

# Cyber Defense Management

# 360°

## Managed Security Operations Center (SOC)

*Powered by CrowdStrike Falcon® LogScale*

Building a mature security operations center is a daunting task for many organizations. It requires untangling an alphabet soup of acronyms to make smart investments in the right tech stack; developing programs for monitoring, investigation, response, detection engineering and more; and hiring the right people to staff it 24/7/365. The costs can easily run into millions of dollars, and most organizations take months or years to get it right.

Few organizations have the luxury of time or budget to do this on their own, particularly given the rapid pace with which the threat landscape changes. Many are stuck in a reactive loop, continuously fighting yesterday's battles, while the adversary continuously shifts and adapts.

To succeed, organizations must break out of this cycle and transition security operations from reactive to predictive defense. Fortunately, the path is clear, but it requires a consistent approach that many organizations struggle to complete.

### KEY BENEFITS OF CYBER DEFENSE MANAGEMENT 360°

#### **Reduce costs**

Consolidate tools and vendors with a managed SOC that delivers visibility across your full security stack including Falcon® and non-Falcon® solutions

#### **Minimize the attack surface**

White glove service manages deployment, configuration, tuning, and optimization of Falcon® LogScale to meet your unique requirements

#### **Gain expertise 24/7**

Reveald's Cyber Fusion Center provides around-the-clock monitoring and response to cyber threats, ensuring you're never caught off guard.

## Break Free from Reactive Defense with CDM360°

Reveald's Cyber Defense Management 360° (CDM360°) subscription service provides managed security operations powered by Falcon® LogScale. The experts in Reveald's Cyber Fusion Center deliver triage, investigation, and response to cyber threats, as well as management, monitoring, and tuning. Built on the Epiphany intelligence platform, CDM360° gives organizations a fast path to mature endpoint protection, and a clear path to predictive defense.

### Capabilities of Cyber Defense Management 360°, powered by CrowdStrike Falcon® LogScale

<b>Onboarding and Planning</b>	Collaborate closely with the Reveald Fusion Center to collect critical context on your business and environment, and establish key use cases and metrics for the Reveald partnership.
<b>Deployment and Configuration</b>	Provision LogScale, establish connectivity with necessary data sources, and implement detection rules.
<b>Triage and Investigation</b>	Expert alert triage and investigation, to understand emerging threats and develop a plan of action, fast.
<b>Notification</b>	Real-time notifications and detailed incident reports provide you with the context and information you need to understand and act against emerging threats. Insights are delivered through multiple channels, including directly within the Epiphany console.
<b>Tuning and Optimization</b>	Ongoing health checks ensure that your data pipeline is operating cleanly and LogScale continues to be properly configured for optimal defense.
<b>Reporting and Collaboration</b>	Regular reporting and review meetings ensure all stakeholders are properly informed and armed to make better decisions.
<b>Troubleshooting and Support</b>	Reveald partners closely with you to ensure any issues are tracked closely and resolved quickly.

### A Clear Path to Security Maturity

Reveald's subscription services are crafted to guide organizations who have standardized on the CrowdStrike platform to walk a predictable, repeatable path to security maturity.

Prepare	Optimize	Predict & Prioritize
<b>Endpoint Defense Management 360°</b> Powered by CrowdStrike Falcon® Complete Managed Detection and Response (MDR)		<b>Continuous Exposure Management 360°</b> Continuous Threat Exposure Management (CTEM)
<b>Cyber Defense Management 360°</b> Powered by CrowdStrike Falcon® Logscale Managed Security Operations Center (SOC)		

### ABOUT REVEALD

Reveald guides organizations along their journey from reactive to proactive defense. Reveald's AI-driven Epiphany Intelligence Platform™ empowers security teams to break free from existing reactive processes by leveraging Continuous Threat Exposure Management (CTEM), supported by the expertise to guide them on every step of the journey. Known for its innovative and proactive approach to cyber threats, the company is powered by a client-first approach, prioritizing risk mitigation and operational efficiency. **To learn more, visit [reveald.com](https://reveald.com)**