Unlocking the **Next Generation of Threat Intelligence** with GenAI

How AI transforms cybersecurity
by enabling more scalable, cost-effective
and faster threat intelligence.

Polaris

Powered by AXUR

Executive Summary

Cybersecurity requires continuous innovation to make sure defenders have the upper hand against attackers. Today, **defenders are overwhelmed** by thousands of alerts, which are challenging to assess when they lack information about the most pressing threats. Professionals in the field feel that **cybersecurity is the most challenging it has been in the past few years.**

On average, security operations teams receive 11,000 alerts each day.

28% are never addressed. Members of Security Operation Centers (SOCs) say they are only able to get to 49% of the alerts they were supposed to.

Source: Forrester Consulting, 2020, and Morning Consult/IBM, 2023

This isn't very surprising, given how **criminals are more persistent and financially motivated than ever.** Businesses disrupted by ransomware attacks have paid millions of dollars to criminals in exchange for their data or as protection money to avoid personal data getting leaked to the internet. Attackers have no reason to stop.

To effectively protect our businesses, Artificial Intelligence can be leveraged to improve many cybersecurity processes by correlating and prioritizing alerts. **Generative AI goes a step further, turning alerts into actionable insights that can change the way security teams make critical decisions and allocate resources.**

AI-powered Cyber Threat Intelligence is defined by speed. In cybersecurity, attackers will quickly scale their campaigns to find hundreds or thousands of vulnerable organizations. **AI allows defenders to respond earlier and with more confidence** – they can patch vulnerabilities or adopt mitigation strategies before criminals have enough time to scale their attacks, increasing the chance an incident is completely prevented.

Cybersecurity professionals also often find themselves explaining the alerts they receive to request data or actions from other departments. The human-readable insights produced by GenAI facilitates communications with non-security staff. This means less time spent on explaining why a patch is important or that additional care with certain types of messages is needed.

In this document, you will find:

- How cybersecurity has become so challenging
- Why CTI can provide immense value to cybersecurity teams today
- Why CTI is not always viable or available, despite its value
- How AI enables the next-generation of CTI while also being more scalable, cost-effective and faster than traditional threat intelligence efforts
- The advantages of leveraging AI-powered CTI inside cybersecurity teams

Why AI Matters for Cybersecurity Today

According to the 2023 ISC2 Cybersecurity Workforce Study, 75% of cybersecurity professionals view the current threat landscape as the most challenging it has been in the past five years. Yet most of them — 67% — also say their organizations have a shortage of professionals to deal with the problem, usually due to budget or pay constraints, but also because finding qualified people can be a challenge.

The concerns expressed by the professionals in the ISC2 study are not unfounded. Far from it. While information security is an ever-changing discipline by nature, the whole decade was still very taxing for cybersecurity teams.

The demands that the IT infrastructure is expected to meet, and the profile of threat actors have both changed dramatically. The rise of the ransomware threat, increased regulatory oversight, cloud migration, policies to allow people to work from home or with their own devices, the surge in APIs and connected services and software — there is a substantial list of risks stemming from these and other trends.

To rise to the challenge, we need to innovate in how we approach cybersecurity.

Current Challenges for Cybersecurity

Hybrid Environments

The corporate network is now a hybrid environment that connects on-premises IT infrastructure, new cloud-native systems, third-party services, and people working from a diverse number of locations.

The SolarWinds hack of 2020 is the most well-known example of how attackers can exploit different parts of the IT infrastructure to reach their final targets. According to the World Economic Forum Global Cybersecurity Outlook 2024, 41% of organizations that had a material impact from a cybersecurity incident said that the problem originated at a third party.

Focusing on the traditional network perimeter is no longer effective, requiring a broader view of the attack surface.

Regulatory Oversight

As digital systems become inseparable from the means through which people perform all their daily tasks and their basic needs met, government institutions are more likely to regulate how technology companies operate. Making sure the appropriate rules are followed usually falls to compliance or cybersecurity governance teams.

In 2023, the Securities and Exchange Commission (SEC) adopted new rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, covering all publicly traded companies.

When every project has an IT component, any regulation that imposes cybersecurity requirements has the potential to affect the whole business.

Data Privacy

Most computing tasks, joint ventures, or online interactions require data to be shared with another party. Businesses are concerned with their trade secrets, and consumers want to avoid becoming victims of fraud after having their data stolen by criminals. Governments have also stepped in to create many different regulations to protect personal data.

While the General Data Protection Regulation (GDPR) from Europe is the most well-known data privacy regulation, the United States has the Health Insurance Portability and Accountability Act (HIPPA) and dozens of state regulations, including the California Consumer Privacy Act (CCPA), which is considered one of the most strict.

While many companies avoided disclosing leaks and security failures in the past, this is no longer allowed. Businesses, regulators, and consumers expect transparency.

Sophisticated Adversaries

Threat actors are no longer relying on luck and opportunistic attacks. Recent vulnerabilities are now exploited to establish a foothold inside corporate networks.

While traditional malware only caused by damage by spreading to other systems and running predetermined routines, threat actors now carefully manage each intrusion, aiming to cause as much damage as possible. They adapt their tactics to each system, moving laterally inside the network in search of domain controllers, databases, and backup infrastructure.

Vulnerability management can no longer rely on a slow process tied to a schedule. Significant vulnerabilities need to be patched as soon as possible.

Responsive Security with Threat Intelligence

Traditionally, security has sometimes been treated as a fixed value or condition of a system, but this is not very useful. Even when no known vulnerabilities exist, breaches can still occur due to leaked credentials, insider threats, or unexpected zero-day attacks. Today, being able to detect and respond to incidents is seen as an integral part of the security process.

The same principle can be applied to prevention. By understanding that the assets at risk of exploitation change with time and attacker patterns, there is an opportunity to respond proactively, allocating resources to protect them. This avoids the inordinate undertaking of trying to secure every asset against all known and unknown threats.

When preventive measures and thorough monitoring are adopted where they are most needed, teams can focus their eyes on where they are more likely to see threat activity and expedite the patching of vulnerabilities that present a higher threat to the business. This can be especially beneficial to Managed Security Services Providers (MSSPs), who often oversee large and diverse IT infrastructures on behalf of their customers.

SOLUTIONS BASED ON **THREAT INTELLIGENCE**

CTI paves the way for a more proactive posture

How Intelligence Changes Cybersecurity

Smarter Vulnerability Management	IT infrastructure is large and complex, but vulnerabilities can be managed based on the risk they present. With proper threat intelligence, vulnerability management can be made smarter. You can patch or mitigate the issues that represent the most risk to the business.
Threat Actor Profiling	By keeping track of threat actor activity, teams can focus on mitigation strategies and events that are more likely to be linked to current threat activity.
Credential Security & Identity Management	Implementing access management processes based on a Zero Trust model reduces the chance that attackers can steal usable credentials. However, businesses can improve their identity management with monitoring solutions to be able to block intruders before they even attempt to use a stolen password or authorization token.
Exposure Monitoring	To comply with data privacy regulations, avoid fraud, and anticipate incidents, businesses can rely on information gathered from data leak monitoring.

Cyber Threat Intelligence has a place as a key component of cybersecurity. It improves resource allocation, allowing teams to move faster and counter the most pressing threats, putting defenders ahead of the attackers.

Gathering and processing data to create actionable intelligence can be time-consuming — but that is where Artificial Intelligence fits in.

AI Enters the Chat

While threat intelligence can be very advantageous to security teams, it is not always immediately available. Even when sources of information are public and plentiful for Open Source Intelligence (OSINT) activities, combing through the data and finding what really matters is time-consuming, and intelligence can become less useful as time goes on. Conversely, the faster you can create actionable intelligence, the more useful it is going to be.

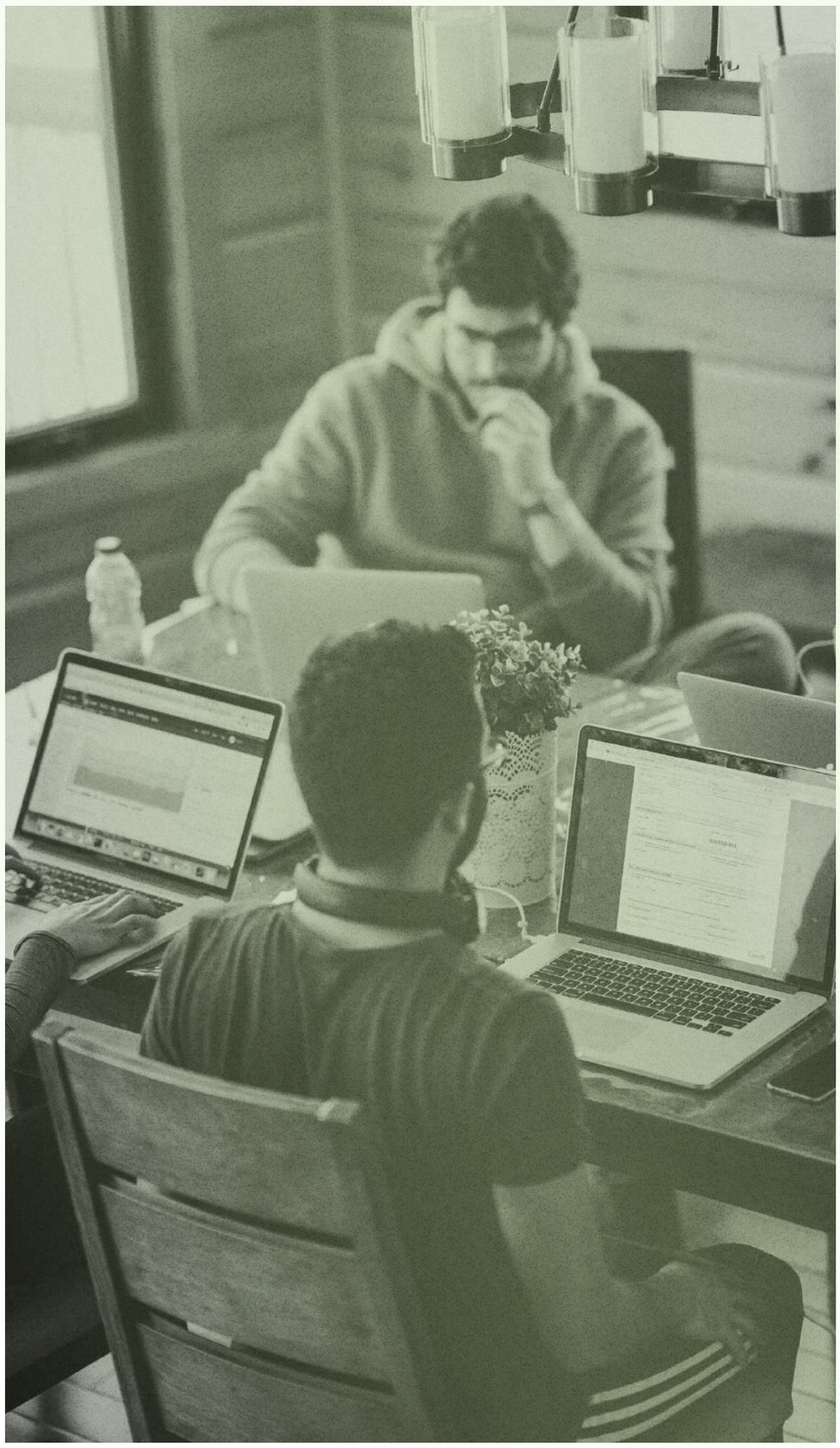
The 2023 ISC2 Cybersecurity Workforce Study found that **23% of organizations have a threat intelligence analysis gap in their cybersecurity teams.** While it is fortunate that Artificial Intelligence has very interesting properties to solve this problem, many professionals have not yet realized this potential — the same ISC2 study notes that **32% of organizations struggle with an AI skill gap.**
It is not surprising, then, that many people still do not see AI as a solution to CTI and other challenges.

Nevertheless, probability algorithms have been part of cybersecurity for years. Spam filtering was completely revamped with the adoption of algorithms that could "learn" from users and what they considered spam, for example.

As machine learning has advanced, algorithms gained the capability to label images and sort data. Today, thanks to Deep Learning, Large Language Models (LLMs) can generate text on the fly, answering questions (or prompts) on any text-based data set that has been processed by the model. Many have described these AI as chatbots, but this is just a form of **data analysis through a human-like interface.**

AI has several applications in cybersecurity. By having AI label and prioritize events, analysts can avoid the alert fatigue caused by an excessive number of events that require no concrete action; algorithms for Natural Language Processing (NLP) and visual recognition can extend data-gathering capabilities so that we are not limited to text data.

But gathering data by itself is not enough — it should be part of a larger intelligence effort. For CTI, then, it is worthwhile to look a little bit deeper into what AI can and should do.



To develop an AI-first security strategy, it's important to understand what AI can do and what steps should be considered to make the most of what this technology can offer.

How AI Takes CTI to the Next Level

Cyber Threat Intelligence can provide many advantages, but it is often seen as part of the long-term security strategy. Collecting and analyzing data can take time, so fresh intelligence is not always available in a way that is helpful for daily tasks or incident response scenarios.

Another complicating factor is that data is usually fragmented or scattered. An analyst first locates a thread or topic of interest, and then follows along that thread to collect many little pieces of information that may prove useful. It is onlya fter connecting all the dots that a valuable insight starts to take shape.

Artificial Intelligence completely changes this. Thanks to its speed, AI can produce and update insights quickly and when they are needed the most. There is no need to look for data or comb through hundreds of news feeds to find something that might be relevant — AI can do all of that and process the information to create an actionable insight that makes sense for your environment.

This is different from standard threat reports that contain information for a whole industry or environment that is not exactly like your own. While undoubtedly helpful, strategic threat reports require more time to be read and understood — and this is not necessarily very useful for allocating and prioritizing resources in your daily operations.

AI can correlate information from multiple sources to generate tailored insights at an unprecedented speed. It can also find patterns and potentially predict attacks based on similarities with previous campaigns or vulnerabilities.
By leveraging AI insights, security teams get a head start to prevent attacks and respond to ongoing campaigns.

Security teams that have this kind of threat intelligence available to them can then change their processes, taking this information into account when making decisions and prioritizing their next steps.

This is important because security teams are under a lot of pressure. When it comes to vulnerabilities alone, multiple estimates suggest over 25,000 new CVEs (Common Vulnerabilities and Exposures) were published in 2023 — or more than 68 vulnerabilities per day. Making matters worse, one vulnerability was exploited as a zero-day every four days, on average.

Many businesses have complex IT environments, as they require systems to meet their needs in a very competitive landscape. This often involves adding new software packages or services, increasing the attack surface and the number of products that must be monitored for vulnerabilities.

Security teams also receive an average of 11,000 alerts a day, and analysts take about 30 minutes to check each one. In practice, they are forced to only take a quick glance at certain alerts and completely skip many others — a decision that often must be made based on prior knowledge and intuition instead of data, as there is no way to tell beforehand whether an alert is relevant.

When up-to-the-minute intelligence insights are available from AI, analysts remain informed of the latest threat and vulnerabilities that matter to them as they filter through alerts and decide what to do next.

In cybersecurity, accelerating your response and acting to fight the most current threats usually leads to cost savings. The Cost of a Data Breach 2023 survey by IBM found that extensive use of AI and automation could save nearly US$ 1.8 million in costs associated with data breaches. This was possible because the use of this technology helped these companies identify and contain breaches fast by over 100 days, on average.

By leveraging AI, security teams can make better decisions in the field, and counter the attacker's that are most threatening to the business's assets.

Benefits of AI-Powered Threat Intelligence

1. Fast	**AI insights are done before you can even start your data collection.** Its speed alone enables a new form of CTI that has never been possible until now.
2. Tailored	**AI saves time by filtering information that is not relevant to the attack surface.** Analysts do not have to waste time filtering irrelevant information to find what they need to accomplish their tasks.
3. Cost-Effective	**AI implementation is not expensive and can save money by reducing breach costs.** Thanks to its actionable insights that keep analysts informed of the latest attacks, AI can be instrumental in detecting breaches faster to reduce the damage.
4. Automated	**AI is always available and can be part of workflows accelerated by automation.** It never rests, it does not get tired, and it can advise the whole team right from the first minute of the day.
5. Scalable	**AI can scale to accommodate an expanding attack surface.** While you can and should use AI to help defend your most important assets, it is also useful to monitor and gather intelligence on systems that are low-risk and do not have human resources dedicated to them.
6. Reliable	**Dedicated cybersecurity AIs can be more accurate and understand the context.** Unlike generalized chatbots, cybersecurity AIs can source information correctly and provide appropriate context. This makes the information more reliable and accurate, allowing the analysts to quickly determine how the AI insight was generated.
7. Easy Integration & Engagement	**AIs use friendly interfaces like chat commands or human-readable text.** AI can be very intuitive and require little to no specialized training, reducing costs associated with many other security tools. Its output can also be shared with other teams and used in internal reports and communication. With APIs, it also can be integrated into existing tools.

The Takeaway

It is essential to understand that traditional intelligence gathering and analysis will not be entirely replaced by AI, but that AI establishes an innovative way to approach many daily CTI tasks.

As we work smarter with the help of AI, everything that we do becomes more effective — decisions are based on data and other factors, such as ongoing campaigns, that correlate to real active threats. By having this information at our disposal without even having to look for it, we are more likely to detect problems and protect our systems.

As CTI should be a cornerstone of your cybersecurity strategy, having AI gather and create intelligence at unmatched speeds will allow nearly every defensive measure to be accelerated and underpinned by AI.

Polaris: 180x Faster Threat Intelligence with GenAI

Polaris is an AI-powered threat intelligence advisor that provides AI-curated, actionable insights tailored to each company's specific attack surface map, representing Axur's vision for an AI-first approach to Cyber Threat Intelligence.

While security teams have many signals and data available to them from public records or security platforms, attackers are moving faster every day. As they only need to find one vulnerability or weakness in a system, defenders are always under pressure to win this race, making sure they have the appropriate mitigations in place before an adversary finds and exploits their system.

The best way to overcome this challenge is by making sure security teams are aware of what really matters and do not get bogged down by the noise. Polaris empowers security teams to act rapidly and decisively, **putting an end to the burden of impossible manual tracking and analysis. Polaris reduces the time spent on an alert by 99.4%.**

To accomplish this, Polaris scans thousands of sources looking for information about common vulnerabilities (CVEs), ransomware alerts, Zero-Day exploits, Indicators of Compromise (IOCs). Its highly specialized LLM model can correlate this data to frameworks (MITRE ATT&CK), and your custom surface map to generate curated, actionable alerts with what you really need to know.

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.

Optimize budget allocation and decision making

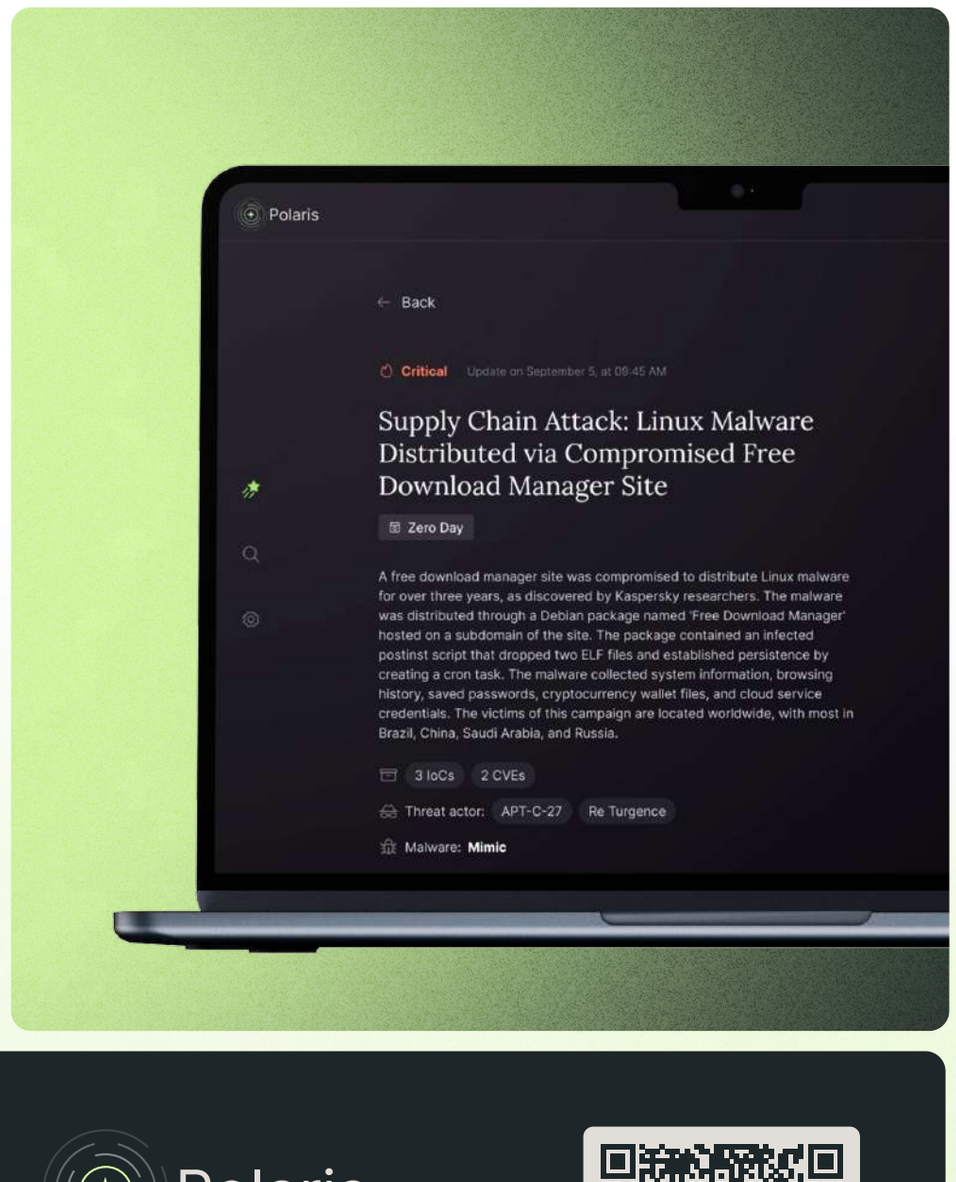
Guide strategic budget decisions by presenting a clear and straightforward view of the cyber threat landscape to the board, highlighting key areas for investment.

Proactive insights to build board trust

Maintain board confidence by showcasing comprehensive control over your cybersecurity landscape, even in the absence of immediate vulnerabilities. Optimize budget allocation and decision making

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.



Be a part of the next generation of CTI

START YOUR FREE TRIAL

Polaris

Instantly activate a free trial of Polaris and start experimenting with AI today with no learning curve needed.