Trusted Internet provides clients access to a single source comprehensive cyber security provider.

TRUSTED INTERNET KEY FACTS:

Experience: Elite Cyber Security/Threat Capabilities and Operators Provide Clients Industry-Leading Solutions

- Trusted Internet cyber operators are trusted by individuals, leaders in Corporate America and our National Security Infrastructure to monitor, defend and defeat emerging and known digital threats. Cyber technology solutions include first-in-industry offerings and novel, automated global threat and analysis collection.
- Each of our virtual CISOs is a Certified Information System Security Professional with an average of over 20 years experience.
- Each virtual CISO has also held a TS/SCI security clearance.
- Key positions include Command, AF SOC, Director/GS-15 at the DOD Cyber Crime Center, Principal Engineer, Carnegie Mellon University, Software Engineering Institute, CISO for Northrop Grumman Electronics, Chief, Cyber Threat Analysis and Intelligence, Northrop Grumman, Information Security, Cisco, Navy Intelligence, Air Force Communications

Past Performance:

- CEO: Former DCISE Director (09-12) and CISO, Northrop Grumman Electronics Sector, Cisco Systems, USN Intelligence Officer
- Virtual CISO™ staff:
  - Former Director, USAF SOC, ITPM at Dartmouth College and retired USAF LCOL
  - Former CISO, SkillSoft
  - Former CISO, Alion Science and Technologies
  - Current head of IT, University of Arizona and retired USAR E9
- Corporate espionage and insider threat experience going back almost 20 years.
- Saved a Houston based $3.5b Oil and Gas company from Ransomware extinction. Third largest ransomware case in 2018.
- 10+ years of Advanced Persistent Threat hunting experience.
- White label services to Global Guardian, a highly skilled physical security company for nearly 5 years.

Capabilities:

- Leverage a Core Suite of Advanced Cyber Security Technology Capabilities
- Expert level took kit includes next-generation firewalls and endpoints, running artificial intelligence and machine learning, backed by a 24/7 Security Operations Center staffed by CISSP's MS and BS level analysts.
- Utilize one of the largest private repositories of intelligence and malicious entities in the world.
- Utilize an Industry-first solution to identify file-less malware in real-time.

CYBER RISK ASSESSMENT

In many cases, clients wish to perform a cyber threat assessment before ordering any equipment or planning for a more secure system. Trusted Internet performs testing using passive means by installing a next-generation firewall on your network and monitoring activities entering and leaving your network, for approximately seven days. Once complete, you'll have an accurate picture of the threats you face.

ENGINEERING

Your assigned Chief Information Security officer and engineering team will work with you, the Trusted Internet representative to design and then engineer an appropriate response or system to seamlessly secure your customer's (physical or other) network with minimal impact on their day-to-day operations. Following the report, you may choose to retain Trusted Internet for network protection and monitoring, management, remote troubleshooting, and quarantine capabilities.

WHO AND HOW WE DEFEND

Trusted Internet is a Single Source Provider of Cyber Security Solutions that delivers Peace of Mind to both Corporations and Individuals; we provide our clients with a single view of their entire digital threat and vulnerability exposure (external/internal/personal activity hygiene)

DIGITAL FORENSICS

We can help with Network intrusions; breaches of sensitive, regulated, or proprietary data; hackers; malware (viruses, trojans, ransomware); insider threats; employee misconduct, and other compromises.

INSIDER THREAT MONITORING

Insider threat monitoring includes reduced out-of-policy data interactions, prevention of data exfiltration from the end point, scalable architecture for up to 300k endpoints and risky user behavior alerts.

MONITOR, DETECT AND RESPOND, INCLUDING MANAGED OPEN XDR

Monitor Detect and Respond includes the installation of one Next Generation Firewall per internet connection, Secure Workstation bundles on every computer, and VPN on your phones and mobiles to allow you to communicate securely through your firewall while on travel. We use DNS monitoring to stop you from visiting malicious websites, and where possible, bring in multi-factor authentication to replace your passwords. The MDR package allows Trusted Internet several capabilities, including immediate response to threats, vulnerability management of your computing environment, patch management, remote troubleshooting, and quarantine capabilities.

If you already have firewalls and other security tools, we now offer an AI-Driven Stellar Cyber XDR service that allows us to collect data from your existing systems and protect them remotely without ripping and replacing your current infrastructure.

WHAT'S INCLUDED IN OUR MDR PACKAGE?

Cyber Risk Assessments – Baseline and

- Internal & External Vulnerability Assessments
- Assess the cyber readiness and security of physical
- security systems Internal & External Vulnerability
- Assessments

24x7 Monitoring, Detect and Respond

- Subscription-based cybersecurity MDR
- Ingress/Egress network traffic
- One time or ongoing external Threat Intelligence
- Monitoring – cyber indicators of compromise, supply chain, third party

Network
Insider Threat

On-Demand Rapid

- Incident Response
- Forensics
- Attribution & Adjudication

On-Demand

- Strategic Consulting
- (Virtual CISO) Security
- Design/Architecture

To learn more about Trusted Internet's Cyber Security options simply call 1-800-853-6431 or email staysafeonline@trustedinternet.io Our team is standing by to support 24/7.