CyberSecurity Services

CyberSecOp

Dedicated to helping organizations optimize the security performance of their people, processes, and technologies to deliver positive financial and operational business outcomes.

ISO 27001 CERTIFIED

CYBER AB REGISTERED PRACTITIONER ORGANIZATION RPO

AICPA SOC aicpa.org/soc4so

PMP® Professional Certification

SOC 2 TYPE 2 AICPA SOC

www.CyberSecOp.com

866-973-2677

UNLEASH YOUR ORGANIZATION'S FULL POTENTIAL WITH OVER 20 YEARS OF EXPERTISE IN CYBERSECURITY

At the heart of our mission lies a commitment to safeguarding our clients from the devastating emotional, operational, and financial consequences of cyberattacks. By focusing on the performance of the people, processes, and technologies, we strive to create a robust defense system tailored to each organization's unique needs. We pride ourselves on our ability to integrate seamlessly into a client's existing security team, delivering the necessary support and expertise to bolster security measures effectively.

As a recognized industry leader in cybersecurity by Gartner and Javelin Research, we offer highly effective and cost-efficient solutions designed to elevate security, ensure compliance, and strengthen digital defenses.

INDUSTRIES WE SERVE

- FINANCIAL SERVICES
- HEALTHCARE & PHARMA
- MANUFACTURING
- EDUCATION & RESEARCH
- LEGAL
- RETAIL & ECOMMERCE
- TECH COMPANIES
- ENERGY & UTILITIES
- UNION & PUBLIC ADMINISTRATION
- CRITICAL INFRASTRUCTURE
- AEROSPACE & AVIATION
- PROFESSIONAL, BUSINESS, & CONSUMER SERVICES

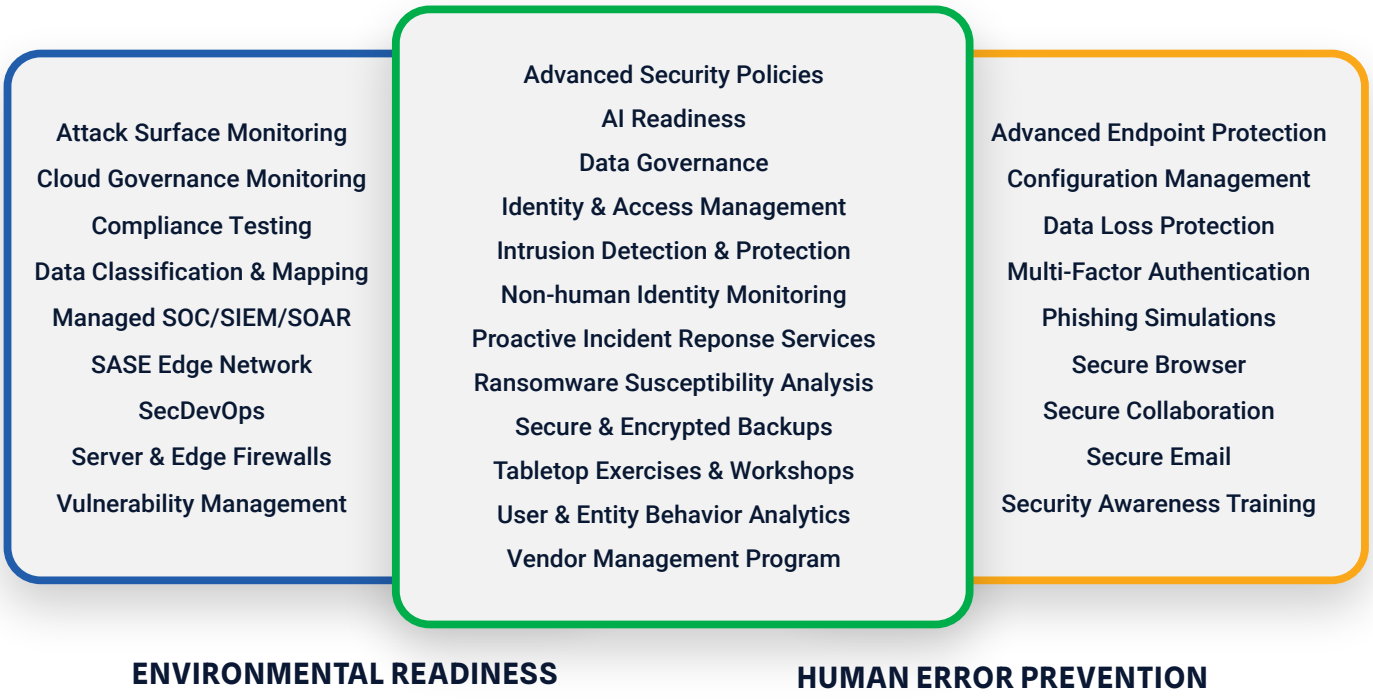
CORE OFFERINGS

BUILDING CYBER RESILIENCY

1. Perform a Comprehensive Risk Assessment
2. Create a Cybersecurity Governance Structure & Program
3. Establish Incident Response Plans
4. Set Up Encrypted Data Backups & Recovery Processes
5. Update & Patch Systems Every 2 Weeks
6. Develop a Culture of Employee Cybersecurity Awareness & Training
7. Review/Update Security Controls & Implement Strong Authentication Protocols
8. Continuous Monitoring 24x7x365
9. Institute Robust Vendor Management Practices
10. Carry Out Routine Cybersecurity Training & Drills

LAYERED APPROACH TO SECURITY

CyberSecOp continues its heritage focusing on assisting our clients on their needs and goals around Governance, Risk, and Compliance (GRC) but that journey requires a blended approach to truly manage risk, meet regulations, and operate ethically. A blended approach to security plays a crucial role in producing and preserving corporate value, achieving objectives, addressing uncertainty, and acting with integrity towards a common goal of minimizing Strategic, Operational, Financial, and Reputational Risks.



GOVERNANCE, RISK, & COMPLIANCE

- Improve Cybersecurity
- Align IT with Business Goals
- Make Informed Decisions
- Promote Operational Excellence
- Protect Reputations
- Protect Your Employees

PRAGMATIC SECURITY

- Minimize Risk
- Enhance Security Posture
- Perimeter & Endpoint Defenses
- Encrypted Backups in Flight & at Rest
- Network Micro-Segmentation
- Security Awareness Training

VCISO & CONSULTING SERVICES

Elevate Your Cybersecurity Posture with a Virtual CISO

CyberSecOp empowers organizations to navigate the complex and ever-evolving cybersecurity landscape with unparalleled confidence. We possess deep expertise across a wide range of industry standards, including NIST CSF, NIST 800-171, CMMC, FedRAMP, SOC II, ISO 27000 & 42001, CIS, GLBA, GDPR, NYDFS, PCC-DSS, HIPAA, HITECH, and FISMA. The Virtual CISO role encompasses the full spectrum of a Chief Information Security Officer, providing unparalleled leadership in safeguarding your organization's digital assets.

KEY RESPONSIBILITIES

01 DEVELOP A ROBUST CYBERSECURITY STRATEGY
Craft and implement a comprehensive Cybersecurity Strategic Plan, ensuring alignment with your business objectives and compliance with relevant regulations.

02 LEAD AND EMPOWER YOUR TEAM
Direct and mentor your internal security team and seamlessly integrate with CyberSecOp's expert consultants to deliver exceptional results.

03 FORGE A CULTURE OF COMPLIANCE, GOVERNANCE, & SECURITY
Establish and implement robust security policies and procedures, fostering a culture of security awareness across your organization.

04 PROACTIVE THREAT MITIGATION
Drive the development and implementation of effective remediation plans to address identified vulnerabilities and minimize risk.

05 NAVIGATE THE REGULATORY LANDSCAPE
Provide expert guidance on navigating the complex regulatory landscape, ensuring compliance with all applicable laws and regulations.

06 CHAMPION A CULTURE OF SECURITY
Lead and conduct security awareness training, including phishing simulations and tabletop exercises, to empower your employees to become part of your security defense.

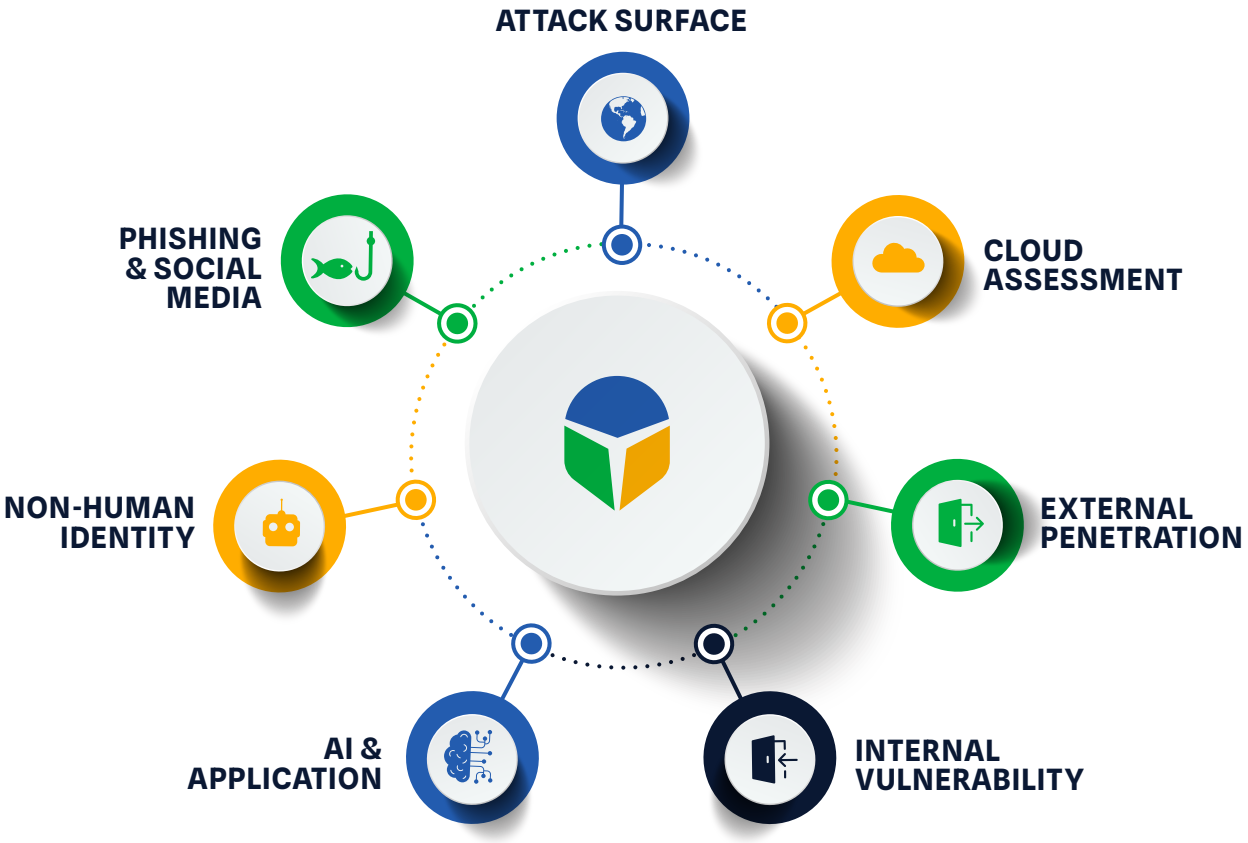
07 DRIVE CONTINUOUS IMPROVEMENT
Monitor the effectiveness of your cybersecurity program, conduct regular reviews, and implement continuous improvements to maintain a robust and resilient security posture.

COMPLIANCE & VULNERABILITY TESTING

Unleash the Power of Proactive Vulnerability Assessment with CyberSecOp

CyberSecOp empowers organizations to elevate their security posture through a comprehensive suite of Technical Testing services. Our cutting-edge vulnerability assessments provide deep insights into the effectiveness of your operating systems and third-party software patching, illuminating potential security gaps and weaknesses.

Furthermore, our advanced penetration testing employs sophisticated techniques to simulate real-world attacks, meticulously evaluating your defenses and assessing your organization's ability to detect and respond to threats. By combining our technical expertise with a deep understanding of your unique environment, we empower you to strengthen your security posture and minimize your risk by leveraging some of the following Scans:



By combining these powerful assessments, we provide a 360-degree view of your threat surface, identifying potential entry points and vulnerabilities. This comprehensive understanding empowers you to proactively address risks and strengthen your overall security posture.

RANSOM SUSCEPTIBILITY ANALYSIS

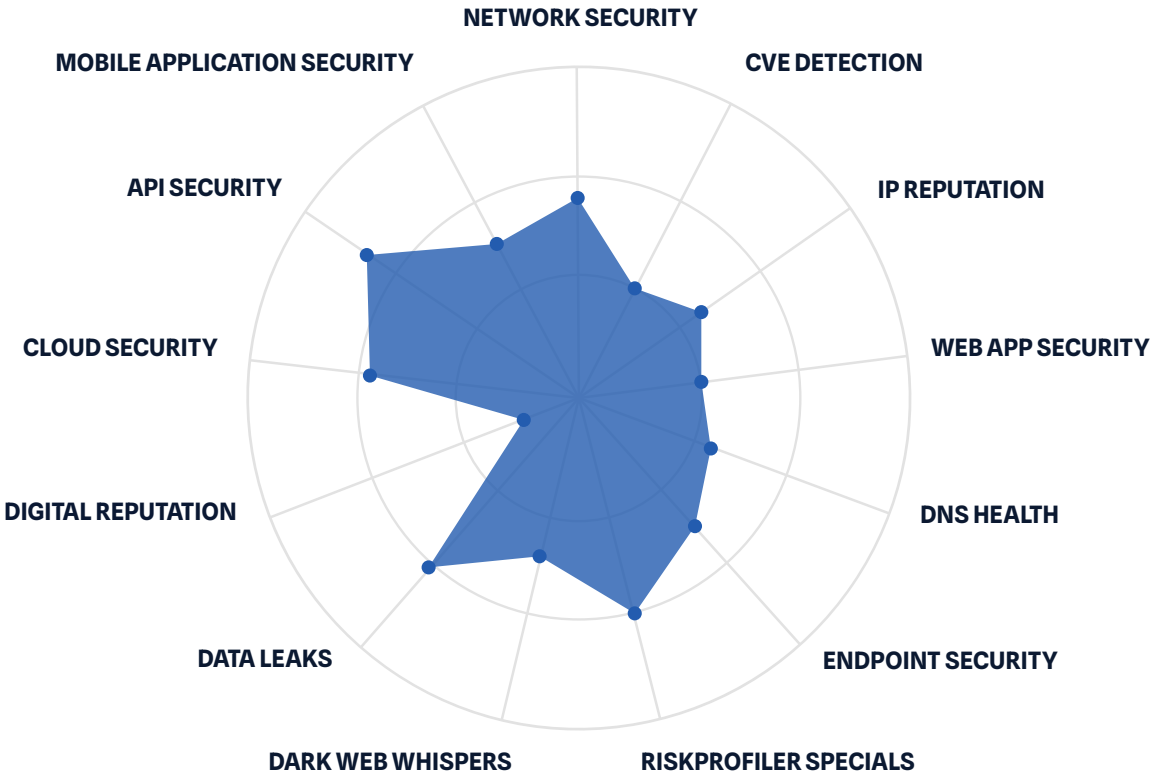
Through a combination of in-depth interviews, comprehensive questionnaires, and cutting-edge data analysis, we leverage proprietary algorithms to deliver a comprehensive cybersecurity analysis that pinpoints your organization's susceptibility to ransomware attacks.

Our analysis goes beyond traditional assessments, examining your organization's unique risk profile by:

- **Uncovering Hidden Vulnerabilities:** Identifying critical weaknesses such as unpatched systems, insecure network settings, and risky user behaviors (like falling victim to phishing scams).
- **Quantifying the Impact:** Assessing the potential financial impact of a ransomware attack, including ransom payments, recovery costs, loss of revenue, and the devastating impact on your reputation.
- **Benchmarking Your Security Posture:** Providing a unique security rating that benchmarks your organization against industry peers, highlighting key areas for improvement.

With our expert guidance and actionable insights, you can:

- Strengthen your defenses against cyber threats.
- Minimize the impact of a potential attack.
- Gain peace of mind knowing your organization is protected.



MANAGED SECURITY OPERATIONS CENTER (SOC)

Elevate Your Security Posture with CyberSecOp's Relentless Cyber Surveillance

Experience unparalleled security with CyberSecOp's Managed Cyber Surveillance, where our team becomes an extension of yours or yours alone. Our SOC Analysts provide 24/7 coverage, delivering a comprehensive suite of services, including:

SKILLED SIEM MANAGEMENT

Gain insightful visibility into your security landscape with our robust SIEM platform, enabling log collection, correlation, forensic analysis of security events, and adherence to compliance controls.

MANAGED DETECTION AND RESPONSE

AI powered, 24x7, comprehensive threat protection of your endpoints & cloud.

ADVANCED THREAT HUNTING

Expert cyber analysts combine the power of AI, machine learning, correlation, and real-time telemetry analysis to identify and neutralize hidden threats.

STREAMLINED INCIDENT RESPONSE

Swiftly identify, contain, and remediate security incidents via automated response and expert guidance from our security analysts.

MANAGED DATA LOSS PREVENTION (DLP)

Advanced data loss prevention that combines user behavior analytics, real-time monitoring, and automated responses to protect sensitive data from accidental or malicious exfiltration.

EXPERT VULNERABILITY MANAGEMENT

Proactively identify and mitigate vulnerabilities with cutting-edge scanning and expert analysis.

ADDITIONAL MANAGED SECURITY SERVICES: MFA, Email, SASE, and MDM

Experience integrated "Cybersecurity as a Service" with thousands of security professionals working in unison to protect your organization. We provide a cohesive platform where protection technologies, human expertise, 24/7 monitoring, and incident response are unified and delivered as a service and priced for mid-market budgets. This comprehensive approach ensures your organization is protected by a vast, dedicated security force, making sophisticated security operations accessible without the complexity and expense of managing technology and internal staff.

- Mature your security posture rapidly and at scale.
- Enhance your team's capabilities.
- Minimize risk and maximize your organization's resilience.

INCIDENT RESPONSE SERVICES

Fortify Your Organization's Resilience with CyberSecOp's Proactive Incident Response Program

A cyberattack can lead to severe consequences, including significant downtime, financial losses, legal and compliance issues, and long-lasting damage to your brand's reputation. Encrypted systems and data held hostage by cybercriminals are among the most daunting threats facing organizations today. CyberSecOp equips you to face these challenges head-on with confidence. Our comprehensive, proactive incident response and recovery services offer the peace of mind you need.

Rapid Managed Incident Response Retainer Services

- **World #1 according to Gartner Peer Review for Security Services:** Our extensive assessment and planning services prepare you for a worst-case scenario. We assist you in avoiding, managing, and recovering from damaging breaches, including handling negotiations in ransomware situations.
- **USA #1 according to Javelin Research for our Dedicated Team of Experts:** Our elite squad of cybersecurity, forensic, and legal professionals is always on standby, ready to implement your custom Incident Response playbook swiftly and effectively.
- **Meticulous IR Case Management:** We ensure thorough case management with detailed documentation and continuous support, guiding you through a smooth recovery process.
- **Proactive Improvement:** Post-incident, we perform a detailed analysis to pinpoint areas for enhancement, providing a strategic road map to bolster your cybersecurity resilience. Recommendations often include:
    - Dark Web Monitoring
    - Tabletop Workshops
    - Air-gapped and Encrypted Backups
    - Managed SOC Services like Managed Detection and Response (MDR), Data Loss Prevention (DLP), and 24/7 monitoring, all available from CyberSecOp.

By partnering with CyberSecOp, you're not just responding to incidents; you're fortifying your future against them. Let us help you turn cybersecurity challenges into opportunities for strengthening your organizational resilience.

THIRD PARTY RISK MANAGEMENT

Protect Your Organization with Comprehensive Cyber Third-Party Risk Management

In today's interconnected world, your organization's security is inextricably linked to the security of your third-party vendors. CyberSecOp offers a robust and comprehensive Third-Party Risk Management (TPRM) solution that empowers you to:

- **Identify and mitigate critical risks:** Proactively identify and assess potential vulnerabilities across your entire third-party ecosystem.
- **Enhance your security posture:** Continuously monitor vendor security postures and implement proactive remediation measures to safeguard your organization's data and operations.
- **Gain a competitive edge:** Navigate the complex landscape of third-party risk with confidence and ensure compliance with industry standards.

KEY FEATURES OF RISK COGNIZANCE TPRM

Comprehensive Vendor Assessment
Conduct thorough due diligence with our in-depth vendor assessment tools. Evaluate cybersecurity practices, compliance levels, and performance history to make informed decisions about third-party relationships.

Risk Categorization and Prioritization
Classify and prioritize vendors based on their risk profile and the criticality of their services. Our solution ensures that you focus resources and efforts on managing high-risk vendors effectively.

Continuous Monitoring and Review
Stay ahead of potential threats with continuous monitoring capabilities. Our platform provides real-time insights into third-party performance, security practices, and compliance status, helping you address risks proactively.

Robust Contractual Controls
Enhance vendor accountability with our integrated contract management features. Define cybersecurity requirements, service level agreements (SLAs), and risk management clauses directly within vendor contracts.

Incident Response and Communication
Be prepared with a comprehensive incident response plan. Our platform facilitates effective communication and coordination with vendors during security incidents, ensuring a swift and organized response.

Training and Awareness
Foster a security-conscious culture with our training and awareness programs. Equip your team with the knowledge and skills needed to manage third-party risks effectively.

AI & APPLICATION TESTING

Be Aware When Unlocking Growth with Generative AI

Navigating the exciting world of Generative AI requires a thoughtful and strategic approach. Concerns around data privacy, security, and bias often hinder organizations from realizing the full potential of this transformative technology. At the core of successful AI implementation lies a commitment to data security and responsible AI practices.

A strong focus on cybersecurity is paramount. By proactively addressing the potential for misuse by cybercriminals and implementing safeguards against malicious activities, you can unlock the true power of Generative AI while mitigating potential risks.

By prioritizing data classification & mapping, implementing robust access controls, and ensuring data quality, you can mitigate risks, maintain data integrity, and ensure the ethical and responsible use of AI within your organization. By adopting a strategic approach and prioritizing ethical considerations, you can position your organization for success in the age of AI.

Unlike traditional machine learning, which validates its knowledge against training data, newer AI models (Gen-AI/LLMs) lack self-verification. Their output requires user validation, making unsupervised use appropriate only when alternatives are unavailable, rigorous testing is complete, and some error is acceptable.

Given the widespread employee use of supervised AI like ChatGPT and Copilot, and the data-retention practices of standard licenses, enterprise-level control is crucial. A secure, enterprise-grade solution that avoids data storage and retention is essential to protect sensitive company information.

AI-driven automation requires model-provided confidence thresholds to ensure accuracy and enable human review when needed. Without these thresholds, the system cannot assess its reliability, leading to potential errors in critical systems and compromised data integrity.

Agentic AI empowers LLMs/Gen-AI to autonomously make decisions and access data, making data governance crucial. Robust access controls protect sensitive information and ensure data quality, ultimately enhancing the agent's competency and preventing security breaches.

Mitigation Strategies

Clear Policies: Set guidelines on what data can be fed into AI tools and which tools are approved.
Training: Educate employees on risks and best practices, like avoiding sensitive data input.
Access Controls: Use enterprise-grade AI platforms with robust security, logging, and data retention policies.
Monitoring: Track usage to spot unauthorized tools or suspicious activity.
Output Validation: Encourage double-checking AI-generated content before use.

Gartner Peer Insights Customers' Choice 2025

> *"CyberSecOp offers a rare combination of white glove service normally only seen in individual consultants or very small, boutique consulting firms (which charge double market price) along with the professionalism and experience you'd expect from a multi-national, large cyber security agency."*

> *"CyberSecOp is a customer-centric service provider. They value the business relationship they establish with you."*

> *"I have been extremely satisfied with the security services from CyberSecOp. During a stressful period of transition, they were able to seamlessly step in due to their extensive knowledge and experience in the IT and Cyber areas."*

★★★★★

Ranked #1 in Gartner Peer Insights

CyberSecOp

5 Hillandale Avenue
Stamford, CT 06902
www.CyberSecOp.com
Toll Free: 866-973-2677

Monday-Friday: 24 Hours
Saturday: 24 Hours
Sunday: 24 Hours