Hanto Cybersecurity Services

Telophase Hanto Cybersecurity Services identify security flaws and vulnerabilities in systems, devices, and controls that protect your organization's information and resources. We achieve this by simulating internal and external attacks, acting as a malicious hacker seeking to compromise systems, and gaining access to your information. With Hanto, we offer customized security assessments tailored to assist you in preventing attacks that put your organization at risk.

HANTO

Hanto (meaning "the hunt") is the cybersecurity services line under Telophase Corporation

By evaluating your organization's networks, applications, Cloud-based workloads, endpoints, and any threats attempting to access unauthorized resources, we dig deep to explore your organization's ability to defend itself from security threats. These threats can pose catastrophic consequences, such as financial loss, a tarnished reputation, decreased customer loyalty, negative press, and costly fines.

One of the best ways to protect your mission-critical systems is to conduct regular security penetration testing to improve your cyber defense implementations. Our Hanto services increase awareness of your true security posture and help identify where and how hackers might get into your network. Organizations that embrace frequent and comprehensive penetration tests can detect emerging security risks and prevent unauthorized access to critical systems and valuable information.

HANTO CYBERSECURITY ASSESSMENTS

Hanto's Cybersecurity Assessments are designed to evaluate your system configurations from their current state to a high-level security standard that can be found in CIS, NISTRisk Management Framework (RMF), DISA, or other frameworks. These assessments recognize risks and help identify common vulnerabilities and exposures. We evaluate contextual risks to environments using testing, examination and interviewing methodologies.

- **Red Team** – Hanto's Red Team methods challenge organizations to improve their effectiveness by assuming an adversarial role . We design and execute a series of technical and social engineering attacks to identify exploitable weaknesses of an organization's people, processes, and technologies. As part of Red Team, *Penetration Testing* emulates real-world attacker techniques that could compromise information technology, assets, and data. Our penetration testing is different; we focus on actively attacking vulnerabilities and mis-configurations to create actionable reports and recommend remediations. Hanto also leverages the MITRE ATT&CK framework of adversary tactics and techniques based on real-world observations.

- **Purple Team** – Hanto's Purple team deploys engineers virtually or on-site to help the customer detect and stop attacks collaboratively. We evaluate the enterprise security architecture and effectiveness of customer cyber defense implementations.

- **CMMC Gap Analysis** – Our CMMC Gap Analysis helps organizations move towards becoming CMMC Level 2 or 3 certified. We provide CMMC Registered Practitioners (RPs) trained to identify gaps and help companies efficiently prepare for the CMMC certification process. In addition, this service is designed to provide a view into the current state of the Controlled Unclassified Information (CUI) environment and identify areas for improvement.

HANTO CYBER LABS

Our specialized cyber labs allow our security engineers to create and test customized attacks and simulate real world attacks for use with clients. We employ Cloud-based and mobile lab environments for testing of the latest security threats.

HANTO PAST PERFORMANCE

Our reputable, highly experienced, industry-certified Cyber security engineers have backgrounds supporting US Federal government agencies such as DHS, CBP, HHS, NASA, IRS, HHS, Washington Area Airport Authority, and various commercial institutions.

For more information please contact: hantoinfo@telophase.com