CyberESI | CONSULTING GROUP

STREAMLINED SOLUTIONS TO COMPLEX SECURITY PROBLEMS.

CUSTOMIZED SERVICES FOR YOUR SPECIFIC CYBERSECURITY NEEDS.

WHO WE ARE

CyberESI Consulting Group is a small business built to deliver innovative cybersecurity solutions. CyberESI CG was founded in 2010 by the former Chief of Intrusions for the Defense Cyber Crime Center (DC3) Center – the world's largest accredited computer forensics laboratory – and is managed by the former Program Manager of the NIST Cybersecurity Framework – the world's most prevalent approach to cybersecurity risk management. Our corporate objective is to inform proactive cybersecurity risk management with our expert knowledge of threat trends and adversary behavior.

Our corporate headquarters is located in Baltimore, Maryland and supports our team of cybersecurity experts that have an average of 17 years' experience designing and providing information security services across multiple industries. Many of CyberESI CG's personnel have backgrounds as instructors and investigators at DC3. Our team of government and private sector experts draw upon years of experience of enhancing companies' security postures to counteract even the most sophisticated adversaries. Our expert staff is well connected within the cybersecurity community and has established a solid reputation delivering customized solutions tailored to fit specific business needs.

CyberESI | CONSULTING GROUP

SERVICES

The cybersecurity landscape is constantly changing and filled with increasingly sophisticated cyber-attacks. Our cost-effective services help you successfully navigate that landscape to stay ahead of the dangers and keep your network safe.

CyberESI-CG provides a suite of cybersecurity services which provide an in-depth defense of network systems, allowing you to constantly assess your IT needs and vulnerabilities and develop effective solutions to mitigate the risk of data breaches. CyberESI-CG's services are designed to prevent cybersecurity incidents, based on expertise in successfully processing thousands of criminal and nation-state cybersecurity incidents. Each service is also aligned to NIST's Cybersecurity Framework (CSF), the most successful and prevalent approach to cybersecurity risk management. CyberESI-CG provides practical, specific, and prioritized recommendations with every service. Each client will know exactly where to start to reduce risk, address an issue, and improve security posture.

Risk Assessment

Conducted in accordance with industry best practices and national standards, CyberESI CG's risk assessment services provide independent evaluation of security posture ranging from the technical-control to the overall program level. Threats are assessed based on their probability of occurrence, their potential impact to the client, and the controls implemented to mitigate their impact. CyberESI CG's risk assessments are informed by national standards, such as NIST Special Publications, and used to create and evolve disaster recovery plans as well as impact mitigation practices.

- **Network Packets** - pull PCAPs with push-button efficiency
- **Logs** - quickly identify hosts that have triggered alerts from any of your data sources
- **Endpoint Information** - launch an endpoint scan or perform eDiscovery actions

CyberESI | CONSULTING GROUP

Managed Detection and Response

The CyberESI CG Managed Detection & Response (MDR) service identifies and addresses unauthorized activities on networks and computers before those activities become costly cybersecurity incidents. MDR utilizes proprietary, open-source, and closed-source industry-leading technologies, such as Splunk, and the expertise of world-renowned adversary pursuit and incident response professionals.

- **24x7 continuous monitoring and response**
- **8x5 analyst evaluation and hunt**
- **Weekly endpoint security scans**
- **Continuous threat intelligence updates**

The CyberESI CG Managed Detection & Response (MDR) service identifies and addresses unauthorized activities on networks and computers before those activities become costly cybersecurity incidents. MDR utilizes proprietary, open-source, and closed-source industry-leading technologies, such as Splunk, and the expertise of world-renowned adversary pursuit and incident response professionals.

Security Operations Center

CyberESI CG operates a 24/7 automated SOC, in addition to its 10x5 staffed SOC. Outside of the staffed hours, the automated part of the SOC continues to monitor all network traffic and generates alerts for analysts to investigate during staffed hours. Automation provides a more comprehensive view for the analysts to work from, without an overage of hours required to operate the SOC.

Incident Response Services

The first steps of incident response are a part of CyberESI CG's MDR services. CyberESI CG analysts have the training and experience necessary to investigate alerts in order to determine a proper response. CyberESI CG analyst's investigation often reveals a simple fix, patch, or remedy which is then relayed to the client. The investigation may result in a necessary response level escalation where a more senior analyst investigates the alert and, if necessary, engages with the client to resolve any threats. CyberESI CG is prepared to assist clients in handling the more intense threats to their networks when requested.

Vulnerability Assessment and Penetration Testing

CyberESI CG's vulnerability assessment and penetration testing services are related disciplines that enable an organization to look for holes in their security posture and remediate before an adversary finds the weakness. Knowledge of a network's strengths and weaknesses enables an organization to have an on-going understanding of their environment. Vulnerability assessments look for holes in a network firewall, where malicious outsiders can break in and attack a network. Penetration tests try to actively bypass security controls and enter a network environment. This insight allows an organization the opportunity to confirm their assets are protected, or to proactively take action to mitigate any discovered risks.

CyberESI | CONSULTING GROUP

For both disciplines, testing administered by cybersecurity professionals is great, but testing administered by incident responders is excellent! Over 50% of CyberESI CG's workforce has worked at the acclaimed Defense Cyber Crime Center (DC3), successfully responding to both criminal and nation-state incidents. Network architecture strengthened to the recommendations of incident responders dramatically reduces the risk of known tactics, techniques, and procedures (TTPs) used by today's sophisticated cybercriminals.

- **External scanning**
- **Internal Scanning**
- **Social Engineering**
- **Penetration testing**

Policy and Compliance Analysis

CyberESI CG's policy services cover the full lifecycle of cybersecurity, from policy, process, and best practices development to program management and implementation of a tailored cybersecurity program. CyberESI CG's approach, based on years of experience, uses industry best-practice frameworks while measuring against any regulatory requirements to a specific industry.

- **Policy development and review**
- **Review Compliance Policy Requirements**
- **Review Program Maturity**
- **Support Security Control Implementation**

Training and Awareness

Having a security-aware organizational staff greatly reduces the likelihood of a successful cyber attack. CyberESI CG offers training opportunities that capitalize on the findings from other service offerings. Integrating a training session with these other offerings provides staff an immediate opportunity to deeply understand the relevant risks and vulnerabilities specific to each organization.

- **Employee training event**
- **IT staff training event**
- **Tabletop exercise event**
- **Incident response training event**
- **Phishing simulations**

CyberESI | CONSULTING GROUP

Cybersecurity Consulting

CyberESI CG offers customized services for an organization's specific cybersecurity needs. CyberESI CG experts craft streamlined solutions to complex security problems, helping organizations to enhance their security posture, reduce the risk of data breaches, and ensure compliance with relevant industry regulations.

- **Compliance scanning and verification**
- **Endpoint security management**
- **Incident response planning**
- **IT and security architecture assessment**
- **Network security device management**
- **Network and system implementation and configuration**
- **Security gap analysis**

TEAM

Get expert insight from professionals who helped design the CSF, write the NIST SP 800-150 standard, and who have performed thousands of successful incident responses.

JOESEPH DRISSEL

Joseph is the Founder and Chief Executive Officer of BlackhawkNest. He's responsible for all corporate vision, culture, and oversight.

MATT BARRETT

Matt is Chief Operating Officer of BlackhawkNest. He is responsible for all facets of operation, including service oversight, client communications, employee well-being, and corporate operations.

JIM HANSON

Jim brings over 40 years of experience in software development, built on a foundation of hardware experience, to his work for BlackhawkNest. He is responsible for designing and implementing software support for all operations.

RON DE LEOS

Ron has over 20 years of experience in information technology, specializing for more than 13 of those years in cybersecurity, particularly in cyber intrusion investigations, incident response, and cyber threat intelligence.

REGINA SHERIDAN

Regina has over 15 years of experience in cybersecurity, with a strong emphasis on program management, communications, and training.

CyberESI | CONSULTING GROUP

WHY US?

Fill in the gaps. You don't have to be an expert in everything. Let us fill in the gaps!
"Augmenting your team with experts can provide the talent and 'surge capacity' that small businesses need."
– Cyber Security and the Small Business, Frost & Sullivan

Customized. One size does not fit all. Our team becomes familiar with your specific needs and resources and crafts our solutions to help. The result is a much-reduced risk of data breach and a far better return on your investment.

Cybersecurity Framework Focused. The Cyber Security Framework (CSF) is the most successful and prevalent approach to cybersecurity risk management. The five Functions of CSF – Identify, Protect, Detect, Respond, and Recover – remind us of the need to balance preventative measures with preparations should something go wrong. CyberESI-CG helps you gain visibility into all five CSF Functions and reduce risk.

Flexible. CyberESI-CG can leverage your existing team and tools or augment them with our powerful in-house resources.

Trusted. *"CyberESI has been able to work with our organization to help advance our security program, increasing our overall posture. This partnership grants admins time to focus on internal priorities. Our security program continues to mature and evolve in today's aggressive landscape.CyberESI helps us stay ahead of potential threats, as a result, we can sleep at night."*
– Matt Grayson, Chief Information Officer, American Postal Workers Union

TESTIMONIALS

American Postal Workers Union

"CyberESI-CG has been able to work with our organization to help advance our security program, increasing our overall posture. By integrating with our established program, we have been able to replace systems and maintain compliance. This partnership grants admins time to focus on internal priorities. Our security program continues to mature and evolve in today's aggressive landscape. CyberESI-CG helps us stay ahead of potential threats, as a result, we can sleep at night."

– Matt Grayson, Chief Information Officer,
American Postal Workers Union

Analytical Graphics, Inc.

"We appreciate how supportive CyberESI-CG is of our in-house team and talent. They don't just give us recommendations; they help us learn and become better in our areas of responsibility. As I like to say, 'CyberESI-CG doesn't fish for you, they help you learn to fish.'"

– David Downs, Senior Director of Information Technology,
Analytical Graphics, Inc

CyberESI | CONSULTING GROUP

KEY BUSINESS RELATIONSHIPS

CyberESI Consulting Group, Inc. is a Blackhawk cybersecurity service provider focused on time and materials consulting work, and has relationships with several other trusted corporations. These relationships bring multiple patents and proprietary technologies that set them apart from the competition, and allow CyberESI-CG the ability to provide individualized solutions to each client.

CyberESI

Cyber Engineering Services, Inc. - A cybersecurity managed service provider focused on fixed firm price efforts.

BLACKHAWK

BlackhawkNest, Inc. - A cybersecurity software product company focused on providing a comprehensive and innovative analytics platform. The Analytic Platform uses Storbyte's custom-designed hardware to house a unique suite of software curated to deliver managed detection and response capabilities.

storbyte

Storbyte, Inc. - A computer storage company focused on providing reliable, high-capacity hardware for the cybersecurity community and the general computer storage market.