# Polaris

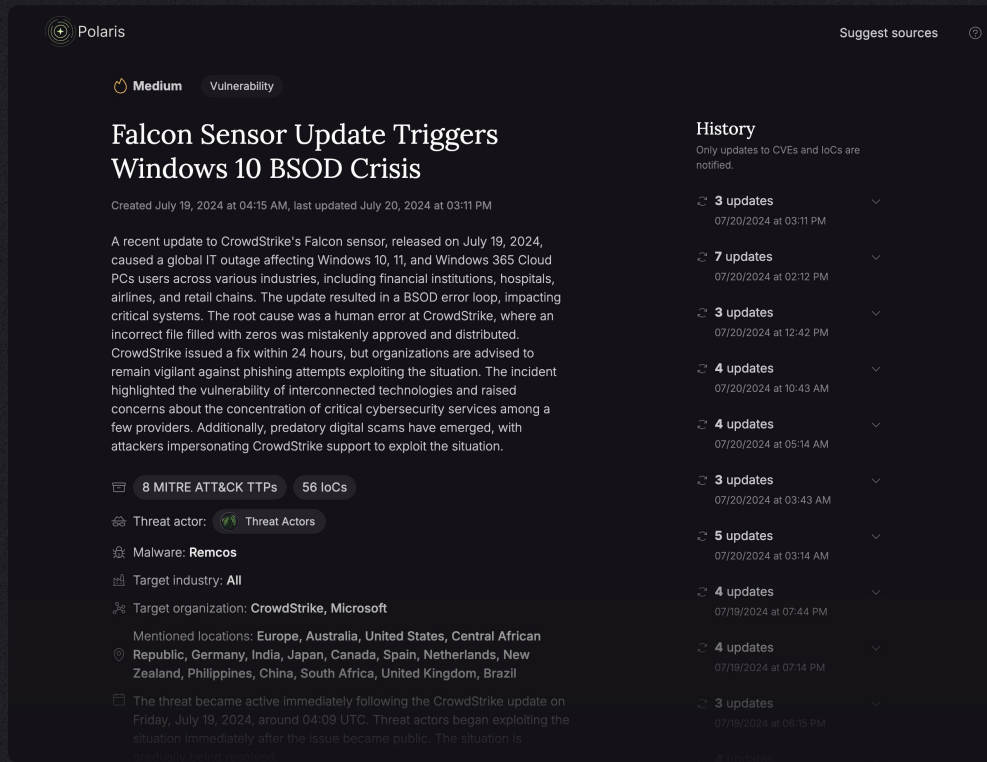# Implement Seamless 24/7 Vulnerability Management for Your Clients

Polaris is a CTI solution by Axur that collects information from over thousands of sources, using AI technology to create actionable insights tailored to your client's Attack Surface Map (ASM). Receive information first-hand and become a strategic partner to your clients.

## ⚠ 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 struggle under the weight of their own data, providing extensive but non-customized information that leaves organizations to navigate a sea of signals on their own.
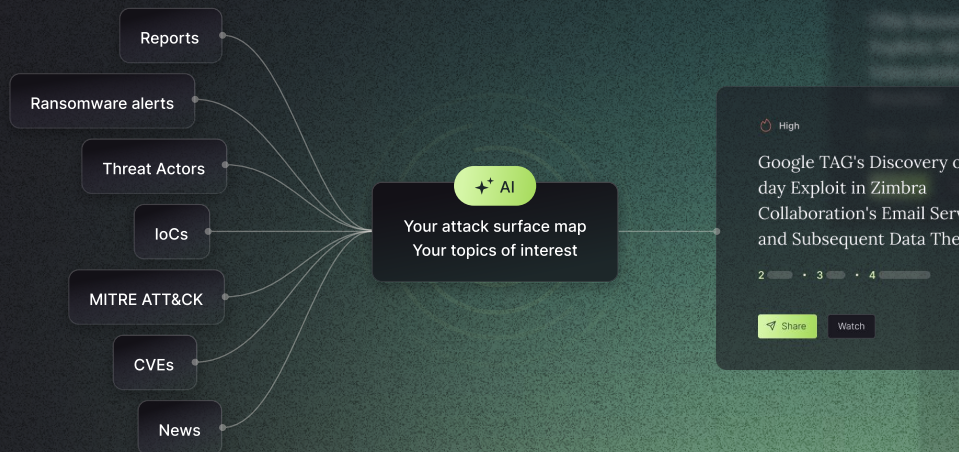
## ✧ Solution

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.

---

### Polaris

Suggest sources

🔥 **Medium**   Vulnerability

## 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

**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

---

# 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.

Reports

Ransomware alerts

Threat Actors

IoCs

MITRE ATT&CK

CVEs

News

✦ AI

**Your attack surface map**
Your topics of interest

🔥 High

Google TAG's Discovery of day Exploit in Zimbra Collaboration's Email Serv and Subsequent Data The

2  ·  3  ·  4

✈ Share     Watch

# Customized 24×7 collection for your unique needs

⊘ **BEFORE**

## 11,000 alerts
faced by security teams daily

✦ **WITH POLARIS**

## 99.4%
reduction time in alerts analysis

→ Prioritize what's crucial, never missing key alerts

→ Know first, act fast and overcome threats with confidence

→ Swiftly eradicate false positives and unleash your team's full potential

## 30% revenue growth scenarios

### Investment Prioritization Advisory

Use Polaris' data-driven insights to advise clients on how to prioritize the most critical vulnerabilities and allocate their cybersecurity investments correctly.

### Managed Threat Intelligence Services

Offer ongoing threat intelligence services that translate Polaris' insights into extended measures, with continuous updates and adjustments as the threat landscape evolves.

### Bespoke Cybersecurity Training

Develop training programs that address the unique threats and vulnerabilities faced by the client, using the insights to inform curriculum development.

### Vendor Risk Management

Offer vendor risk management by using Polaris' insights to identify which third-party risks are most pressing and require immediate action.

## 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.