OpenText Core Adversary Signals for the aviation industry

Gain strategic visibility into global adversary activity, uncovering blind spots and early signs of attack

Benefits

- **Enhanced threat visibility:** Identify malicious traffic for earlier threat detection
- **Zero-touch global coverage:** Easily deployed across networks and supply chains
- **Actionable insights:** Distill insights specific to your network

Learn what an aviation customer says about OpenText Core Adversary Signals

Read the press release ›

As a vital sector in socio-economic development, aviation is a prime target for cyber terrorists, nation-state actors, and cybercriminals seeking to exploit legacy systems, disrupt operations, and steal valuable IP and PII. An intricate, interconnected digital ecosystem—spanning supply chains, manufacturing, distribution, maintenance, and more—makes it challenging to identify where threats are emerging. There's potential for significant disruptions to both airline operations and global infrastructure that put lives at risk.

OpenText™ Core Adversary Signals introduces a powerful approach to aviation cybersecurity through global adversary signal analytics. OpenText Core Adversary Signals discovers and analyzes malicious internet traffic relevant to your organization to unmask adversary activity, outline sophisticated attack paths, uncover early signs of attacks, and provide actionable intelligence about the activity affecting your digital environment.

This SaaS-based solution can be quickly and easily deployed across complex, interconnected ecosystems to provide unparalleled visibility into adversary traffic affecting your global network and supply chain. Seamlessly integrating into existing security infrastructure, OpenText Core Adversary Signals enhances capabilities without adding complexity, ensuring your organization stays ahead of emerging threats with a superior level of detail and a unique external perspective.

Enhanced threat visibility

OpenText Core Adversary Signals empowers aviation organizations by analyzing global adversary signals to identify and monitor malicious internet traffic targeting your networks. It compliments traditional log-based security systems by taking an "outside-in" approach, assessing your security posture from an external perspective.

Resources

Discover, define, and contextualize cyberthreats with SaaS-based global signal analytics

Read the overview ›

Introducing OpenText Core Adversary Signals

Watch the intro video ›

What is Adversarial Threat Visibility?

Request a demo ›

Learn how to see beyond your perimeter

Learn more ›

This approach enables earlier threat detection by discovering entry points and eliminating blind spots that traditional SOC tools may be missing. It allows you to detect adversarial scanning activity, enabling you to discover early attack signs and outline sophisticated adversary attack paths and patterns without collecting a single event log.

By integrating OpenText Core Adversary Signals' global adversary signal visibility into your existing SOC ecosystem, you gain a strategic advantage in detecting and responding to threats before they can disrupt operations or exploit system vulnerabilities.

Zero-touch global coverage

OpenText Core Adversary Signals is a plug-and-play SaaS solution that requires no additional hardware and minimal effort for integration. It is ideal for seamless deployment across even the most intricate networks and supply chains. Users simply define the IP addresses, ranges, or ASNs they want covered, and OpenText Core Adversary Signals employs machine-aided adversary analytics on global signals entering and exiting that "covered space." This space can encompass IT, OT, supply chain partners, and more.

While OpenText Core Adversary Signals doesn't decrypt or access PII data, it effectively analyzes traffic entering and exiting the covered space to uncover vulnerabilities being targeted by adversaries. It can also cross-reference patterns and indicators of compromise (IoCs) across multiple departments and divisions to identify commonalities and corroborating findings. Additionally, OpenText Core Adversary Signals easily co-exists with existing security infrastructure (SIEM, XDR, etc.), amplifying their effectiveness and raising their ROI.

Actionable insights

While traditional threat intelligence is often generic, outlining what might happen, OpenText Core Adversary Signals delivers precise, actionable insights on what has happened and is happening to your specific organization.

By applying deconfliction analysis to filter out noise, OpenText Core Adversary Signals delivers a clear view of relevant activity, including where data exfiltration is occurring, how geopolitics are affecting your cybersecurity, and how coordinated attacks are unfolding. OpenText Core Adversary Signals' threat actor attribution capabilities allow you to see beyond digital disguises and multiple proxies to uncover the origins of the adversaries targeting your networks. With OpenText Core Adversary Signals, you gain actionable insights into who is targeting you, where the attacks are happening, and how they're being executed—empowering you to act with precision and protect your most vulnerable assets.

OpenText Core Adversary Signals is an easy-to-deploy SaaS solution that takes an outside-in approach to monitoring threat actors and their activities. It adds a surprisingly simple, yet invaluable layer to your security, enhancing visibility beyond traditional log-based solutions to keep your organization ahead of potential threats. With OpenText Core Adversary Signals, you gain a superior level of detail and perspective, accelerating threat readiness and response without added complexity. It provides the clarity you need to confidently secure your aviation network.

opentext™