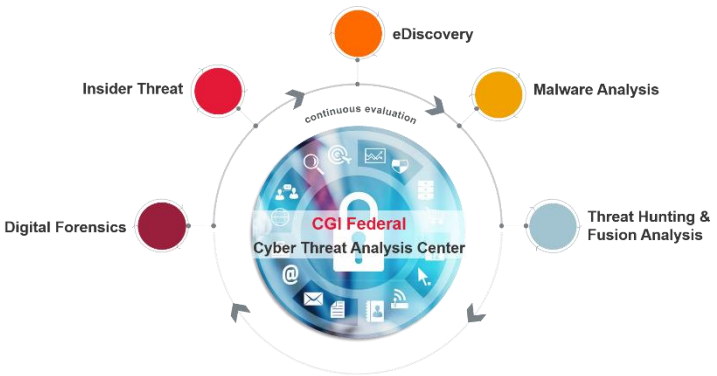
CGI Federal
Cyber Threat Analysis Center

The CGI Federal Cyber Threat Analysis Center (CTAC), an extension of CGI's Security Operations Center, is a full-service solution center that focuses on proactive measures to combat challenging cyber threats and to improve the security posture of government agencies.

CTAC services are provided by qualified analysts who actively maintain industry standard certifications in the cybersecurity field and average over 30 years of experience in incident management, digital forensics, threat intelligence, and malware analysis. An extensive set of industry leading cybersecurity analysis tools are maintained and utilized by our CTAC analysts to ensure the work consistently yields quality results found with the highest level of integrity. The services provided adhere to strict procedures, processes and guidelines defined by organizations such as the National Institute of Standards and Technology (NIST) and the SANS Institute. CTAC has partnered with multiple government and cyber intelligence programs to further expand its capabilities in a variety of fields and services.

The Center also helps Federal customers improve security posture, operational efficiency and incident identification and response efforts through expanded use of agency's commercial-off-the-shelf (COTS) security solutions, data mining, data visualization and data analysis tools to produce tangible results. Our experts identify and address gaps in security monitoring while leveraging an agency's existing COTS security tools through cross-tool integration and automation efforts.

Our CTAC approach encourages the integration of insights from existing COTS tools and DOD and DHS Continuous Diagnostics & Monitoring (CDM) sources and dashboards, as well as other internal tools and threat intelligence sources, thus further optimizing government investments. CTAC focuses on providing cyber analysts the ability to pivot quickly between tools and perform more robust and timely analysis to enable accurate detection of and response to increasingly sophisticated and complex cyber-attacks.



CGI Federal's Cyber Threat Analysis Center services include:

- Digital Forensics
- Insider Threat
- eDiscovery
- Malware Analysis
- Threat Hunting and Fusion Analysis

"CTAC helps Federal customers improve security posture, operational efficiency, incident identification and response efforts."

cgi.com/us-federal

DIGITAL FORENSICS

Digital or Computer forensic investigations usually begin as Incident Response cases; because of this, the first step in any forensics case is to verify the actual occurrence of an incident. Following this verification, the scope, nature and characteristics of an incident are given and the best method for investigation is chosen. Utilizing industry standard toolsets to perform investigations on a wide range of computer systems and mobile devices, CTAC's lab gathers and records data and interviews specific to systems and their incidents. Through the use of monitored Chain of Custody forms, regulated systems of data collection and timeline documentation of evidence, the CTAC Digital Forensics lab works to gather and preserve material relevant to system incidents with integrity and accuracy. Once a timeline and analysis of all data is complete, the results of the work are included in a comprehensive report and provided to leadership/customers for review. CGI can also provide customers expert consulting to remediate the issues and vulnerabilities identified.

INSIDER THREAT

CTAC employs several methods of detecting the existence of potential insider threats. These methods include the monitoring of actions and behaviors on organization-owned systems, devices or networks, as well as recording this information to build a behavioral profile for analysis.

Monitoring sources may include web traffic, work and personal email traffic, logon/logoff times, unauthorized access of accounts or systems, use of unapproved software, file transfers using portable media, usage of online storage services, instant messaging data and physical access logs. CTAC personnel are trained to recognize trends that can act as indicators of insider threat activity. Once trend analyses are complete, a computer forensics investigation may be required for further analysis. The decision to pursue further investigation is determined by the agency.

EDISCOVERY

Short for "electronic discovery", eDiscovery is a term used to describe the process of compiling, storing and securing digital information. Common data sources include email, messaging data and Microsoft Office documents; however, custom format—such as files from a proprietary company-specific database—are also included. The eDiscovery process follows both a structured model created by forensic and legal practitioners as well as an eDiscovery tool vendors known as the Electronic Discovery Reference Model. Growth in this market is fueled by the need for corporations to comply with amendments to the Federal Rules of Civil Procedure covering the discovery of digital information.

Beyond circumstances where litigation is active, eDiscovery services are utilized when employees separate from the company, when litigation is or may be pending or when internal investigations require the preservation of potential evidence for later use.

Security incidents requiring computer eDiscovery support for the customer have the potential to go to court, especially in cases of insider threat, fraud or misuse of the corporate network. CGI experts can provide consulting services for customers needing help preparing for such cases. In situations where an eDiscovery Examiner from the CTAC may be subpoenaed to testify in court, CTAC personnel will consult with CGI's Legal Department for proper proceedings.

CTAC utilizes specialized tools and equipment to store eDiscovery data in a secure environment as required by the client, helping the client fulfill their internal, external and legally-required obligations.

MALWARE ANALYSIS

Malware analysis begins with properly obtaining the malware sample in a way that prevents accidental execution and keeps the sample preserved to ensure sample integrity. CTAC personnel utilize four different methods for malware analysis: static, dynamic, interactive and reverse engineering.

Depending on the circumstances, more than one method may be employed to fully analyze the sample and discover all of the malware capabilities. All four types of analysis take place in either an isolated physical or virtual environment.

- **Static analysis** involves looking at various aspects of a malware sample without executing the sample.
- **Dynamic analysis** involves using automated tools in order to execute the malicious code and record its behavior.
- **Interactive analysis** involves manual execution of the malware in order to observe its behavior, while stepping through each phase of the infection process.
- **Reverse engineering** of malware samples involves revealing the underlying code of the malware sample for in-depth analysis from a developer perspective and to identify content to build custom defense measures.

THREAT HUNTING AND FUSION ANALYSIS

Federal agencies face incredible pressure to continually improve their security posture and keep up with the development of new or improved cyber threats. The threat landscape continues to expand, with thousands of Indicators of Compromise released daily, and it takes a team of professionals to research, analyze, correlate and deliver high quality reporting, fusion analysis and in-depth threat actor profiling to connect the critical dots that drive operations and keep environments secure.

Our experts provide threat hunting capabilities separate from general automated means of threat detection to assist our customers in developing an optimal security posture. The goal of threat hunting is to supplement our clients' defensive operations by providing intelligence reports that further secure their infrastructure and prioritize operations. Threat actors are aware of the automated threat detection methods and have re-written code and modified their tactics, techniques and procedures to bypass traditional firewalls, security information and event management (SIEM) tools, intrusion detection system (IDS), intrusion prevention systems (IPS) and analytics tools that rely on patterns and heuristic analysis for detection. Human analysis is therefore still a critical component of detection, which CTAC provides as part of the human-driven operations associated with threat hunting. Threat hunters are another line of defense assisting client security personnel in the effort to ensure threats are identified, assessed and eradicated from the network, no matter at which point the threat is operating within the kill chain.

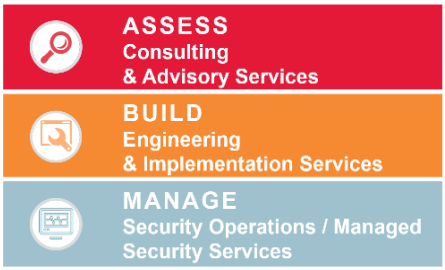
By conducting a deep dive in various data points within the client network, analysts are able to identify various anomalies within the enterprise. They note items of interest for the observed anomalies and pivot off of the observations to paint a full picture of the threat actor(s) that may be present, reporting all relevant findings to the client for remediation. CTAC utilizes cyber threat intelligence services in conjunction with the Diamond Model of Intrusion Analysis to support CGI Federal customers with cyber actor identification, fusion analysis and recommendations that assist in the remediation of threats that seek to violate the confidentiality, integrity or availability of their network, systems, devices and information.

CGI EXPERTS DELIVER CYBER THREAT ANALYSIS SOLUTIONS

CGI Federal's CTAC team brings together diverse experience in cybersecurity, networking, development/coding, cloud computing, compliance and project management. Team members are experts in the latest techniques, attack vectors and approaches to threat monitoring, detection and response, with multiple members holding advanced degrees in cybersecurity and industry certifications such as GCIA, GCIH, C|EH, CISSP, and Security+. Our team performs near real-time analysis of security alerts generated by client assets to identify and respond to security events and incidents. Our capabilities are supported not only by our CTAC and tool vendor provided intelligence, but also by cybersecurity community intelligence available through trusted partnerships.

PROTECTING AMERICA'S ASSETS

CYBERSECURITY OFFERING FRAMEWORK



The CGI Cybersecurity Offering Framework provides an end-to-end portfolio of enablement and transformation solutions that assist clients through the journey of becoming a highly secure organization.

ABOUT CGI

Founded in 1976, CGI is one of the largest IT and business consulting services firms in the world. Operating in hundreds of locations across the globe, CGI professionals help clients to achieve their goals, including becoming customer-centric digital organizations. We deliver an end-to-end portfolio of capabilities, from high-end IT and business consulting to systems integration, outsourcing services and intellectual property solutions that help accelerate clients' results. CGI works with clients around the world through a unique client proximity model complemented by a global delivery center of excellence network to help clients accelerate results, transform their organizations and drive competitive advantage.

cgi.com/us-federal