



Be Prepared: Manage Risks through Proactive Threat Detection

Organizations are under constant attack, from persistent attackers and threat groups around the world, and need to shift from just focusing on compliance approach to a broader risk identification, mitigation and protection strategy. The ability to understand what threats exists in your environment, what these types of threats are and how to remediate is a critical element of a cyber defense strategy.

Solution Overview

Attacks today target multiple entry points simultaneously in a coordinated and methodical approach, making it difficult for organizations to keep up with these constant threats.

The ability to search for compromising activity against your brand, assets, employees and partners is essential to help you create a remediation action plan to address risks.

Data Collected and Reported

Frontline Cyber Threat Assessment™ (Frontline CTA™), a unique service offered by Digital Defense that offers organizations visibility of their:

- Stolen data
- Credentials
- Customer lists
- Private employee information
- Intellectual property

Through Frontline CTA, you have the ability to uncover malicious activity, threat indicators to the enterprise, illegal marketplace dealings and so much more, providing insight into the your organization's risk exposure, inclusive of specific types of threats. Your security operations and risk mitigation actions can be strategically guided by the assessment findings.

Understanding Your Threat Exposure

Digital Defense Intelligence Analysts work with your team to identify specific areas of concern, sensitive markers and key personnel to create you assessment profile. Your assigned analyst will review historical information from multiple sources (Social Media, Dark Nets, Paste Sites, Forums, etc.) to create a customized, risk prioritization, contextualized intelligence assessment report inclusive of:

- Identification and prioritization of threats
 - High, medium and low
- Exposure
 - Brand
 - Assets
 - Retrieved data (i.e. credit cards, email accounts, credentials and passwords)
- Adversarial behavior against your organization
- Specifics around dates and activity observed
- Executive and key personnel exposure

Upon delivery of Frontline CTA, you will receive a web briefing from an Intelligence Analyst to review the findings and provide recommendations to respond to identified threats.