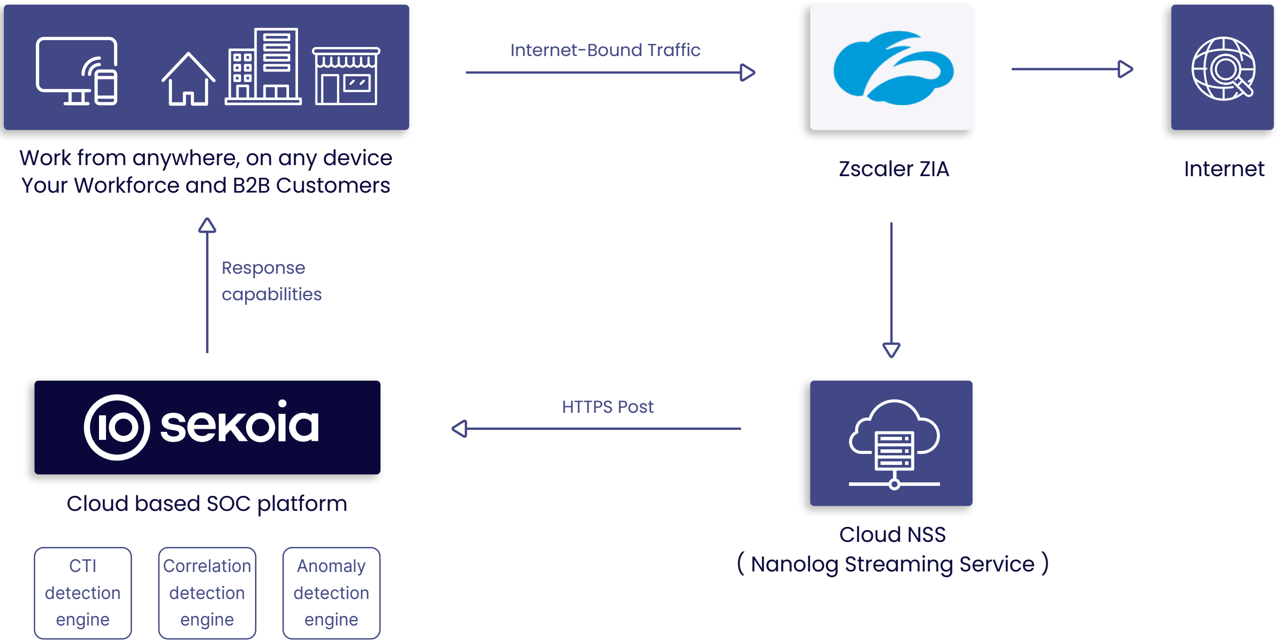
Zscaler and Sekoia.io solution brief

Where the power of ZIA's secure internet access converges with Sekoia.io's cutting-edge Intelligence driven SOC platform.

*In the ever-evolving landscape of cybersecurity, organizations are continually seeking innovative solutions to enhance their network and data security of their on-prem/cloud/hybrid infrastructures. The proliferation of cybersecurity tools that work in silos makes it difficult for operational teams to be effective, requiring them to constantly navigate between the consoles of these tools. The integration of **Zscaler** Internet Access (ZIA) with **Sekoia.io**, an advanced Extended Detection and Response (XDR) platform, offers a compelling solution to solve this problem by centralizing security management within **Sekoia.io**, thereby emphasizing **Sekoia.io**'s unique detection capabilities with its native Cyber Threat Intelligence (CTI) features.*

A SEAMLESS CLOUD-TO-CLOUD INTEGRATION

Zscaler Cloud NSS builds on the foundation of the Nanolog Streaming Service (NSS) to provide a simple and fast way to perform cloud-to-cloud log streaming to a SIEM. **Zscaler** Cloud NSS provides a direct, one-click integration with **Sekoia.io** platform, allowing organizations to focus on data insights instead of maintaining logging infrastructure. **Zscaler** logs are sent via a secure HTTP push, ensuring secure and reliable delivery of logs. This feature is easy to set up and can be configured with a few clicks. Logs start streaming immediately and are normalized within **Sekoia.io**, allowing correlation across the organization’s additional data sources.



Work from anywhere, on any device
Your Workforce and B2B Customers

Internet-Bound Traffic

Zscaler ZIA

Internet

Response capabilities

HTTPS Post

Cloud based SOC platform

CTI detection engine

Correlation detection engine

Anomaly detection engine

Cloud NSS
(Nanolog Streaming Service)

DETECTION IMPROVEMENT AND ORCHESTRATION

Use a single console

The integration of ZIA with **Sekoia.io** centralizes all security functions within a single platform. streamlining security operations. This eliminates the need to navigate between multiple security consoles, thereby streamlining security operations making it more efficient and comprehensive.

Enrich Zscaler logs and alerts

This integration allows **Sekoia.io** to enrich ZIA logs with native Cyber Threat Intelligence (CTI). ZIA generates logs and security event data which are enhanced with real-time threat indicators, IoCs, and contextual information from **Sekoia.io**. This enrichment provides security teams with the necessary data to improve threat detection, incident response, and proactive security decisions, in addition to the base provided by **Zscaler**.

CTI based detection

Sekoia.io CTI detection engine leverages a complete threat intelligence database (modelized in STIX 2.1) and compares it to the events integrated in the SOC platform. This ensures improved detection capabilities and associated threat context to help analysts correctly qualify and mitigate alerts.

Anomaly based detection

Sekoia.io's anomaly detection capabilities help identify deviations from established baselines, enabling organizations to detect and respond to unusual and potentially harmful activities logged by **Zscaler** or other technologies.

Correlation based detection

Sekoia.io's Sigma Correlation engine enhances threat detection by correlating various security events & their behavior (from ZIA and other specific cybersecurity technologies) and creating a more accurate and comprehensive picture of potential threats.

Automated retrohunt

When a new IoC (Indicator of Compromise) is added to the **Sekoia.io** platform, the XDR will search for this indicator in your logs, including historical data. This feature, combined with very strict IoC lifecycle management, ensures powerful automated retrohunt capabilities, with very few false positives. Necessary remediation actions can be taken retrospectively based on traffic logged by **Zscaler** that is considered malicious.

Response capability

Sekoia.io excels in orchestration and incident response through its centralized platform. Its automated capabilities enable swift and consistent responses to streamline incident management by enhancing operational efficiency through its playbooks. Moreover, it empowers security teams to seamlessly orchestrate and control security tools across the entire IT landscape.

zscaler™

About Zscaler

Zscaler *(NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The* ***Zscaler*** *Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform.*

Learn more at ***zscaler.com***
or follow us on Twitter ***@zscaler****.*

About Sekoia.io

Sekoia.io is a European cybersecurity company whose mission is to develop the best protection capabilities against cyber-attacks. Its intelligence-led operational security SaaS platform acts as a true control tower for effective, real-time detection and response to cyber threats. **Sekoia.io** believes that effective protection must enable customers to fully utilize their existing technologies and prioritizes interoperability and standards enforcement in its development.

www.sekoia.io

contact@sekoia.io

BLOG