



## Extended Detection and Response (XDR)

### EXPECTED OUTCOMES: VALUE TO YOU

- Financially Feasible Security Expertise - A cost effective cybersecurity team for threat monitoring and response.
- 24/7 Cybersecurity Partner - A true partner on the job 24/7 protecting your business.
- Security Confidence - Peace of mind so you don't have to think about security 24/7.
- Helping Hand When You Need it Most - We are there with your team working to prevent cyber-attacks and responding immediately when threats appear.



212-363-1111  
info@derivetech.com  
www.derivetech.com

### 24/7 Threat Detection and Response for your entire IT infrastructure delivered by our **Vector Security Team**.

The majority of all cyber-attacks happen to small businesses and midmarket enterprises. When it comes to cybersecurity, these IT teams have the toughest job out there. They have to take care of everything IT-related - in addition to managing security. All too often there is no one dedicated to security – and even if there is, they can't work 24/7.

### THE GRADIENT CYBER SOLUTION

Introducing Gradient Cyber's Extended Detection and Response (XDR) Service! Now, for a fraction of the cost of hiring one cyber analyst, our trusted Vector Security Team can be on the job 24/7 to improve your security. We'll tell you what we find, what needs to be done about it, and eliminate the noise and false positives.

Gradient Cyber is the only security operations as a service (SOCaaS) partner working to improve your security with our 24/7 Vector Security Team; a cloud native, proprietary SecOps delivery platform for threat detection across all your IT infrastructure; and diagnostics to strengthen your security posture even when there are no threat alerts.

➤ HEALTH	➤ DETECT	➤ RESPOND	➤ RECOVER
<p>Managed monitoring of your cybersecurity health and expert guidance on making improvements.</p>	<p>Managed 24/7 threat detection and threat hunting by our security team across your infrastructure.</p>	<p>Managed threat response (confirm, triage, and analyze alerts) to quickly contain threats.</p>	<p>Managed updating of current protections based on lessons learned to prevent future recurrence.</p>

### KEY DELIVERABLES: WHAT YOU GET

- **Named Vector Security Team Members** – A Gradient Cyber team consisting of an account team leader, cyber analysts, senior cyber analyst, and service delivery support.
- **Technology and Tools** – State of the art technology and tools to enable a 24/7 security operations organization providing real-time cybersecurity coverage including but not limited to the SecOps Delivery Platform.
- **Methodology and Approach** – Tried and true security operations processes and methodologies that we constantly put to the test, making improvement continually.
- **Certified Cybersecurity Expertise** – Experienced Vector Security Team personnel that are highly trained and tested experts in their fields including cybersecurity and penetration testing among others.
- **24/7 Security Operations Coverage** – Redundant Vector Security Team locations and geographically diverse personnel to ensure 24/7 cybersecurity monitoring and uptime.
- **Fortified Security Operations Infrastructure** - Thoroughly tested and secured end-to-end data collection, analysis, and security information and event management.

### SOLUTION SCOPE: WHAT WE DO

Service Deployment	Gradient Cyber will deploy the service to the customer's specific IT environment including custom design, hardware and software deployment guidance, SecOps Delivery Platform access, and any necessary additional support.
Endpoint Security Data Monitoring	XDR for Endpoints (EDR) service includes endpoint security data and alert collection from a deployed endpoint detection and response (EDR) tool. Supported EDR tool list is available upon request.

## SOLUTION SCOPE: WHAT WE DO

Cybersecurity Health Evaluation	Gradient Cyber will work with customer on a detailed scoring of their current IT environment and risk profile based on known security frameworks (NIST, etc.) that provides them with a go forward plan (roadmap) of what is needed in order to improve the cyber/risk profile. The security team will also conduct customer health checks to discuss governance, risk, and compliance (GRC) and road mapping plans as well as Situation Report management and system training on a monthly basis.
Network Security Data Monitoring	The XDR for On-Premise Network Infrastructure service includes passive network security data collection and/or generation including bi-directional NetFlow data, firewall log data, network based intrusion detection data, and LDAP log collection.
Onsite Network Intrusion Detection	XDR for On-Premise Network Infrastructure service also includes on-site network intrusion detection (IDS) capabilities delivered in the Gradient Cyber Collectors. Network intrusion detection rulesets are wholly managed by Gradient Cyber.
SaaS Application Security Data Monitoring	XDR for SaaS Applications service includes SaaS application account and security data collection via API. Supported SaaS applications list is available upon request.
Cloud Infrastructure Security Data Monitoring	XDR for Cloud Infrastructure service includes cloud security data monitoring via API. Supported cloud platforms list is available upon request.
24/7 Monitoring and Support of the Entire IT Environment	The XDR service provides round the clock monitoring and support for rapid incident response to ensure minimum attacker dwell time and minimal attack impact on the customer's business. 24/7 security monitoring of the entire IT environment including on-premise network infrastructure, endpoints covered with an EDR tool, SaaS application environments, and cloud infrastructure.
Multi-Stage Threat Detection Ecosystem	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, on-going cyber analyst threat hunting and observation, and customer community-based sharing of observed threats.
Threat Intelligence	The XDR service includes proprietary curated threat intelligence to support effective threat detection and comprehensive threat prevention measures. Threat intelligence includes, but is not limited to, open source and commercial data feeds for malware, domain lookup, IP reputation, geo locations, and other information sharing.
Reduction of False Positives	Through the use of automated technologies and manual investigations, the Gradient Cyber team strive to eliminate 100% of false positives to keep customer resources focused solely on real security events.

## SOLUTION SCOPE: WHAT WE DO

Passive Incident Response	Gradient Cyber will investigate incidents, confirm findings, and provide incident response delivered through Situation Reports (Sitreps). The Sitreps include details for the event, investigation findings, priority, and recommended response actions for threat mitigation, containment, and to prevent further recurrence.
Active Incident Response	Available with "XDR for On-Prem Network Infrastructure - Active Response" and "XDR for Endpoints (EDR) Active Response". Cyber analysts will, in addition to passive event response, implement recommended response actions on customer's firewall(s) and or EDR tool for threat mitigation, containment, and to prevent further recurrence. The "XDR for On-Prem Network Infrastructure - Active Response" service also includes a full initial firewall rules audit.
SIEM Provision	The SecOps Delivery Platform provides for monitoring and analysis of all identified security-related events and can be used in place of and in addition to an existing SIEM.
Security Status Reporting	The XDR service includes regular security status reporting to enable customers to ensure that all necessary security controls and processes are implemented and working effectively to defend against relevant threats.
Secure Data Transfer	The service ensures that the data in transit to and from customer sites for analysis is encrypted and secured against unauthorized access.
Regular / Monthly Cybersecurity Interactions	The XDR service includes regular interaction and monthly security checkups with internal security teams where they exist. This is to ensure coordinated and effective defense actions and to help improve internal capabilities through greater understanding of the threat environment.
Support for Business Leaders	The XDR service includes regular interaction with business leaders to ensure security capabilities support business objectives, and that business leaders have the understanding they need to make strategic security investments.
Asset Discovery	The XDR service includes continuous monitoring of asset communications thereby discovering assets on the network. The service is not to be considered a replacement for a comprehensive on-going asset management program.
SecOps Delivery Platform / Portal	The XDR service includes access to the Gradient Cyber cloud-based SecOps Delivery Platform for tracking Cybersecurity Health Scorecard improvement, detecting security threats, monitoring threat alerts, conducting alert investigations, conducting manual threat hunting, and accessing Gradient Cyber situation reports and remediations.
Extended Data Retention	Gradient Cyber retains 14 days of all customer collected security data including Netflow and IDS data to enable analysts to conduct proper and historical digital forensic investigations. This prevents sophisticated attackers from removing historical log/SIEM data in order to hide their tracks. Optional log retention, up to 1-year, is available to support customer best practices or regulatory requirements.

## WHAT OUR CUSTOMERS SAY

“With Gradient Cyber we have deeper visibility into what happens on our network and are able to react quickly to attacks and exploits thanks to them.” - CIO, Multinational Industrial Company

“The cost is worth it, there is no better value I’ve seen out there for the level of protection you get.” - IT Manager, Texas Petroleum Distributor

## 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>.

Derive Technologies is a Minority-Owned Business Enterprise (MBE) and a brand-agnostic full-service IT integrator aligned with best-of-breed technology to optimize and empower your IT environment.

### Contact Us

[www.derivetech.com](http://www.derivetech.com) | (212) 263-1111 | [info@derivetechnology.com](mailto:info@derivetechnology.com)  
40 Wall Street, 20th Floor, New York, NY 10005, US