Polaris

POLARIS FOR CYBERSECURITY TEAMS

Navigate vulnerabilities and cyberattacks to stay one step ahead of global threats

Polaris is an AI-powered threat intelligence advisor that provides AI-curated, actionable insights tailored to attack surface maps.

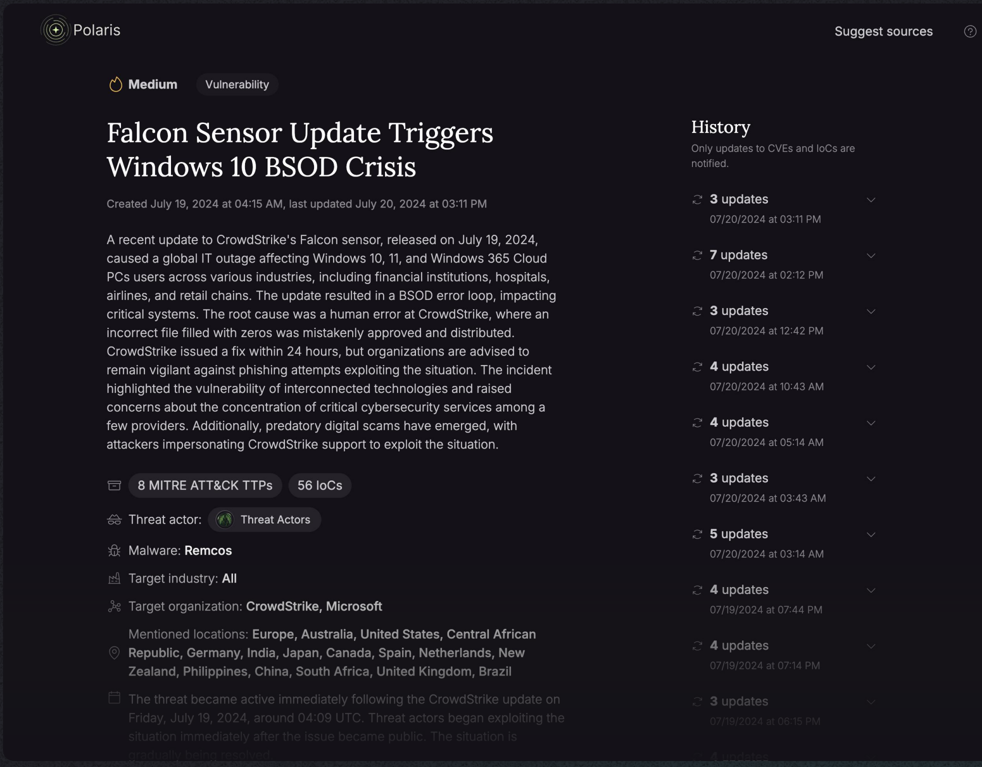
⚠ Problem

As cyber threats advance more rapidly, security teams are often overwhelmed and paralyzed trying to distinguish significant dangers within the data flood, instead of quickly identifying and acting on critical threats. Meanwhile, cybersecurity platforms provide extensive but non-customized information that leaves organizations to navigate a sea of signals on their own.

✧ Solution

Polaris uses AI technology to scan over thousands of sources, selecting insights tailored to your attack surface map. Receive prioritized alerts with comprehensive coverage and detailed threat information. Let AI do the hard work, empowering your security team to act quickly with actionable intelligence.

Everything you need to know aligned perfectly with what you need to do.



Falcon Sensor Update Triggers Windows 10 BSOD Crisis

Created July 19, 2024 at 04:15 AM, last updated July 20, 2024 at 03:11 PM

A recent update to CrowdStrike's Falcon sensor, released on July 19, 2024, caused a global IT outage affecting Windows 10, 11, and Windows 365 Cloud PCs users across various industries, including financial institutions, hospitals, airlines, and retail chains. The update resulted in a BSOD error loop, impacting critical systems. The root cause was a human error at CrowdStrike, where an incorrect file filled with zeros was mistakenly approved and distributed. CrowdStrike issued a fix within 24 hours, but organizations are advised to remain vigilant against phishing attempts exploiting the situation. The incident highlighted the vulnerability of interconnected technologies and raised concerns about the concentration of critical cybersecurity services among a few providers. Additionally, predatory digital scams have emerged, with attackers impersonating CrowdStrike support to exploit the situation.

8 MITRE ATT&CK TTPs · 56 IoCs

Threat actor: Threat Actors

Malware: **Remcos**

Target industry: **All**

Target organization: **CrowdStrike, Microsoft**

Mentioned locations: **Europe, Australia, United States, Central African Republic, Germany, India, Japan, Canada, Spain, Netherlands, New Zealand, Philippines, China, South Africa, United Kingdom, Brazil**

The threat became active immediately following the CrowdStrike update on Friday, July 19, 2024, around 04:09 UTC. Threat actors began exploiting the situation immediately after the issue became public. The situation is gradually being resolved.

History

Only updates to CVEs and IoCs are notified.

3 updates
07/20/2024 at 03:11 PM

7 updates
07/20/2024 at 02:12 PM

3 updates
07/20/2024 at 12:42 PM

4 updates
07/20/2024 at 10:43 AM

4 updates
07/20/2024 at 05:14 AM

3 updates
07/20/2024 at 03:43 AM

5 updates
07/20/2024 at 03:14 AM

4 updates
07/19/2024 at 07:44 PM

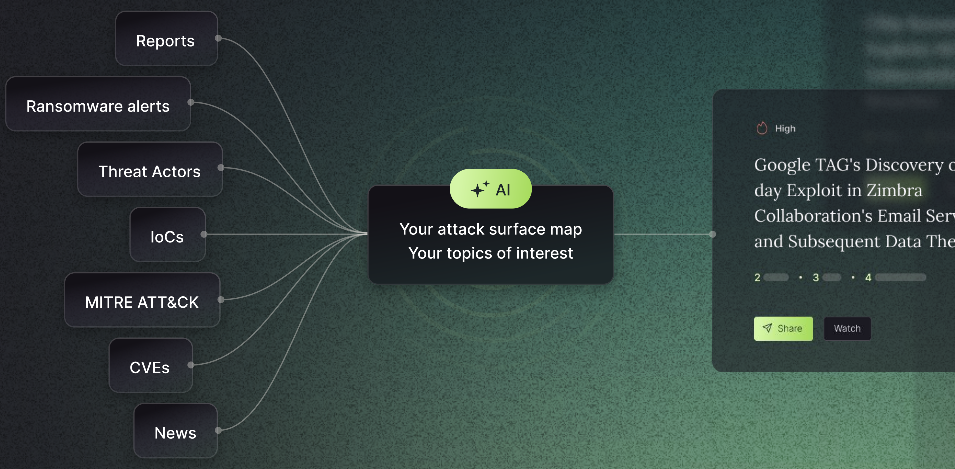
4 updates
07/19/2024 at 07:14 PM

3 updates
07/19/2024 at 06:15 PM

4 updates

How Polaris works

- Everyday, Polaris scans thousands of sources looking for information about common vulnerabilities, ransomware alerts, Zero-Day exploits, IOCs, frameworks (MITRE ATT&CK), and exposures (CVEs).
- Its highly specialized LLM model sums up every relevant attack, threat, or vulnerability and cross-reference with your Attack Surface Map;
- So it sends curated, actionable alerts with only what you really need to know, nothing else.



Let AI do the hard work for you, by searching, analyzing, and prioritizing relevant alerts

→ Coverage
of thousands of sources

→ Speed
new reports in up to 5 minutes

→ Prioritization
receive alerts according to region and assets

☒ BEFORE

11,000 alerts
faced by security teams daily

✦ WITH POLARIS

99.4%
reduction time in alerts analysis

Transform alerts into actionable insights

Enhanced insight for patch management

Polaris consolidates diverse data sources, offering comprehensive insights that simplify the process of convincing IT teams to implement necessary patches.

Receive first-hand vulnerability alerts

Stay ahead of emerging threats and be the first to know and quickly inform management for immediate action.

Strategic data for CISOs and security teams

Polaris is the ideal solution for the detailed analysis that security teams need to carry out on a daily basis and provides CISOs with strategic data to prevent possible attacks and strengthen the company's security posture.

No more endless tabs or contextless alerts

Say goodbye to the chaos of juggling numerous tabs with contextless alerts. Streamline your alert management and receive only crucial actionable insights.

Get started with Polaris

Start your free trial

///AXUR

Polaris is a Cyber Threat Intelligence (CTI) solution by **Axur**. Axur's solutions empower companies and make the Internet a safer place with scalable intelligence and automation.
Learn more about Polaris at axur.com/polaris.