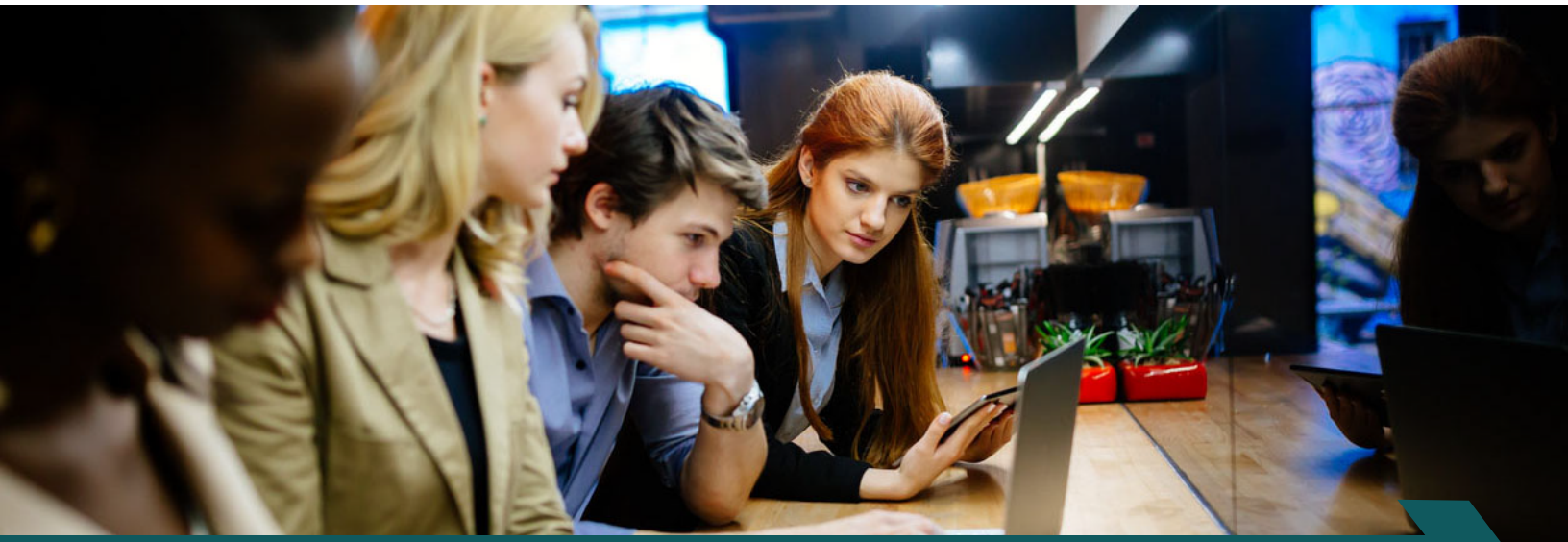
Gradient CYBER



Managed Risk and Threat Assessments

EXPECTED OUTCOMES: VALUE TO YOU

- Learn Where You Stand – See where your security posture stands today relative to known and identified vulnerabilities. And see what threats might be happening in your IT environment right now. Understand risks facing your organization today.
- Knowledge & Guidance to Confidently Act – Get a prioritized list of improvement projects to reduce cyber risks and threats and detailed guidance on possible solutions to consider.
- Improved Cybersecurity Posture – Improve cybersecurity readiness, reduce risk exposures, and increase cybersecurity based on implemented recommendations.
- Cyber Insurance Benefits – Use documented cybersecurity investments and improvements to negotiate cyber insurance savings or lower premiums.

972-532-1878
contact@gradientcyber.com
www.gradientcyber.com

Managed Risk Assessments and services delivered by the Gradient Cyber expert **Vector Security Team.**

The majority of all cyber-attacks happen to small businesses and midmarket enterprises. Thus, maintaining a hardened attack surface is critical. But identifying and managing security risks in the IT environment is difficult for IT and security teams to keep up with. Even maintaining basic asset inventories, patch levels, existing vulnerabilities, and configuration issues is challenging, much less prioritizing and addressing these attack surface weaknesses. But without addressing these issues continuously, the overall risk increases leaving companies ever more exposed to serious cyber-attacks.

THE GRADIENT CYBER SOLUTION

Introducing Gradient Cyber's Managed Risk and Threat Assessments! Working with our trusted Vector Security Team and SecOps Delivery Platform you can conduct a full one-time assessment of your IT environment including networks, endpoints, and cloud environments to identify your current cybersecurity strengths and weaknesses. Our proprietary technology-based risk and threat monitoring lets you work with our expert cybersecurity team to baseline your current cybersecurity state, benchmark against industry best practices and standards, and develop a prioritized plan to improve.

BASELINE

Document the current state of your IT environment attack surface with a technology-based risk and threat assessment analysis.

BENCHMARK

Find out where you stand and score your security practices and controls relative to best practice cybersecurity frameworks like NIST.

HARDEN

Get a full risk-based out-briefing with assessment findings and prioritized, recommendations to guide improvement efforts.

KEY DELIVERABLES: WHAT YOU GET

- **Severe Vulnerability Reporting** – If during the course of the assessment severe vulnerabilities are noted, Gradient Cyber will issue a Critical Vulnerability Alert immediately so the customer can perform validation and/or remediation efforts to limit continued exposure.

- **Mapping Vulnerability Criticality** – Gradient Cyber will assign a criticality rating to each finding of Critical, High, Medium, Low or Informational. The ratings are based on the risk to the customer and are determined by the access required, the technical difficulty to exploit, and the organizations' exposure if successfully exploited.

- **Document and Review of Findings** – At the conclusion of the assessment, Gradient Cyber will conduct an out-brief meeting with the customer to review the findings and to provide detailed recommendations for remediation of identified vulnerabilities and threats. Complete findings are provided in full at this time and include the scope of testing, identified listening services and applications along with risks associated with each, details of and risks associated with identified network layer vulnerabilities, details of and risks associated with identified web application vulnerabilities, and recommendations on remediation for each.

SOLUTION SCOPE: WHAT WE DO

Summary	Introductory Risk & Threat Assessment	Complete Risk & Threat Assessment
Cyber Risk Survey / Scoring	Full survey and scoring against a single framework.	Full survey and scoring against a single framework.
Vulnerability Scanning	External IP address ranges and corporate website.	External IP address ranges, corporate website, and internal IP address ranges.
Penetration Testing	External penetration test sampling.	External, internal, and application penetration testing.
Threat Monitoring	Network-based threat monitoring – one site.	Network, endpoint, and cloud-based threat monitoring.
Email Compromise Checks	Checks based on all corporate email domains.	Checks based on all corporate email domains.
Findings Review	One-hour technical team out-brief session.	One-hour technical team out-brief session and written report.

Summary	Introductory Risk & Threat Assessment	Complete Risk & Threat Assessment
Cyber Risk Survey / Scoring	Gradient Cyber will work with the customer to evaluate and score current security practices and controls against a leading industry standard / framework (e.g.; NIST, etc.) that provides customer with a go forward plan (roadmap) of what they need to do in order to improve their cyber / risk profile.	Gradient Cyber will work with the customer to evaluate and score current security practices and controls against a leading industry standard / framework (e.g.; NIST, etc.) that provides customer with a go forward plan (roadmap) of what they need to do in order to improve their cyber/risk profile.
Vulnerability Scanning	**External vulnerability scanning** - During the assessment, Gradient Cyber security professionals examine the results of automated vulnerability scanning / testing of external IP addresses and assess the risks that may be introduced as a result of the identified vulnerabilities. Using a proprietary database of application vulnerabilities with public sources of vulnerability information we analyze the collected data and detail resolutions. In addition, we classify each of the findings by criticality and provide an application reference to show where the finding was discovered, and when possible, how to repeat the attack.	**External and internal vulnerability scanning** - During the assessment, Gradient Cyber security professionals examine the results of automated vulnerability scanning / testing of external IP addresses and assess the risks that may be introduced as a result of the identified vulnerabilities. Using a proprietary database of application vulnerabilities with public sources of vulnerability information we analyze the collected data and detail resolutions. In addition, we classify each of the findings by criticality and provide an application reference to show where the finding was discovered, and when possible, how to repeat the attack.
Threat Monitoring	**Network-based threat detection** - The service includes 24/7, multi-stage threat detection including local network intrusion detection (IDS), external threat intelligence indicators of compromise / attack, data / behavioral analytics, machine learning threat detection techniques, and cyber analyst threat hunting and observation. This monitoring is conducted for a 2-week period.	**Network, endpoint, SaaS app, and cloud threat detection** - The service includes 24/7, multi-stage threat detection including local network intrusion detection (IDS), on-device endpoint threat detection (EDR), integrated cloud-based threat detection based on external threat intelligence indicators of compromise / attack and entity behavioral analysis, machine learning threat detection techniques, and cyber analyst threat hunting and observation. This monitoring is conducted for a 2-week period.
Email Compromise Checks	Gradient Cyber security analysts will conduct searches to quickly assess if company employee addresses for all corporate email domains may have been put at risk due to accounts having been compromised in previous data breaches.	Gradient Cyber security analysts will conduct searches to quickly assess if company employee addresses for all corporate email domains may have been put at risk due to accounts having been compromised in previous data breaches.

Summary	Introductory Risk & Threat Assessment	Complete Risk & Threat Assessment
Penetration Testing	**External penetration test sampling** is designed to evaluate public facing websites and applications infrastructure, provide guidance in resolving identified weaknesses, and provide recommendations for improvements.	**External penetration testing** is designed to evaluate public facing websites and applications infrastructure, provide guidance in resolving identified weaknesses, and provide recommendations for improvements. **And internal penetration testing** is designed to evaluate private network and applications Infrastructure, provide guidance in resolving identified weaknesses, and provide recommendations for improvements. Both include a complete scan of in-scope IP addresses provided without valid credentials. **And application penetration testing** of the application and related infrastructure is performed using a series of tools and manual procedures on the server(s) hosting the web application and on the application itself. In conducting application pen tests, Gradient Cyber employs methods outlined in the Open Web Application Security Project (OWASP) Testing Guide as well as best practices from other sources including the National Institute of Standards and Technology (NIST). The high-level testing steps include information gathering, business logic testing, authentication testing, session management, data validation testing, and API / web services testing (if required).
Findings Review	At the conclusion of the assessment, Gradient Cyber will conduct an out-brief meeting with the customer to review the findings and to provide detailed recommendations for remediation of identified vulnerabilities and threats. Complete findings are provided in full at this time and include the scope of testing, identified listening services and applications along with risks associated with each, details of and risks associated with identified network layer vulnerabilities, details of and risks associated with identified web application vulnerabilities, and recommendations on remediation for each.	At the conclusion of the assessment, Gradient Cyber will conduct an out-brief meeting with the customer to review the findings and to provide detailed recommendations for remediation of identified vulnerabilities and threats. Complete findings are provided in full at this time and include the scope of testing, identified listening services and applications along with risks associated with each, details of and risks associated with identified network layer vulnerabilities, details of and risks associated with identified web application vulnerabilities, and recommendations on remediation for each.

WHAT OUR CUSTOMERS SAY

"Great service, providing great insights and protection." - Security Administrator, Midsize Medical Group

"Gradient Cyber allows me to sleep a little better at night." - Director of Information Systems, State-Based Education

ABOUT US

Gradient Cyber is a trusted cybersecurity partner operating primarily across the United States and specializing in small and mid-market enterprises concerned about cybersecurity but lacking the staff to give it the attention it deserves. For a fraction of the cost of hiring one cyber analyst our cybersecurity team is on the job 24/7 to improve your security, so you don't have to think about it anymore. We'll tell you what you need to know, what needs to be done, and eliminate the noise. Gradient Cyber is the only SOCaaS partner improving your security using 24/7 cybersecurity expertise, a SecOps delivery platform for threat detection across your IT infrastructure 'swim lanes', and diagnostics to strengthen your security posture even when there are no threat alerts. Learn more at https://www.gradientcyber.com.