CROWDSTRIKE

The Universal Need for Threat Hunting

SIX COMPONENTS FOR EFFECTIVE THREAT HUNTING

If your organization was the target of a cyberattack, how quickly would you know?

The CrowdStrike Falcon OverWatch™ team's most recent threat report, *2021 Threat Hunting Report: Insights From the Falcon OverWatch Team*, reveals that organizations have just 90 minutes to detect an attack before a cybercriminal begins expanding their foothold in the organization.

As companies increasingly shift to the cloud and rely on a distributed, remote workforce, protecting the organization has become far more complex. Businesses must develop an **advanced threat hunting program**, a next-generation threat detection capability to pinpoint cyber threats that have been carefully crafted to circumvent traditional security measures.

What Is Threat Hunting?

Threat hunting is the practice of proactively searching for cyber threats that are lurking in a network. Cyber threat hunting digs deep to find undetected malicious actors in the environment that have stealthily evaded initial endpoint security defenses.

Takeaways From Our Falcon OverWatch Threat Hunters

60%
increase in interactive intrusion activity from July 2020 to June 2021

68%
of detections in Q2 2021 were not malware-based

92 minutes
is the average breakout time for eCrime attacks

What Hackers Are After

Data

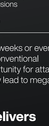
Intellectual Property

Customer Information

Introducing SEARCH: CrowdStrike's Threat Hunting Methodology

SEARCH Methodology:
Six Steps to Better Protection

1 SENSE

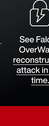


Leverage broad and deep telemetry that captures a wide range of activity and behaviors to establish the foundation for the organization's threat hunting efforts.

2 ENRICH

Put data in context to enable threat hunters to extract insights with speed and accuracy.

3 ANALYZE



Leverage statistical methods combined with human intuition and experience to form and test hypotheses around where and how an advanced attacker might gain a foothold.

4 RECONSTRUCT

Gather and connect data into a cohesive picture, stitching together all of the pieces of the intrusion into a single attack narrative to reconstruct the threat.

5 COMMUNICATE

Share relevant information and supporting context with the security operations center (SOC) so they can stop or contain the breach.

6 HONE

Review activity to determine how automated detection techniques can be improved to identify and prevent intrusions more quickly and effectively.

Falcon OverWatch: CrowdStrike's Managed Threat Hunting Service

CrowdStrike Falcon OverWatch is a 24/7 security solution that proactively hunts, investigates and advises on threat activity in an organization's environment.

Our elite team of hunters sifts through endpoint event data from across CrowdStrike's worldwide customer community to swiftly identify and stop highly sophisticated attacks that would otherwise go undetected.

65,000
potential intrusions were identified and stopped with the help of Falcon OverWatch

8 minutes
is the average interval at which OverWatch threat hunters uncovered potential intrusions

Source: 2021 Threat Hunting Report: Insights From the Falcon OverWatch Team

This proactive managed hunting finds breaches days, weeks or even months before they would have been uncovered by conventional automated-only methods, effectively limiting the opportunity for attackers to coordinate data exfiltration operations that ultimately lead to mega breaches.

What Falcon OverWatch delivers

- **HUMAN EXPERTISE**
- **HISTORICAL DATA**
- **THREAT INTELLIGENCE**
- **24/7/365 OPERATIONS**

Find out more about the powerful security advantage that Falcon OverWatch gives you.

- Falcon OverWatch Product Page
- Falcon OverWatch Data Sheet
- Read the latest blogs from the Falcon OverWatch experts.
- See Falcon OverWatch reconstruct an attack in real time.

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:

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

CROWDSTRIKE

We Stop Breaches