS)—or customized "Bring-Your-Own-Tech" (BYOT) solutions, which help clients to effectively leverage their current toolset investments (e.g., SIEM, Vulnerability Scans, Threat Intelligence, Identity Management, etc.) in close integration with TorchLight security processes and personnel.

The most inclusive package spans four key service components:

Threat Intelligence and Research regarding cyber threats and threat actors, which helps clients mitigate harmful events before they impact the enterprise.

Endpoint Detection and Response (EDR) tools that provide cloud-delivered detection and forensic capabilities, which are vastly superior than perimeter controls, traditional endpoint software, and OS or Applications logs.

Perimeter Telemetry tools that quickly correlate data from data from firewalls, IDS/IPS, WAFs, and network infrastructure to investigate threat alerts—even the ones that originate from within—which effectively confirms and expands upon endpoint reporting data.

Incident Management and Response support, based on a structured methodology for handling security incidents, breaches, and cyber threats.

TorchLight Designed, Cisco Powered.

Cisco Secure Endpoint offers cloud-delivered endpoint protection and advanced endpoint detection and response across multi-domain control points.

Secure Cloud Analytics (formerly Stealthwatch Cloud) collects and analyzes network data to automatically detect threats that manage to infiltrate the perimeter, and even the ones that originate from within.

Cisco Secure DNS (formerly Umbrella) unifies multiple security functions in a single cloud service to secure internet access and control cloud app usage from your network, branch offices, and roaming users.

50% By 2025 over 50% of organizations will be using MDR services for threat monitoring, detection, and response functions.

24/7 Monitoring and improved communications mechanisms with experienced SOC analysts

170K In 2021, the average payout by a mid-sized organization was $170,404.

80% Of victims who submitted a ransom payment experienced another attack soon after