INTSIGHTS
Defend Forward™

CROWDSTRIKE

IntSights for CrowdStrike

External Threat Protection and Continuous Breach Prevention

Enterprises are forced to navigate a tsunami of threat data, leaving security teams without a clear vision of how to operationalize threat intelligence and proactively secure endpoints. Practitioners are challenged to understand which attacks are relevant to their environments, quickly detect attack behavior, and better defend their networks. Organizations must continuously identify and understand sophisticated attacker motives and indicators with advanced solutions that enable proactive protection of targeted networks and endpoints.

Gain threat knowledge and stop breaches with the IntSights + CrowdStrike integration. Stay ahead of adversaries with a scalable solution that enables mutual customers to seamlessly integrate IntSights External Threat Protection Suite and CrowdStike Falcon Enterprise. Discover, view, validate, and investigate IOCs from within a CrowdStrike device. Your security teams now have a single threat library for internal and external intelligence.

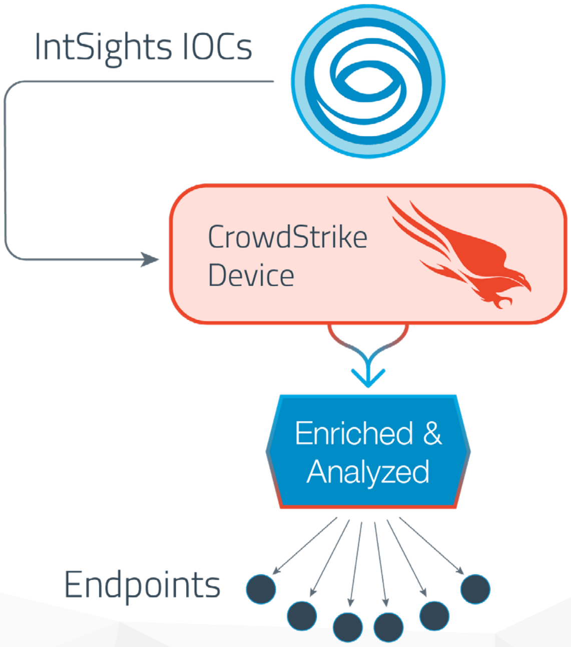
Expand the value of existing security tools with external threat intelligence for informed decisions on threat prioritization and mitigation. Together, IntSights and CrowdStike offer contextual threat intelligence and continuous endpoint protection.

Integration Overview: How It Works

IOCs (domains, IP addresses, and file hashes) from IntSights Threat Intelligence Platform (TIP) are exported to a CrowdStrike device in the IntSights External Threat Protection Suite. IOCs enriched with source name, severity, first seen, and last seen data are validated, aggregated, and analyzed by CrowdStrike for integrated endpoint protection. Indicator filtering gives users full control over which IOCs are pushed to CrowdStrike, allowing them to identify the endpoints that are vulnerable to specific indicators.

Integration Benefits

- Instant visibility of threat environment and endpoint vulnerability
- Accurate, relevant, and timely threat intelligence
- Greater context, control, and collaboration
- Efficient and effective threat management
- Continuous breach prevention
- Constant protection against all types of attacks
- Endpoint security powered by tailored threat intelligence



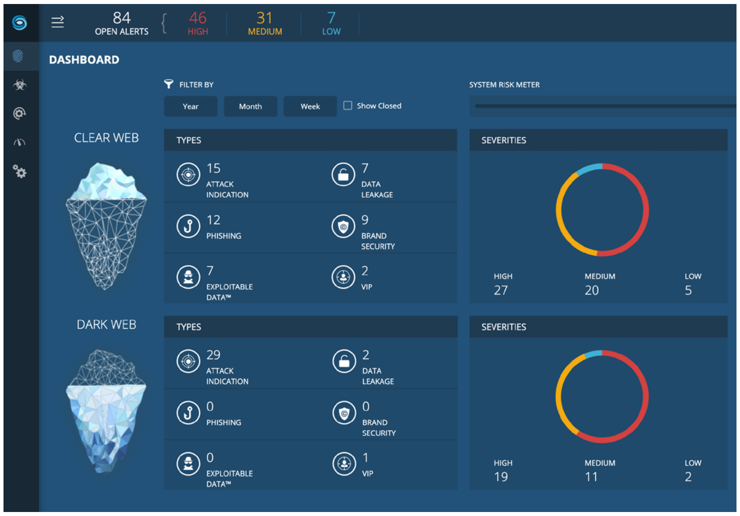
Visit: Intsights.com Call: +1 (800) 532-4671 Email: info@intsights.com

INTSIGHTS + CROWDSTRIKE

IntSights Threat Intelligence Platform

Visualize, investigate, and operationalize IOC data

IntSights ETP features a SaaS-based Threat Intelligence Platform (TIP) to centralize all security threat feeds (proprietary, public, and private) and data sources for deeper user-driven threat analysis, sharing, and proactive threat prevention. It rapidly ingests, normalizes, and enriches this threat data, outputting unified and contextually relevant IOCs that drive proactive security action.



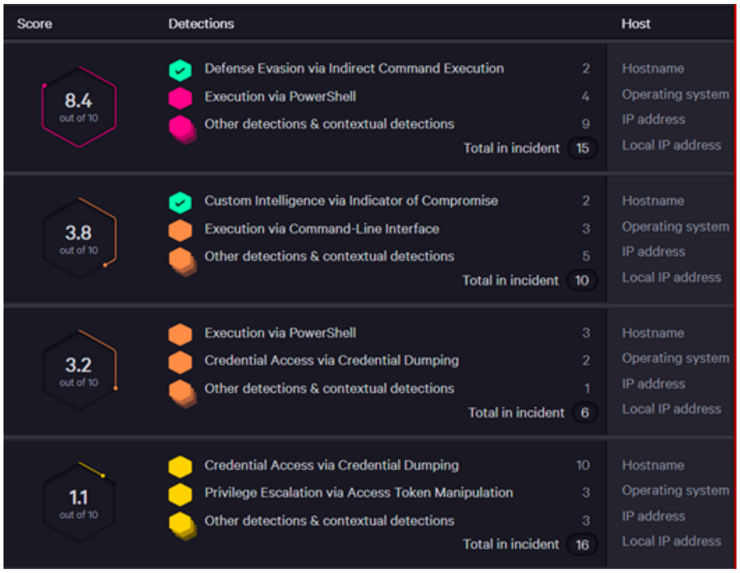
Features and Capabilities

- IOC aggregation and enrichment
- Contextualized attack profiling
- Visualized investigation
- Automated threat blocking
- Centralized dashboard for all threat feeds

CrowdStrike Falcon Enterprise

Built to stop breaches

CrowdStrike Falcon® Endpoint Protection Enterprise sets the new standard in endpoint security with the first and only cloud-native security platform proven to stop breaches by unifying next-generation antivirus (NGAV), endpoint detection and response (EDR), managed threat hunting, and integrated threat intelligence in a single cloud-delivered agent.



Score	Detections		Host
8.4 out of 10	Defense Evasion via Indirect Command Execution	2	Hostname
	Execution via PowerShell	4	Operating system
	Other detections & contextual detections	9	IP address
	Total in incident	15	Local IP address
3.8 out of 10	Custom Intelligence via Indicator of Compromise	2	Hostname
	Execution via Command-Line Interface	3	Operating system
	Other detections & contextual detections	5	IP address
	Total in incident	10	Local IP address
3.2 out of 10	Execution via PowerShell	3	Hostname
	Credential Access via Credential Dumping	2	Operating system
	Other detections & contextual detections	1	IP address
	Total in incident	6	Local IP address
1.1 out of 10	Credential Access via Credential Dumping	10	Hostname
	Privilege Escalation via Access Token Manipulation	3	Operating system
	Other detections & contextual detections	3	IP address
	Total in incident	16	Local IP address

Features and Capabilities

- Intelligent EDR
- 24/7 managed threat hunting
- Device control
- Firewall management
- Integrated threat intelligence

The IntSights Advantage

Proprietary Collection

Gather intelligence from the deepest and hardest-to-reach places on the web.

Tailored Intelligence

Instantly discover threats that matter most to your business by mapping intelligence to your digital assets.

Orchestrated Mitigation

Coordinate proactive response to dismantle and block threats before they cause damage.

Visit: Intsights.com   Call: +1 (800) 532-4671   Email: info@intsights.com

GET STARTED TODAY

Configure and add a CrowdStrike cloud device to the IntSights ETP Suite to receive IOCs. Log in to the IntSights platform and click **Automation > Integrations.** From the Integrations window, click **Cloud** and **Add new device**, then select **CrowdStrike**. For additional details, please refer to the ETP Suite User Guide in the IntSights platform.

About IntSights

IntSights is revolutionizing cybersecurity operations with the industry's only all-in-one external threat protection platform designed to neutralize cyberattacks outside the wire. Our unique cyber reconnaissance capabilities enable continuous monitoring of an enterprise's external digital profile across the clear, deep, and dark web to identify emerging threats and orchestrate proactive response. Tailored threat intelligence that seamlessly integrates with security infrastructure for dynamic defense has made IntSights one of the fastest-growing cybersecurity companies in the world. IntSights has offices in Amsterdam, Boston, Dallas, New York, Singapore, Tel Aviv, and Tokyo. To learn more, visit: intsights.com or connect with us on LinkedIn, Twitter, and Facebook.

About CrowdStrike

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network.