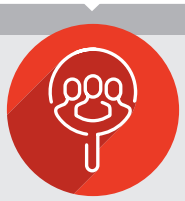
CROWDSTRIKE

# CROWDSTRIKE FALCON OVERWATCH STANDARD AND PREMIUM

GET THE LEVEL OF PROACTIVE HUNTING RESPONSE BEST SUITED TO YOUR NEEDS



## GOING ABOVE AND BEYOND ALERTING

CrowdStrike® Falcon OverWatch™ managed hunting offers the expertise of an elite group of cyber intrusion detection analysts and investigators, all dedicated to proactively hunting for adversary activity in your environment and on your behalf 24/7. The Falcon OverWatch team hunts for subtle signs of attack and alerts you when it identifies adversary activity. The OverWatch **Standard** and **Premium** offerings allow you to choose how you want to respond to incidents, with response levels ranging from email alerts to escalating notifications until an appropriate contact in your organization is reached. The OverWatch response process adheres to the following guidelines:

- **Delivering detailed actionable alerts —** OverWatch provides actionable alerts that include recommendations for remediation. The alerts are individualized, providing the detailed analysis you need to understand what happened and how to respond to the incident.

- **Discussing alerts with an analyst —** In response to an OverWatch-generated email notification, you have the option to reply with follow-up questions and may discuss your case in more detail with an analyst, if necessary.

## KEY BENEFITS

» Threat Hunting — Proactively hunts for threats in your environment on a 24x7x365 basis, eliminating false negatives

» Alert Prioritization — Uniquely pinpoints the most urgent threats in your environment and resolves false positives

» Guided Response — Threat hunters partner with your security operations team to provide clarity on an attack and guidance on what to do next

» Standard & Premium Levels — Choose the level of response that meets your requirements

# LEVELS OF OVERWATCH SERVICES

## OVERWATCH STANDARD

- **Ensure 24/7 operational readiness —** OverWatch identifies and stops more than 15,000 breach attempts a year, thanks to the expertise gained from daily "hand-to-hand combat" with sophisticated adversaries.
- **Provide 24/7 protection against the stealthiest attacks —** OverWatch has your back, hunting down subtle signs of attack to identify stealth attackers quickly and stop them. They also detect security incidents that are lurking, stopping them before your organization is compromised.
- **Built on the Falcon platform —** OverWatch seamlessly integrates with the powerful Falcon platform, processing over 60 billion events per day.
- **Provide email notifications —** The OverWatch team will alert you via email within moments of a detection.

## OVERWATCH PREMIUM

- **Ensure you never miss an OverWatch alert —** Provides "closed loop" communication, with proactive 24/7 follow-up calls in the event of a detection, ensuring that critical alerts don't go unnoticed.
- **Offer expert advice when you need it most —** Includes the option of engaging directly with a CrowdStrike OverWatch expert who can provide the guidance and expert advice you need to understand your situation and how to respond.
- **Access security expertise, anytime —** Elevates your security team efficiency and proficiency by providing the expertise, assistance, optimization and knowledge your security team wants and needs.
- **Proactively improve your security posture —** Ensure optimal protection with health checks, security briefings and recommendations, and proactive configuration of Falcon endpoint protection.

# FLEXIBLE OFFERINGS TO MEET YOUR SPECIFIC NEEDS

| | STANDARD | PREMIUM |
|---|---|---|
| 24/7 THREAT HUNTING | ● | ● |
| EMAIL ALERTS | ● | ● |
| CLOSED LOOP COMMUNICATION | | ● |
| OVERWATCH REPORTS | | ● |
| PROACTIVE CONFIGURATION | | ● |
| PREVENTION HEALTH CHECKS | | ● |
| OVERWATCH ONBOARDING | | ● |
| QUARTERLY BRIEFINGS AND SECURITY RECOMMENDATIONS | | ● |
| ACCESS TO OVERWATCH THREAT RESPONSE ANALYST | | ● |

CROWDSTRIKE

**CrowdStrike** is the leader in cloud-delivered next-generation endpoint protection. CrowdStrike has revolutionized endpoint protection by being the first and only company to unify next-generation antivirus, endpoint detection and response (EDR) and a 24/7 managed hunting service — all delivered via a single lightweight agent.

Learn more at **crowdstrike.com**