CROWDSTRIKE

FALCON OVERWATCH ELITE

An extension of CrowdStrike's global 24/7 threat hunting operations, providing tailored threat hunting, unique attack insights and specialized, hands-on expertise and support

CROWDSTRIKE THREAT HUNTING TAILORED TO YOU

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

Falcon OverWatch Elite extends the standard Falcon OverWatch offering by introducing an assigned threat response analyst to expertly contextualize the targeted and emerging adversarial tradecraft impacting the customer organization, and to determine effective measures for the customer to best prepare and defend against even the stealthiest and most advanced adversaries in operation today. Your assigned Falcon OverWatch Elite analyst provides deep expertise, tactical day-to-day insights into your organization's threat landscape and strategic advisory to help drive continuous improvement.

What Customers Say

"CrowdStrike [Falcon OverWatch] 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 an assigned analyst who has 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 threat hunting coaching, receive unfolding attack updates and review industry-focused data and insights to keep pace with the evolving threat landscape — including identity-based attacks — to improve maturity across your security team

KEY CAPABILITIES

PERSONALIZED THREAT HUNTING EXPERTISE

- **Assigned analyst:** Build an ongoing relationship with the Falcon OverWatch Elite threat response analyst assigned only to you and a limited number of additional customers.
- **New perspectives:** Use tailored threat hunting insights to assess existing controls and design purposeful countermeasures with a trusted analyst who knows your organization's requirements and restraints.
- **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 with unique visibility and telemetry at unprecedented scale.
- **Proactively hunt identity-based attacks:** Outpace adversaries by bringing the most experienced Falcon OverWatch threat hunters to the identity attack surface. These threat hunters' capabilities are powered by world-class threat intelligence, augmented by AI and aided by patented hunting techniques.
- **Custom investigation support:** Request custom hunts to gain an even deeper understanding of the threats and adversary tradecraft affecting your environment.
- **Fast, closed-loop communications:** Get on-demand access to expertise via multiple channels, including email and Slack.
- **Proactive escalation:** If you miss a critical alert and don't acknowledge it within 60 minutes, Falcon OverWatch Elite begins contacting you directly and repeatedly to ensure you're informed of the new severe threat impacting your organization.

STRATEGIC THREAT HUNTING ADVISORY

- **Expert coaching:** Work side-by-side with experienced threat hunting experts to develop your personalized plan for tailored threat hunting at your organization.
- **Falcon OverWatch Elite threat hunting reports:** Use your tailored threat hunting reports to identify and close gaps in your environment and to reduce your attack surface against advanced adversaries and targeted attacks.

24/7 PROACTIVE THREAT HUNTING

- **Attacker mentality:** Effective threat hunting requires the ability and expertise to think like an attacker.
- **Cross-disciplinary expertise:** Falcon OverWatch Elite employs highly skilled experts from a wide range of backgrounds, including government, law enforcement, commercial enterprise and the intelligence community.
- **Continuous vigilance:** When sophisticated intrusions occur, time is critical. Your adversaries don't sleep and aren't restricted by time zones or geography — and neither can your threat hunting team. Falcon OverWatch Elite is backed by a global team of threat hunters providing around-the-clock threat hunting coverage.

CLOUD-SCALE SECURITY TELEMETRY

- **Massive data:** The CrowdStrike® Security Cloud regularly ingests trillions of events every day, giving Falcon OverWatch a global view of threat activity at unprecedented scale.
- **Real-time visibility:** Falcon OverWatch takes full advantage of the cloud-scale telemetry processed by the proprietary CrowdStrike Threat Graph®, giving threat hunters the extensive and deep real-time visibility they need to detect and disrupt today's advanced attacks.
- **Tools for the hunt:** Threat hunters can't simply rely on their skills and experience — they need the right tools too. Falcon OverWatch Elite leverages patented and proprietary tools to hunt threats at scale across vast amounts of data and to identify even faint traces of stealthy intrusions.

UP-TO-THE-MINUTE THREAT INTELLIGENCE

- **Threat context:** Understanding the adversary is essential to proactive and hypothesis-driven threat hunting — which is why Falcon OverWatch maintains intimate knowledge of the latest TTPs to ensure the team hunts efficiently and effectively.
- **CrowdStrike threat intelligence:** CrowdStrike intelligence powers Falcon OverWatch Elite with detailed, always-current knowledge of tradecraft and IOCs for more than 180 adversary groups, ensuring holistic and accurate hypothesis-led threat hunting.

SEAMLESS EXTENSION OF YOUR TEAM

- **Gained operational efficiencies:** Falcon 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 your team understand threats and act faster.
- **Cost-effective coverage:** Standing up your own internal 24/7 threat hunting operation, like Falcon OverWatch, would require a minimum staffing investment of several skilled full-time threat hunters.
- **One team, one fight:** Falcon OverWatch operates as an extension of the Falcon platform and your team, delivering timely threat alerts and insights to you via the Falcon console.

THE FALCON OVERWATCH ELITE ADVANTAGE

Falcon OverWatch Elite tailors the standard Falcon OverWatch experience for organizations seeking deeper, contextualized threat hunting analysis, insights and support. Engage directly with assigned Falcon OverWatch Elite experts. Hone your understanding of emerging and novel attacks targeting your organization. And master the critical steps to hunt, respond and defend against these advanced threats yourself. Learn more about the advantages of Falcon OverWatch Elite in the chart below.

Capabilities	Falcon OverWatch	Falcon OverWatch Elite
24/7 Threat Hunting Vigilance		
Global, 24/7 human-led operations	✓	✓
Relentless vigilance	✓	✓
Cutting-edge processes and tooling	✓	✓
Telemetry at unprecedented scale	✓	✓
Cross-disciplinary expertise	✓	✓
Integrated IOCs and threat intelligence	✓	✓
Tactical Hunting Collaboration		
Actionable alerts with detailed context	✓	✓
Personalized guidance, insights and support		✓
Frictionless two-way communications		✓
Identity threat hunting capability*		✓
Monthly hunting exchanges		✓
Expert advisory and coaching		✓
Strategic Hunting Insights		
Quarterly hunting reviews		✓
Tailored hunting assessments and reports		✓
Falcon OverWatch Elite threat hunting library		✓

*Customers must have CrowdStrike Falcon OverWatch Elite and CrowdStrike Falcon® Identity Threat Detection or Identity Threat Protection to take advantage of the new capability.

Add a Falcon OverWatch Elite Analyst Dedicated to You

If you anticipate heavy threat hunting volumes and mounting requests for tailored hunts and analysis, ask us about **Falcon OverWatch Elite Dedicated Analyst.** With this option, you get your very own Falcon OverWatch Elite analyst who is embedded with and fully dedicated to your organization, your priorities and your requests.

Your dedicated Falcon OverWatch Elite analyst works in lockstep with you and your team to conduct tailored threat hunts, load-balance assignments and investigations, and take on other one-off threat hunting tasks you throw their way — all while they leverage the advanced threat hunting resources, tooling and proprietary tradecraft of the CrowdStrike Falcon OverWatch team.

Start Free Trial
of Next-Gen AV

Learn more at **www.crowdstrike.com**

ABOUT CROWDSTRIKE

CrowdStrike (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/