CROWDSTRIKE

FALCON INTELLIGENCE PREMIUM

Cyber threat intelligence for proactively defending against adversaries and their attacks

EXPOSING ADVERSARIES TARGETING YOUR BUSINESS

CrowdStrike® Falcon Intelligence™ Premium is CrowdStrike's premier threat intelligence subscription that enables organizations to predict and prevent nation-state, eCrime and hacktivist attacks. Falcon Intelligence Premium provides security operations, incident response and cyber threat intelligence teams with everything they need to quickly detect, understand and take action against today's most sophisticated adversaries.

Whether your security team is just getting started or is experienced with cyber threat intelligence, Falcon Intelligence Premium provides everything you need to strengthen your security defenses and better inform your teams to make them more efficient and effective.

KEY CAPABILITIES

KNOW YOUR ADVERSARY AND THEIR ATTACKS

- **Actor profiles:** Access over 170 in-depth adversary profiles. CrowdStrike is a pioneer in adversary analysis, with a global team of intelligence analysts, researchers and geo-political experts providing groundbreaking research to expose adversary intent, motivation and tradecraft.
- **Threat alerts:** Gain immediate visibility into emerging and active cyber threats with real-time threat intelligence alerts that update you on the latest breaches, malware innovations, adversary activity and campaigns.
- **Technical reports:** Enhance your teams' situational awareness and reduce the risk from adversary campaigns targeting your organization. Technical reports expose adversaries' operations, targets and timelines, and their tactics, techniques and procedures (TTPs), enabling you to improve security defenses.
- **Tailored intelligence:** Search social media to find suspicious activity in online forums, and hunt for distributed denial of service (DDoS) and botnet attacks to identify actions against your infrastructure.

FALCON INTELLIGENCE PREMIUM BENEFITS EVERY TEAM

Security operations centers (SOCs): Accelerates alert triage and simplifies incident investigations

Incident response: Improves incident prioritization and containment strategies

Cyber threat intelligence: Delivers unique research and improves situational awareness

Vulnerability management: Enables patch prioritization

Information technology: Improves security control effectiveness

Leadership: Informs risk management and security decision-making

FALCON INTELLIGENCE PREMIUM

EMPOWER BETTER SECURITY AND EXECUTIVE DECISIONS

- **Executive reports:** Enable decision-makers to better understand the implications of cyber risks for the organization. These reports focus on mid- and long-term trends to help leadership make better security investments and align the activities of security teams to the goals and strategies of the organization.
- **Quarterly threat briefings:** Gain insight by attending quarterly CrowdStrike webcasts that examine the current global threat landscape. CrowdStrike experts focus on recent adversary campaigns, targeted regions and industries, and the latest TTP innovations.
- **Request for Information (RFI):** Falcon Intelligence Premium customers are eligible to purchase RFI Packs. RFI Packs enable you to submit up to five requests to a CrowdStrike expert who will perform research and provide a custom response.

ANALYZE MALWARE AND TAKE ACTION

- **Malware analysis:** Defeat today's most sophisticated malware with CrowdStrike's automated malware analysis sandbox — it performs both static and dynamic analysis while monitoring all malicious behavior and system interaction. Beyond analyzing a single malware sample, it also determines whether the suspected file is related to a larger campaign, a malware family or an adversary.
- **Expert malware analysis:** Escalate malware to a CrowdStrike expert for further research or a second opinion. You can submit up to five files per month for this type of analysis.
- **Endpoint integration:** CrowdStrike customers can also analyze potentially malicious files taken directly from endpoints protected by the CrowdStrike Falcon® platform. Analysis results are visible within the Falcon platform, presented alongside threat detection. Tightly correlating detections and threat intelligence enables teams to make faster, better decisions and elevates the capabilities of all team members.

STRENGTHEN DEFENSES ACROSS YOUR SECURITY INFRASTRUCTURE

- **Access to CrowdStrike IOCs:** The CrowdStrike global indicator of compromise (IOC) feed is a real-time, high-quality set of indicators created and curated by the CrowdStrike Intelligence team. The indicators in the IOC feed are enriched with context, including confidence level, attribution, related vulnerabilities, threat type and more.
- **YARA and SNORT rules:** Increase the ability to detect sophisticated attacks from a behavioral or infrastructure perspective. CrowdStrike expertly crafts and tests YARA and SNORT rules so you can automatically detect, classify and attribute sophisticated threats with a minimum of false positives.
- **Easily integrated countermeasures:** Protect against future attacks with IOCs and security rules that are easily consumed by security information and event management (SIEM), firewalls, network devices and intrusion detection systems (IDSs). A rich suite of application programming interfaces (APIs) and pre-built tools enable easy integration with existing security solutions.

Request Free Intelligence Briefing

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

FALCON INTELLIGENCE PREMIUM FEATURES

Automated malware analysis
Real-time IOC feed
Daily threat reports
Technical reports
Strategic reports
Actor profiles
Tailored intelligence
SNORT/YARA rules
Quarterly threat briefings
Expert malware analysis (up to 60 malware files)
APIs and pre-built integrations
Access to RFI Packs (available separately)

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/