hardsecure
WE MAKE **SECURITY**

H-CYBER INTELLIGENCE

(CYBER THREAT INTELLIGENCE ANALYSIS SERVICE)

CYBER EFFECT - LEVEL 3 - PRODUCTIVE

h·cyber
INTELLIGENCE

SERVICE DESCRIPTION

Cyber Threat Intelligence (CTI) Analysis Team deliver to the customers, information about threats and threat actors that helps mitigate harmful events in cyberspace. Cyber threat intelligence sources include open source intelligence, social media intelligence, human Intelligence, technical intelligence or intelligence from the deep, surface & dark web / darknet, Tor, Freenet, I2P, Riffle, and others.

VALUE PROPOSITION

Cyber Threat Iintelligence deliver transforming data, gathered by ‘traditional methods of intelligence’ from the platforms of the attackers, into an actionable report for the target customer. The traditional intelligence methods may include passive follow-ups or actively created ‘persona’ to find out what the attackers are talking about, their new methods, their stolen information, and all other operational details. Surely these methods require high level of knowledge and experience where the customers can get to perform proactive decisions in their IT infrastructure. Threat actors operate in “wolf packs” spread in different locations being difficult to track them down in previous information regarding the gathering of the “wolf pack” is not collected that is one of the added value of this service.

SERVICE FEATURES

Cyber Threat Iintelligence Service is comprised of the following elements:

- **Cyber Bits:** short intelligence notifications on cyber-related topics.

- Open-Source Intelligence (OSINT) Dashboard, which aims to capture the most important events from the passing week in a broadly understood cyber domain.

H-CYBER INTELLIGENCE

(CYBER THREAT INTELLIGENCE ANALYSIS SERVICE)

CYBER EFFECT - LEVEL 3 - PRODUCTIVE

- Open-Source feeds of malicious URLs, exploit packs.
- Online forum, social networks, blogs monitoring.
- Liaison with other security members and organizations.
- Common Taxonomy for the National Network of Computer Security Incident Response Teams (CSIRTs).
- **Trends:** updates on emerging patterns and on new modus operandi, tools and techniques that cyber criminals use.
- **Knowledge:** guidance on different aspects of cybercrime such as infrastructure, tools and modus operandi.

ADDED VALUE OF OUR SERVICE

CTI is an essential capability in an organization's security program. Used properly, CTI can enable better-informed security and business decisions, and ultimately allow customers to take decisive action to protect their users, data and reputation against unknow elements.

CTI often includes signature, reputation and threat data feeds, but goes beyond them in almost every way. Our typical activities involve:

- Constant human and technical information gathering on a global scale.
- The provision of adversary-focused and forward looking rich contextual data.
- Customization for our customers organizations.

Comprehensive CTI allows our customers to be proactive and prepare themselves for tomorrow’s adversaries and threats, rather than reacting to yesterday’s attacks. Without the ability to consider all risks and options available to them, cyber security professionals will be unable to make the best possible security decisions for their organization.

H-CYBER INTELLIGENCE

(CYBER THREAT INTELLIGENCE ANALYSIS SERVICE)

CYBER EFFECT - LEVEL 3 - PRODUCTIVE

Here are some of our services benefits of cyber threat intelligence:

» **Valuable insight and context:** Detailing information on what threats are most likely to affect an organization or industry, and indicators to help prevent and detect more attacks.

» **Improved incident response times:** Prioritizing alerts, which enables an organization to respond faster to real threats and reduce the risk of serious breach consequences.

» **Improved communication, planning and investment:** Security teams can communicate real risks to the business and focus on protecting high-risk targets from actual threats via additional security investment and planning.

SERVICE QUOTE REQUEST

For further information, please contact us using one of the following means:

“Hardsecure – Cyber Threat Intelligence Analysis Service” form (available on the service page on the website)

Contact Hardsecure Account Management:
(+351) 218 278 126 (PT)
(+44) 204 538 6686 (UK)
(+1) 202 2318 9859 (USA)
geral@hardsecure.com

Website:
https://en.hardsecure.com (**"Request Proposal"** form).