CXR

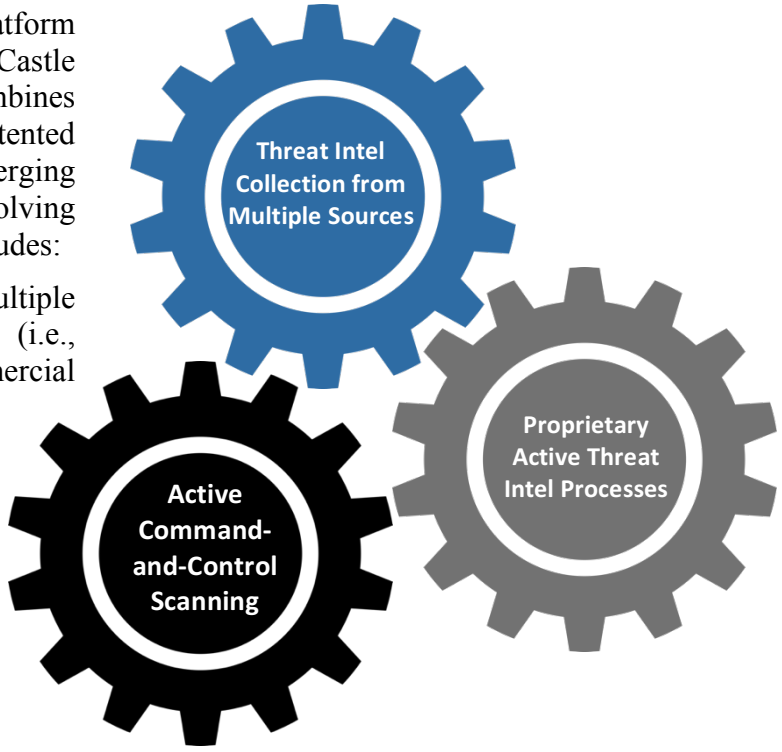
Threat Intelligence Platform

Timely and accurate intelligence is the starting point for effective defense. You can only prevent attacks – and disrupt the cyber kill chain of an attack underway right now – if you clearly understand the threat and are prepared for fast response.

No single source of threat data or single technique can protect your network. It takes broad-based intelligence-gathering that calls on every source, technology and lesson learned from previous cyberattacks.

Collection, Analysis, Integration

CXR is CyberESI's threat intelligence platform and an integral component of our CyberCastle monitoring and management service. It combines multiple sources of threat data with patented techniques to identify existing and emerging threats and keep pace with the ever-evolving threat environment. The CXR solution includes:



- Collection of threat intel from multiple intelligence sources and libraries (i.e., government, open source, and commercial sources).
- Unique threat intelligence processes that actively monitor internet activity to identify and collect new cyber threats and their signatures.
- Active Command and Control Scanning (C2S) to determine if your network is communicating with compromised websites controlled by cyber criminals.
- Continuous analysis and synthesis of all threat intel data sources into actionable results that we integrate into our CyberCastle monitoring and management solution.

CXR adapts continuously to the external threat environment as well your changing security and compliance needs. As a component of CyberCastle, it helps guard your organization's sensitive data, critical IT infrastructure and overall operations, as well as your brand and reputation.

Active C2 Scanning

CXR incorporates CyberESI's patented, cloud-based scanning service for command-and-control nodes on the Web, which can issue commands to your IT infrastructure and receive reports back from corrupted computers. Its patented active C2 monitoring capabilities determine if internal users and devices are communicating with known or unknown command-and-control nodes, thereby putting your organization at risk for a security breach.

For organizations that host some or all of their websites and applications, C2S can automatically crawl those internal assets and determine if they have been breached or are themselves acting as a C2 node. This cloud-based solution operates without customer premise equipment and provides:

- Scanning of all outbound unique URLs
- C2 Spider scanning that crawls internally hosted websites and applications
- Associated malware analysis and reverse engineering
- Experts analysis of results by CyberESI analysts
- Actionable scan results and reports
- Automated and scheduled uploads of URLs and log files

C2S provides enhanced visibility of malicious network activity and improved protection from sophisticated and automated threat actors.

About CyberCastle

CyberCastle is CyberESI's comprehensive security monitoring and management service. CyberCastle provides **defense in depth** that continuously adapts to the latest cyber threats in order to keep your data, applications, and critical infrastructure secure. CyberESI secures your valuable assets, helps ensure regulatory compliance, and enables your IT team to focus on daily IT business operations.

About CyberESI

Founded in 2010 by a team of cybersecurity experts, CyberESI is a Managed Security Service Provider focused on the midsize enterprise with expanding cybersecurity needs. We focus on 24x7x365 remote security monitoring and management of your mission-critical networks. In addition, we offer a full range of professional services that assess your risks, establish the right policies to meet them and design in-depth network defenses.

410-921-3864
info@cyberesi.com
www.cyberesi.com