

CYBER PROTECTION SERVICES

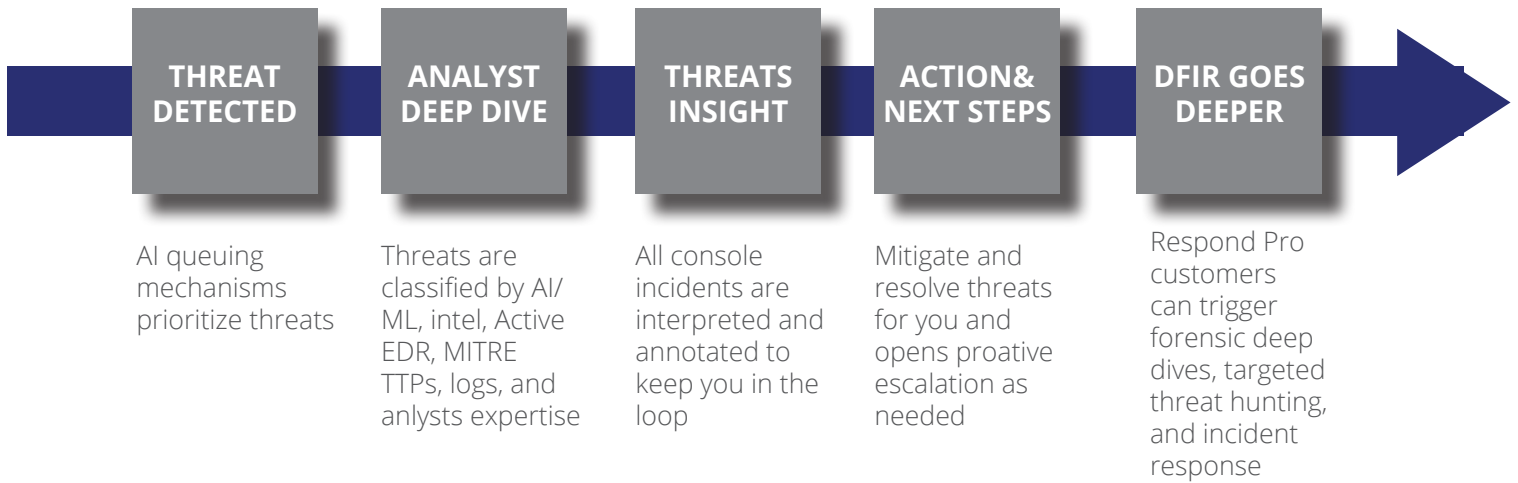
We provide cybersecurity protection services that range from assessments, continuous managed security services, to on-call incident response, when you need it most. We bring the technology, expertise, and focus to address today's gaps and the cyber details needed to protect businesses.

DETECTION & RESPONSE

MANAGED SECURITY

This Respond and Respond Pro Managed Detection and Response (MDR) service brings together SentinelOne with an expert MDR team providing the human side to the AI-based Singularity™ platform. We are here to augment security teams at organizations from a second set of eyes on SentinelOne deployment and then to appropriate responses to contain threats.

HOW MDR WORKS



WE STAND OUT

PROVIDING BEYOND THE BASICS

DIGITAL FORENSICS

**QUALIFY FOR CYBER
INSURANCE
COVERAGE**

**RANSOMWARE
WARRANTY**







**INCIDENT RESPONSE
PACKAGES**

Growing businesses have a lot on the line, we provide options so you can obtain full cyber protection. Add to our base service, incident response service (as a monthly retainer of expert hours), and quality digital forensics providing the details for cyber claims and pursue litigation if necessary. Those using this service will qualify for cyber insurance coverage by design.

QUARTERLY VULNERABILITY SCANNING

By providing insight and valuable intelligence around all your vulnerabilities, you only fix what you truly need to fix. The vulnerability scan data collected is actively mapped against active Internet threats. We provide the data-driven details on what are the most important vulnerabilities to patch. This can be performed from an external perspective, where we view your business like a hacker would, or from an authorized internal scan. Internal scans focus on maintaining a strong foundational security framework.

CYBER PROTECTION PACKAGE

		WHAT'S INCLUDED
24X7 MDR		<ul style="list-style-type: none">• Console threats reviewed, acted upon, and documented• Full response capabilities• Proactive notifications
WATCHTOWER		<ul style="list-style-type: none">• Intelligence based hunting, global APT campaigns, and emerging cyber crimes feed into the console where threats are reviewed and assessed• Threat bulletins and alerting when threats are detected in your environment
THREAT RESPONSE SLA		<ul style="list-style-type: none">• The fastest MDR on the planet• Analyst triage, verdict, and take initial actions
DIGITAL FORENSICS ANALYSIS		<ul style="list-style-type: none">• Full investigation: Infection vector, breach determination, intel-driven hunting, threat intel enrichment & contextualization, malware reversing, memory analysis and code extraction, malicious code de-obfuscation• Triage: console indicator and dynamic analysis
IR RETAINER		<ul style="list-style-type: none">• 10 Retainer hours (use or lose)• Investigation, Active Containment, Eradiction, and Reporting• Assigned IR case managers• 4-hour min. charge per incident
VULNERABILITY MANAGEMENT QTLY SCANNING		<ul style="list-style-type: none">• Consultation guiding long-term remediation and security architecture• Agent version alignment and exclusion reviews• Threat/actor trends

ADD-ON SECURITY OPTIONS

We deliver results for your business and additional services that scale to your needs

SECURITY CONTROL ASSESSMENT

This assessment looks at security controls across your organization to assess their current state, effectiveness, and how they are managed. We'll assist in helping you understand the gaps in protecting your sensitive information and where your next investment should be to get to an acceptable and industry expected level of control.

SECURITY OPERATIONS CENTER (SOC) SERVICES

Augment your security team with 24x7x365 security operations monitoring and handling security alerts and incidents on your behalf. Managing firewall and other IT systems against disruption and security events.

SECURITY AWARENESS TRAINING

Turn your employees into a strong last line of defense against today's cyber attacks. Security awareness training helps to change behaviors and reduce risk at every level of your business.

MULTI-FACTOR AUTHENTICATION

Protects users from an unknown person that tries to access their data such as personal ID details or other sensitive data. When implemented a user must provide two or more pieces of evidence to verify their identity in order to gain access to an app or digital resource. This level of MFA protects against hackers by verifying that digital users are who they say they are.

