Cyber Counterintelligence (Public Sector - Commercial)

We provide integrated CCI and engineering support our clients for both reactive and proactive models. Some of these services include but are not limited to:

- Identify, investigate and analyze cyber events of significance;
- Develop tools for applying standard cyber security and analysis practices. We use client's existing tools or can recommend solutions if there are gaps.
- Analyze classified and unclassified networks to identify security vulnerabilities and intrusion detection parameters
- We act as liaison and work cyber counterintelligence investigations with interagency partners (FBI, DoD, CIA, NSA, and others)
- Report changes, trends and implications of evolving cyber issues
- Provide proactive threat hunting
- Provide integrated cyber-investigative, strategic planning, operational plans and technical engineering support
- Analyze classified and unclassified networks to identify security vulnerabilities and intrusion detection parameters;
- Track and document route cause analysis findings and trace the source of the threat
- Identify high risk, potential threat exposures before they occur and ensure proper proactive measures are in place
- Establish misdirection farms for bad actors and steer them away from your business and confidential systems / data
- Dark web proactive investigations and new threat vector hunting based on dark web findings.

Cyber Counterintelligence Government Sector and Military

Core Insights provides CCI services leveraging various security investigative models and tools along with CYBERINT, OSINT, SIGNIT and HUMANIT for Military and other government agencies. Contact us for more information.