Secure Merger®

Corporate Overview

Headquarters
609 Ponder Place Drive
Suite C
Evans, GA 30809

SecureMerger.com

Mailing Address
PO BOX 540
Augusta, GA 30903

Support Team
Support@SecureMerger.com

Sales Team
Sales@SecureMerger.com

SecureMerger®

SecureMerger.com | 1.844.658.7943

Company Certifications

INDEX OF PAGES

Secure Merger Delivers Cyber Security Services Globally.

We focus on digital asset protection, cyber security assessments, and cyber emergency response. We help protect and value digital assets, detect current intrusions, and dollar quantify an organization's cyber risk.

COMPANY CERTIFICATIONS...

Our team maintains top-tier industry certifications that confirm expertise in the field, and validate specific knowledge. Certifications we hold include:

- (ISC)2 Certified Information Systems Security Professional (CISSP)
- (ISC)2 Certified Information Systems Security Management Professional (CISSP-ISSMP)
- (ISC)2 Certified Information Systems Security Engineering Professional (CISSP-ISSEP)
- ISACA Certified Information Systems Auditor (CISA)
- ISACA Certified Information Security Manager (CISM)
- ISACA Certified in Risk and Information Systems Control (CRISC)
- ISACA Cyber Security Fundamentals Certificate (CSX-F)
- ATAB Certified Anti-Terrorism Specialist-Cyber Terrorism Responder (CAS-CTR)
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Enterprise Defender (GCED)
- GIAC Security Essentials (GSEC)
- IISFA Certified Information Forensics Investigator (CIFI)
- EC-Council Certified Chief Information Security Officer (C|CISO)
- EC-Council Certified Ethical Hacker (C|EH)
- EC-Council Computer Hacking Forensic Investigator (C|HFI)
- EC-Council Emergency Disaster Recovery Professional (E|DRP)
- Cisco Certified Network Associate Route & Switch (CCNA R&S)
- CompTIA Security+ CE
- CompTIA Network+ CE
- CompTIA A+ CE

Cyber Security Risk Assessments

INDEX OF PAGES

Dollar Quantified Risk Exposure

We believe the best way to make actionable decisions from a security risk assessment is to normalize the results in a consistent manner. Our assessments evaluate the annualized, dollar-quantified risk exposure of each of the most significant threat events we find. We put into context what our findings really mean using such numerical sources as:

- Industry studies
- Federal crime statistics
- Organizational business impact analysis
- Secure Merger's own proprietary intelligence
- Open FAIR methodology

Standards-Based Flexibility

Our risk assessments can be flexibly adapted to deliver the same benefits, in terms of the standard most useful to each organization. This includes:

- CIS Controls
- COBIT 5 / 2019
- HIPAA
- ISA/IEC 62443
- ISO/IEC 27001
- NIST SP 800-53

We measure an organization's cyber security maturity. We then zero in on the most serious cyber security risks with dollar-quantified insight into the organization's exposure. We deliver discrete recommendations on how clients can best reduce risks. The result is a comprehensive assessment with big-picture takeaways, as well as granular findings.

Cyber Security Audits

INDEX OF PAGES

Secure Merger assists its clients in understanding not only their organizational compliance with regulatory requirements, but the implications of their cyber security policies and procedures.

We Audit Systems To Determine:

- Systems are in compliance with applicable laws, regulations, contracts, and industry guidelines
- IT data and information have appropriate levels of confidentiality, integrity, and availability
- IT operations are being accomplished efficiently, and effectiveness targets are being met

Type of Audits We Can Perform:

Our thorough expertise delivers quality support to organizations needing:

- IT Audits
- Compliance Audits
- HIPAA Reviews
- IT Security Audits
- Security Assessments
- FISMA Reviews
- COBIT Audits

Incident Response

INDEX OF PAGES

Cyber Breach? We Can Help Fast!

Secure Merger has the capability to detect, investigate, and contain cyber breach incidents. If an issue is uncovered while we are onsite, or if our clients find their networks breached, our team can provide a rapid and effective response. The objectives of security incident response activities are to:

- Limit the incident impact to customers and business partners
- Recover from the incident
- Determine how the incident occurred
- Discover how to avoid further exploitation
- Assess the impact (financial, data, and reputation loss)
- Update security policies and procedures

Practice Makes Perfect

Secure Merger strong suits include:

- Former military cyber experts on staff to handle any situation
- A keen ability to craft efficient security policy
- Years of experience and cyber certification
- A diverse technical skillset (commercial and federal)
- Industry Thought-leaders in the legal, regulatory, and business aspects of cyber security

These coalesce to create engaging breach response scenarios, enlightening table-top exercises, and invaluable training in organizational incident response. Whether as a means of training leaders and key stakeholders, exercising a new process, or growing interdepartmental synergies, our team's guidance enables our clients to approach cyber incidents from a position of strength.

Digital Forensics

INDEX OF PAGES

Forensics For Insurance & Legal

The current situation of business security no longer can be described as a matter of “Will your organization be hacked?” but, rather, “When?”

In the aftermath of a cyber incident, adequate collection, preservation, and analysis of the relevant evidence are the foundational pieces of an effective investigation. If the significant pieces are buried under irrelevant alerts and artifacts, valuable time may be lost in assembling an adequate response strategy.

Breach Investigations are needed if your defenses were penetrated and an investigation is needed for legal or insurance purposes.

Secure Merger’s digital forensics capability provides much-needed context, rich expertise, and keen insight into cyber attacks, so that our clients can effectively investigate and remediate the incident. The Secure Merger team possesses many years of experience and background, the knowledge and “real-world” skills to identify, track, and prosecute the cyber-criminal.

Our ability to collect, process, and preserve evidence and chain of custody sets up our analysis and intelligence capability, which support effective investigation and equip our clients to respond in an appropriate and timely manner. Our team will serve as expert witnesses, including testimony in court for disciplinary procedures.

INDEX OF PAGES

Outside Attack Assessments

Organizations cannot exist on an island; they must interact with the outside world in the form of customers, vendors, business associates, and competitors. All the while, adversaries feast on low hanging fruit, and the means of determining an organization's external weaknesses are becoming increasingly automated and sophisticated.

"Upwards of 90% of successful cyber attacks begin by 'attacking the human' with social engineering" – Leighton Johnson (Chief Security Officer)

For these reasons, we at Secure Merger place a heavy importance on our clients understanding their security posture from the outside looking in. By taking the same steps that adversaries do when canvassing potential targets for attack, we reveal weaknesses in a friendly manner before they can be exploited by an unfriendly actor.

Our Attack Assessment is like a penetration test of our clients' people, and their outward face to the world. Our examination includes:

- Global Network Footprinting
- Intelligence Collection
- Social Engineering – Email, Phone, and SMS Text
- Web Application OWASP Testing

An essential and often overlooked aspect of any security evaluation is the external, "black box" examination, which has the opportunity to reveal weaknesses in areas such as the organization's supply chain, personnel training, web attacks, visitor control, and susceptibility to Business Email Compromise, to name a few. Our team ensures that our clients do not overestimate their defenses when it comes to external adversaries.

Penetration Testing

INDEX OF PAGES

We Emulate The Bad Guys

Large enterprises with complex security programs need to fully explore the implications of new infrastructure and system configurations, particularly when critical systems and sensitive data stand to be impacted. By thinking outside the box, proficient testers who emulate the techniques and abilities of adversaries can help identify and mitigate threats before they are exploited.

A penetration testing event is a focused and targeted attack simulation to identify, evaluate, and demonstrate a particular vulnerability. The specific focus of the engagement can range from penetrating internet firewalls or social engineering, to compromising application architecture.

Secure Merger's skilled penetration testers (many are retired military) have a deep knowledge of system operation, networking, and vulnerability exploitation, and how to best combine automated tools with technical know-how.

Our cooperative penetration assessment process includes such capabilities as:

- Custom Scripting
- System Exploitation
- Privilege Escalation
- Lateral Movement
- Deploy Rogue Host
- Obtain Credentials
- Own the Domain
- Web App Pentest
- Test Incident Response

SecureMerger®

Identify Security Vulnerabilities

Development and deployment of code on critical systems must incorporate secure code review. A proactive approach can preclude a host of financial and regulatory consequences to an organization.

Secure Merger will identify areas of highest risk, including:

- Unvalidated input
- Broken access control
- Broken authentication and session management
- Cross Site Scripting (XSS) flaws
- Buffer overflows
- Injection flaws
- Improper error handling
- Insecure storage
- Denial of service
- Insecure configuration management

When analyzing the attack surface and examining the data flow, our analysts scrutinize each transaction in the application and the associated security functions they invoke. This includes such topics as:

- Authentication
- Authorization
- Data Validation
- Encryption
- Error Handling
- Logging
- Network Architecture
- Security Configuration
- Session Management

Policy/Program Development

INDEX OF PAGES

Pick A Topic

There are few industries in either the public or private sector in which Secure Merger's analysts have not worked to solve cyber security problems. Our insightful approach to programmatic security management to achieve both comprehensive regulatory compliance and efficient risk mitigation equips us to build our clients' security programs into their organizational strengths.

In the same manner that we approach the early aspects of any risk assessment, understanding an organization's existing security posture includes a thorough documentation review of:

- Policies / Procedures
- Previous Audits / Assessments
- Network and System Diagrams
- System Inventories
- Configurations
- Log Analysis
- Incident Response Plans
- Business Continuity Plans
- Disaster Recovery Plans
- Training Records

In each of these topic areas, Secure Merger's problem-solving expertise, resource management experience, and current industry intelligence deliver on-target review and custom-tailored improvement recommendations. In cases where our clients lack certain aspects of an effective security program, or organizational changes prompt an overhaul, Secure Merger's deep well of knowledge in each of these areas delivers world-class security program development.

INDEX OF PAGES

We Train Your Staff Onsite

Secure Merger aims to provide the most innovative and best security practices, procedures, training, and activities to support our clients. It is crucial to provide our customers with the technology and expertise required to thrive in today's fast paced and ever-changing high-tech world. We achieve this by applying state-of-the-art technology and realistic, cost-effective, creative management solutions to a diverse business base—both at home and across the country.

Secure Merger training support efforts include development and delivery in a wide range of areas:

- Network connectivity (internal, third party, public)
- Specialist industry devices/instrumentation
- Platforms, applications, and software used
- On-premises, cloud, or hybrid systems
- Operational support for security
- User community and capabilities

Our focus on building a creative and technically challenging environment has allowed us to attract some of the richest talent available, allowing Secure Merger to develop outstanding cutting-edge solutions and services for our customers. Our certified instructors ensure your employee, even with minimum-level knowledge, is provided the best possible instruction for certification test preparation and workforce requirements. To facilitate an efficient atmosphere, our informative courses are limited to fewer than 50 students and our in-depth technical courses are limited to 30 students per session.

Standard Risk Assessment

INDEX OF PAGES

Built For Mergers and Acquisitions

We deliver an assessment of an organization's cyber security risk, with analysis focused on their most serious threats. This provides you with generalized determinations of the organization's maturity, strengths, and weaknesses, and high-level action plans for where to focus risk mitigation efforts.

ADVANTAGES...

•"Hands-off" assessment can be conducted without the analysis team connecting to the target's network

•Streamlined process digs deeper than simple documentation review, confirming the documentation with interviews and observations

•Can also be used to validate an organization's own assessment of its strengths, weaknesses, and greatest risks

NEXT STEPS...

This assessment reveals enough information to help you decide whether you want to:

•Conduct quantified risk analysis
•Explore risk mitigation options
•Collect network data to confirm suspicions or investigate issues

STEP ONE

Determine the target's compliance requirements

STEP TWO

Assess the target's documentation

- Policies / Procedures
- Previous audits
- Training content
- Network diagrams
- System inventories
- Configurations
- Response & recovery plans

STEP THREE

Travel to site to conduct targeted interviews and observations on the areas of most concern

STEP FOUR

Draw conclusions and provide overall assessment of the organization's cyber maturity, strengths, and weaknesses

STEP FIVE

Provide high-level recommendations for mitigating risk

Dollar-Quantified Risk (M&A)

We thoroughly assess the target's cyber risk, and quantify the loss exposure of their most serious threats. We show you the relative maturity of the cyber program across 23 different areas, with recommended improvements. We provide high-level action plans to focus your risk mitigation and dollar quantify how impactful those action plans will be.

ADVANTAGES...

•Comprehensive, onsite assessment structured around the 108-item NIST Cybersecurity Framework

•Dollar quantifies risk exposure experienced by the organization due to its most critical threats

•Pinpoints exactly where immature aspects of the security program are contributing to risk, and how much they need to be improved to reduce the risk to an acceptable level

•Investigates vendor and third-party relationships

• Highlights training deficiencies among personnel

STEP ONE

Determine the target's compliance requirements

STEP TWO

Advance documentation review

- Policies / Procedures
- Previous audits
- Training content
- Network diagrams
- System inventories
- Configurations
- Response & recovery plans

STEP THREE

Thorough onsite investigation of the organization's cyber security

- Employee interviews
- Onsite observations
- Network scanning tools

STEP FOUR

Quantify the organization's risk exposure, and prioritize threats for mitigation

STEP FIVE

Draw up action plans of varying rigor, quantifying the impact each plan will have on risk exposure, and the cost of implementation

STEP SIX

We deliver reports and answer high level questions from company executives and IT teams onsite