CrowdStrike Products

FALCON OVERWATCH ELITE

Understand threats, optimize defenses and improve response times by augmenting managed threat hunting with assigned analyst support

DRIVE SECURITY MATURITY

Falcon OverWatch™ is CrowdStrike's managed threat hunting service built on the CrowdStrike Falcon® platform. OverWatch augments the powerful autonomous protection provided by Falcon with deep and continuous human analysis, 24/7, to relentlessly hunt for anomalous or novel attacker tradecraft.

Falcon OverWatch Elite extends the standard OverWatch offering by introducing an assigned threat response analyst to help your organization both understand the threats that are most likely to target it and how best to prepare and respond to them. The OverWatch Elite analyst provides dedicated expertise, tactical day-to-day insights into your organization's threat landscape and strategic advisory to help drive continuous improvement.

What Customers Say

"CrowdStrike found the issue, mobilized immediately and got us back to a point where we had no data loss, no major issues and were able to continue normal operations in 24 hours."

Michael Sherwood,
Chief Innovation Officer, City of Las Vegas

KEY BENEFITS

FOCUS ON WHAT MATTERS MOST: Assess your organization's threat risks from a new angle with personalized guidance from assigned analysts with years of diverse expertise

RESPOND WITH SPEED AND CONFIDENCE: Quickly understand threats in your environment through proactive outreach, telecommunications, and highly tailored responses

IMPROVE CONTINUOUSLY: Get expert coaching, threat updates, industry-focused data and insights to drive improved maturity across your security team

KEY CAPABILITIES

PERSONALIZED THREAT HUNTING EXPERTISE

- **Assigned analyst:** Build an ongoing relationship with your OverWatch Elite threat response analyst.
- **New perspectives:** Assess your risks from a new angle with the help of analysts with years of diverse expertise.
- **Laser focus:** Develop a shared understanding of your organization's unique structure and requirements.

TACTICAL THREAT HUNTING INSIGHTS

- **Tailored threat hunting:** Develop, operationalize and tune your threat hunting program.
- **Advanced investigation support:** Gain deeper understanding of threats observed by the OverWatch team in your environment.
- **Fast, closed-loop communications:** Get on-demand access to expertise via multiple channels, including email and Slack.
- **Proactive outreach:** Be contacted about critical, active threats that are not acknowledged by your organization within the first 60 minutes.

STRATEGIC THREAT HUNTING ADVISORY

- **Expert coaching:** Develop your personalized plan for uncovering threats likely to target your organization.
- **OverWatch Elite threat hunting reports:** Review your security posture and gain hunting insights relevant to your industry.
- **"From the eyes of OverWatch" briefings:** Access exclusive quarterly webcasts to review emerging shifts in adversary tactics, techniques and procedures (TTPs) — informed by recent real-world intrusions — and discuss best practices for hunting and defense.

24/7 PROACTIVE THREAT HUNTING

- **Attacker mentality:** Effective threat hunting requires the ability and expertise to think like an attacker.
- **Cross-disciplinary expertise:** OverWatch employs elite experts from a wide range of backgrounds, including government, law enforcement, commercial enterprise, the intelligence community and defense.
- **Continuous vigilance:** When a sophisticated intrusion occurs, time is critical. Your adversaries do not sleep and are not restricted by time zones or geography — and neither should your threat hunting team.
- **Finely tuned response:** OverWatch identifies and responds to hundreds of potential breaches per week. Each threat handled helps team members fine-tune their skills and processes, ensuring that they are always sharp and effective.

CLOUD-SCALE SECURITY TELEMETRY

- **Tools for the hunt:** Threat hunting requires more than just expert hunters — those hunters need the right tools. Falcon OverWatch uses patented tools to hunt at scale across vast amounts of data and identify the faintest trace of an intrusion in near real time.
- **Real-time visibility:** Falcon OverWatch takes advantage of the cloud-scale telemetry of the proprietary CrowdStrike Threat Graph® to get broad and deep visibility delivered in real time.
- **Massive data:** CrowdStrike's Security Cloud ingests trillions of events every day, giving Falcon OverWatch an extensive, global view of threat activity as it happens in real time.

UP-TO-THE-MINUTE THREAT INTELLIGENCE

- **Threat context:** Understanding the threat is key to proactive and hypothesis-driven hunting.
- **CrowdStrike threat intelligence:** CrowdStrike intelligence empowers OverWatch with detailed, always-current knowledge of tradecraft from more than 160 adversaries.
- **Current TTPs:** Intimate knowledge of the latest TTPs in use today ensures that OverWatch is able to hunt effectively and efficiently.

INTEGRATED EXTENSION OF YOUR TEAM

- **Gained operational efficiencies:** OverWatch hunters sift through the noise so that your team doesn't have to. Hunters deliver high-fidelity alerts augmented with contextual details and global insights to help organizations' security teams understand threats and act faster.
- **Cost-effective coverage:** Implementing the continuous coverage that OverWatch provides as an in-house function would require a minimum staffing investment of five highly skilled full-time threat hunters.

SEAMLESS PART OF THE FALCON PLATFORM

- **One team, one fight:** OverWatch operates as an extension of the Falcon platform and your team, delivering timely threat information via the single cloud-native console.

THE FALCON OVERWATCH ELITE ADVANTAGE

Falcon OverWatch detects and disrupts sophisticated threats by leveraging the power of human ingenuity combined with cloud-scale data to hunt relentlessly for advanced attacks that can otherwise go undetected. Across the millions of endpoints in the Falcon community, OverWatch uncovers new and advanced tradecraft every day. There are two offerings to meet the unique needs of your organization.

Capabilities	Falcon OverWatch	Falcon OverWatch Elite
Visibility and Telemetry		
Real-time visibility	✓	✓
Global threat visibility	✓	✓
Immunity by community	✓	✓
Specialized data, tools and processes	✓	✓
24/7 Human Expertise		
Hypothesis-driven threat hunting	✓	✓
Continuous vigilance	✓	✓
Cross-disciplinary expertise	✓	✓
Intelligence-led threat hunting	✓	✓
Tactical Collaboration		
Alerts augmented with context	✓	✓
Email threat notifications	✓	✓
Personalized onboarding		✓
Response advice, advanced investigation and contextual support		✓
Two-way communications via Slack and email		✓
Proactive, closed-loop communications		✓
Strategic Insights		
Quarterly threat hunting reports	✓	✓
Threat hunting and investigation coaching		✓
Tailored threat reports and briefings		✓
OverWatch Elite global insights		✓

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform enables customers to benefit from rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more:
https://www.crowdstrike.com/

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Start a free trial today:
https://www.crowdstrike.com/free-trial-guide/