ADDRESSING YOUR CHALLENGES

Strengthen your security posture and gain greater awareness of threats to your business ecosystem. Our analysts and systems monitor the following:

**Observed on Company Systems:**
- Malware hosting/distribution
- Virus/Botnet infection
- Command-and-Control (C2) activity
- Malicious/Scanning behavior
- Sending Spam
- Questionable asset use: proxy, Tor node, etc.
- Hosting phishing activity
- Evidence of ransomware detected
- Inferred Vulnerabilities
- Open Ports
- SSL Certificate Information

**Observed on Open Source:**
- Suspicious Domain Registrations
- Compromised Account Credentials
- Phishing or spoof sites
- Sensitive/Confidential/ IUser document & information disclosure
- Compromised credit card verified by Issuer Identification Numbers (IIN) for card issuing institutions
- Discussion by known threat actors
- Discussions & threads in the Dark Web, Hacker Forums, IRC, etc.
- Internal & Proprietary Information

WHAT IS MANAGED THREAT INTELLIGENCE?

A managed service that provides 24/7/365 coverage, continuously monitoring the internet for indicators of risks and threats to your network and employees, all while minimizing overhead and reserving your staff for mission-critical tasks.

Our systems and team of security experts continuously monitor the surface, social, and Deep and Dark Web as well as your own publicly facing systems to find these threats, as a managed service.

WHY?

As digital dependence increases, it is more important than ever to protect your organization against cyber attacks. Organizations are struggling to keep up with the growing risk of malware, ransomware, and data breaches. A managed threat intelligence service provides an intelligence-driven external perspective on threats and risks.

ADDITIONAL FEATURES

- Curated global intelligence reports
- 24/7/365 human-vetted alerts
- Monitors for data breach announcements
- Granular incidents delivered via portal and API
- Peer and industry benchmarking
- 24/7/365 support for configuration requests & troubleshooting
- On-Demand Investigation & Analysis (add-on cost)
- Response and Mitigation Services (add-on cost)
Managed Threat Intelligence is the right choice for organizations who need to rapidly gain specialized threat intelligence capabilities, but lack the internal staffing, processes, and capital to build a robust threat intelligence operation of their own.

**WHY MANAGED THREAT INTELLIGENCE?**

**Streamlined and efficient**
Streamline the process and fight your threats from start to finish with the same team, so you can rest assured that all of your issues are handled swiftly and with the same skill and importance.

**Predictable Costs**
Managed Threat Intelligence delivers a consistent service at a predictable price, while minimizing CapEx and OpEx spend associated with building out infrastructure and hiring staff to run your threat intelligence program.

**Quick & Easy Deployment**
LookingGlass provides the team, processes and infrastructure to begin delivering threat intelligence immediately. With Managed Threat Intelligence, you will be up and running in a matter of hours, instead of weeks or months.

**Trained Cyber Experts**
By 2019 there will be nearly two million unfilled cybersecurity positions.² Fill the gaps in your headcount by partnering with an organization that gives you access to fully-trained, industry experts so your staff can use their valuable time to focus on your most important security demands.

**ABOUT LOOKINGGLASS CYBER SOLUTIONS**

LookingGlass is a leader in intelligence-driven risk mitigation, including global attack surface monitoring, threat modeling, and network defense. Our full-service portfolio integrates threat intelligence, analysis, and a robust set of tools to operationalize threat mitigation in the network. With standard and custom solutions, LookingGlass makes cyber security smart and seamless for governments and enterprises.

Learn more at [http://www.LookingGlassCyber.com](http://www.LookingGlassCyber.com)

---


© 2020 LookingGlass Cyber Solutions, Inc. All rights reserved.