CROWDSTRIKE

CrowdStrike Products
Data Sheet

Falcon Adversary Intelligence Premium

Level up your security team to defeat adversaries

Challenges

Today's adversaries operate with unprecedented speed and sophistication. In 2023, eCrime breakout time dropped to an average of 62 minutes,[1] and 75%[1] of detected attacks gained initial access without the use of malware. Defenders are struggling to keep up as many rely on inefficient processes, resulting in false positives and out-of-date countermeasures.

In order to mitigate increasing risks to their brand, reputation and financial stability, organizations require improved strategies for combating adversaries, such as obtaining threat research from trusted advisors and automating the process of adapting security controls to evolving threats.

Solution

CrowdStrike Falcon Adversary Intelligence Premium revolutionizes security defenses by delivering world-class research containing in-depth insights into the latest adversarial tradecraft. By understanding how adversaries evolve their tactics, cyber threat intelligence teams can improve the SOC effectiveness and shape their security strategy to stop breaches more effectively.

Falcon Adversary Intelligence Premium increases the productivity of security teams and and reduces the costs to operationalize threat intelligence. By using world-class cybercrime and nation-state intelligence reports, threat intelligence teams can expect up to 97% reduction in adversary research.[2] Detection engineering teams can save 65%[2] of their time spent on crafting detection rules by using pre-designed hunting and detection libraries. Falcon Adversary Intelligence Premium also accelerates security teams' ability to proactively adjust security controls as threats evolve, with up to 80%[2] estimated improvements in security posture.

Key benefits

- Falcon Adversary Intelligence Premium includes all capabilities provided by CrowdStrike Falcon® Adversary Intelligence
- Eliminate the need for in-house threat research with world-class intelligence reports
- Lower the upfront cost of hunting and detection when delivering defenses that evolve
- Increase productivity of your security team to proactively adjust security controls

[1]CrowdStrike 2024 Global Threat Report

[2]Based on CrowdStrike Business Value Assessments (BVAs). Expected results and actual outcomes are not guaranteed and may vary for every customer. Calculations are based on aggregated averages from over 100 Business Value Assessment (BVA) and Business Value Realized (BVR) cases conducted with CrowdStrike Enterprise customers and completed by CrowdStrike's Business Value team from 2018 to December 2022. BVAs are a projected ROI analysis based on the value of CrowdStrike compared to the customer's incumbent solution. BVRs are a realized ROI analysis for customers deployed for 6+ months using customer inputs and recorded telemetry.

Key capabilities

World-class Intelligence Reporting

CrowdStrike's Counter Adversary Operations tracks 230+ adversaries, exposing their activity, tools and tradecraft. Each year, CrowdStrike publishes thousands of threat alerts, in-depth technical analysis reports and strategic insights into cyber threats targeting your organization, reducing or even eliminating the need for expensive in-house threat research. CrowdStrike's threat intelligence provides trusted insights on recognizing and preventing attacks.

- **Real-time threat coverage:** Stay informed with real-time email alerts containing assessments on the latest cyber events, breaches and adversary activities. Implement recommendations, and confidently take action.
- **In-depth technical analysis:** Reduce in-house threat analysis with technical reports covering adversaries' activities, tools and tradecraft. Use this information to proactively patch vulnerabilities, deploy new detections and execute hunts to ensure protection against the latest threats.
- **Trusted strategic insights:** Understand threats facing your organization with reports exposing trends in the global threat landscape, industry-specific intrusion activity reviews and in-person briefings. Communicate relevant risk to your board, drive security strategy and increase return on investments.

Prebuilt Detection and Hunting Libraries

Falcon Adversary Intelligence Premium provides a built-in library of continuously updated hunting queries and detection rules. This enables in-house security engineering teams to deploy defenses that evolve with the latest adversary tactics and techniques while lowering the upfront cost of hunting and detection efforts.

- **Prebuilt detection rules:** Enhance automated detections with pre-tested rules (YARA/SNORT) created and validated by CrowdStrike experts. Save development time and reduce false positives when identifying adversaries, exploits and malware.
- **Intel-led hunting leads:** Accelerate in-house threat hunting with out-of-the box hunting leads. Reduce the time and expertise needed to find the most sophisticated adversarial activities.

Streamline Security Engineering Processes

Today's fast-evolving threat landscape requires security teams to continuously adjust — at scale — their security controls ahead of the latest threats. Falcon Adversary Intelligence Premium delivers end-to-end processes that enable teams to speed the creation, customizing and refining of hunting and detection libraries.

- **Centralized processes:** Leverage the Falcon platform to accelerate the process of researching, designing, prototyping, and deploying hunts and detections.
- **Operationalize countermeasures:** Protect against future attacks with detection rules that are easily consumed by security information and event management (SIEM) solutions, firewalls, network devices and intrusion detection systems (IDSs). A rich suite of application programming interfaces (APIs) and prebuilt workflows enables easy deployment to existing security solutions.

Every team benefits

1. **Threat Intelligence Teams:** Reduces the need for expensive in-house research, and improves awareness of the threat landscape
2. **Detection Engineering:** Improves effectiveness of security controls, and removes efforts to create, test and validate rules
3. **Hunting Team:** Reduces the upfront time and expertise to find the most sophisticated attacks
4. **Security Operations Center (SOC):** Reduces time wasted on false positives and accelerates responses
5. **Leadership:** Increases return on investments and lowers risk

About CrowdStrike

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

Powered by the CrowdStrike Security Cloud and world-class AI, 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 delivers 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 | X | LinkedIn | Facebook | Instagram

Learn more →