



**V360™
COMPREHENSIVE
VULNERABILITY
MANAGEMENT**

DOCUMENT VERSION 2022.06.001

About Us

Corporate Information Technologies (CorpInfoTech) is a full-service information systems management outsourcing and Information Security risk assessment and advisory firm headquartered in Charlotte, NC. Our Information Security team consists of professional penetration testers, technologists, certified assessors, and risk managers that use a team-based approach to deliver a comprehensive assessment product that addresses practical, technical, regulatory, and operational elements collectively.

CorpInfoTech has extensive experience in defense, energy, critical manufacturing, fintech/finsec, banking, and sensitive logistics industries. Certified and accredited by the leading industry organizations including ISC², ISSA, Cyber-AB, and SIRA. Members of CorpInfoTech's cybersecurity team hold seats on working groups within the Internet Engineering Task Force (IETF), Center for Internet Security (CIS), and Information Security Systems Association (ISSA).

We actively contribute to the cybersecurity community as a whole and have helped develop and promote the Center for Internet Security (CIS) Critical Security Controls (CSC), a set of pragmatic key cybersecurity security control areas. Our security staff maintain active and relevant information technology and information security certifications that include specialties in ethical hacking, IT governance, network security, cloud security, and Linux/Windows systems administration.

Critical Security Controls

To better align business, technology, security, and risk stakeholders, CorpInfoTech has adopted the Center for Internet Security's (CIS) Critical Security Controls ("CSC") Framework as a universal reference standard within its assessment and information security consulting practices. This framework, derived from National Institute of Standards and Technology (NIST) controls, aligns well with many common security standards including those used by the United States Department of Defense (DoD) and constituent members of the Defense Industrial Base (DIB).

The CIS Controls are recognized within formally regulated industries that are required to comply with external regulatory oversight including that enforced by FINRA, SEC, and FFIEC Information Security guidelines within the financial services industry, HIPAA within the healthcare industry, and PCI-DSS requirements within the payments and retail industries. Using the CIS Security Controls Framework permits audit-friendly cross-reference and compliance with multiple dimensions of compliance within a single organization across many stakeholders



The Basics

Modern business information systems are increasingly complex environments which are ever evolving. These systems provide critical access to information and Key Business System to an organizations' users and are integral to the operation of a modern enterprise. Operating both locally, within an organizations' facilities, and within multiple cloud platforms the security and safeguarding of these systems is critical. A key element of securing software systems is the discovery, remediation, and continuous assessment of vulnerabilities and configuration-induced areas of exposure. Managing these security risks in a timely manner is critical to the overall security posture of an organization and its most valuable information assets.

Effectively controlling and mitigating exposures caused by software vulnerabilities and related misconfiguration require multiple overlapping mechanisms of detection. This includes evaluating the software environment of each system from both within the operating system the expression of vulnerable operational characteristics of each system from the network(s) to which they are attached. Commercial cloud environments often complicate these tasks by restricting access to one or more of the required characterization mechanisms. Software-induced security risks are not just limited to traditional Windows and Linux environments. Networks that contain ICS, IOT, SCADA, and MES systems all have the potential to introduce similar and potentially more safety or operationally critical areas of exposure.

Compounding the challenges IT Teams face in this critical area of security is the volume of information that must be analyzed in order to prioritize and effectively remediate areas of exposure throughout the software environment. Correlating the characteristics of each systems' software environment, its configuration, ever shifting vulnerabilities, and regulatorily required configuration elements is a data intensive and laborious task. Frequently due to these challenges, IT teams are unable keep up with the vulnerability management and mitigations requirements of an organizations' business information systems.

Using over 20 years of experience, CorpInfoTech has developed **V360™**, a holistic integrated approach to solving these challenges in modern businesses. Using a combination of software-based and network-based characterization mechanisms the entirety of an organization's software environment is quickly and thoroughly assessed. Our platform utilizes location and platform-agnostic technology that allows integrated characterization of on-premises, multi-cloud, and hosted-platform software configuration and vulnerability data. Through the power of Artificial Intelligence (AI) and semi-supervised Machine Learning (ML) this data is correlated and evaluated against multiple threat intelligence feeds to deliver a risk-prioritized, multi-dimensional, correlated dataset. Using this dataset, a comprehensive risk-prioritized view of the areas of exposure of each system are provided.

Our platform further analyzes the areas of exposure of each system and through the power of big data analysis, correlates areas of exposure with any policy or regulatorily required systems configuration elements to provide a risk-prioritized remediation plan for each system. The resulting information can then be used by IT Teams to prioritize their remediation efforts to address the most operationally critical areas of exposure across the full range and spectrum of systems; From traditional Windows servers to specialized ICS devices our platform delivers actionable risk-prioritized vulnerability detection and remediation information that allows IT teams to tackle the challenges of modern vulnerability management.

Technical Service Description

This service utilizes a combination of software and network-attached specialized hardware to perform characterization of the software environment and related vulnerabilities of network-attached systems.

Through a combination of active-scanning (network-based), passive-scanning (network-analysis), and agent-based characterization mechanisms, V360 enables organizations to automatically discover every asset in their environment, including unmanaged assets appearing on the network, inventory all hardware, and classify and continuously assesses these assets for the latest vulnerabilities.

<u>Service Features</u>	V360™
<u>On-premises Device Inventory</u> Detect all devices and applications connected to the network including servers, databases, workstations, routers, printers, IoT devices, and more.	✓
<u>Cloud Inventory</u> Monitor users, instances, networks, storage, databases and their relationships for a continuous inventory of resources and assets across all public cloud platforms.	✓
<u>Patch Detection</u> Automatically correlate vulnerabilities and patches for specific hosts, decreasing your remediation response time. Search for CVEs and identify the latest superseding patches.	✓
<u>Asset Categorization and Normalization</u> Gather detailed information about an asset's entire software environment, prioritize and group assets based on their operational role, sensitivity, and value.	✓
<u>Vulnerability Management</u> Continuously detect software vulnerabilities with the most comprehensive signature database, across the widest range of asset categories.	✓
<u>Configuration Assessment</u> Assess, report, and monitor security-related misconfiguration issues based on the Center for Internet Security (CIS) benchmarks.	✓
<u>Certificate Assessment</u> Assess your digital certificates (internal and external) and TLS configurations for certificate issues and vulnerabilities.	✓
<u>Certificate Inventory & Analysis</u> Detect and catalog all TLS/SSL digital certificates (internal and external facing) from any Certificate Authority.	✓
<u>Continuous Monitoring</u> Identifies threats and monitors unexpected network changes before they turn into breaches.	✓
<u>Threat Protection</u> Pinpoint your most critical threats and prioritize patching. Using real-time threat intelligence and machine learning, take control of evolving threats, and identify what to remediate first.	✓

Service Deliverables

V360™ is delivered as a comprehensive co-managed service that is adaptable to your unique requirements. Using a shared responsibility model to maximize the value and affordability of the service, V360™ approaches vulnerability management as a team sport. Empowering IT teams to tackle the vulnerabilities that exist within their environments using a prioritized risk-based approach. CorpInfoTech will evaluate the vulnerability posture of the organization and using both established configuration analysis mechanisms and industry-standard vulnerability rating mechanisms, will deliver prioritized guidance on the most critical vulnerabilities to focus remediation efforts toward.

Highly customized and unlimited reporting of compliance, overall vulnerability posture, most critical areas of exposure, and vulnerability remediation timeline is available through V360™.

CorpInfoTech will provide one or more network appliances as part of the V360™ service. These security-hardened devices provide an objective on-network perspective from which to ascertain the inventory and vulnerability posture of connected networks.

<u>Service Features</u>	<u>V360™</u>
<u>Customized Scan Definition</u> Create unlimited expert-level vulnerability assessment scans at a customizable frequency	✓
<u>Flexible reporting</u> Creation and delivery of unlimited asset, patch, vulnerability, and/or scan activity reports customized to your organization.	✓
<u>Patch Detection</u> Enumeration, detection, and validation of installed patches. Event-based and trigger-based actions based on currently installed patches or newly discovered vulnerabilities.	✓
<u>Human-reviewed gap analysis</u> Periodic review of open (missing) patches and prioritized recommendations of actions-required.	✓
<u>Area Under The Curve (AUC) Analysis</u> Quarterly analysis of patch application program and comparative analysis of AUC to similar peer organizations.	✓
<u>Priority Alerts</u> CVSS-based prioritized alerts as urgent or high-impact vulnerabilities are disclosed/discovered	✓
<u>Quarterly Guidance</u> Quarterly meeting to review vulnerability remediation progress and prioritized guidance and recommendations to remediate vulnerabilities and patches that remain open.	✓

GET IN TOUCH

704-392-3031

Info@corp-intech.com

www.corp-infotech.com

**ONE PARTNER.
TOTAL
CYBERSECURITY.**