No-Code, AI-Driven Orchestration and Automation for Agile, Secure, and Resilient Zero Trust Protection

Tines' SOAR platform integrates seamlessly with Zscaler to deliver enhanced security workflows for modern enterprises. Supporting over 65 Zscaler API endpoints and featuring six prebuilt workflows ready for import into any Tines tenant, this integration enables to suit your organization's needs.

With Tines Workbench, security teams can securely harness generative AI to access real-time data, trigger automated responses, and streamline security operations, all from a single chat interface.

Integrated features

- Automated Network Security: Keep access policies up-to-date and block malicious domains automatically, reducing manual work and enhancing security efficiency.
- Faster Incident Response: Use AI-powered workflows to handle incidents in real-time, ensuring rapid threat identification and remediation.
- Unified Security Operations: Centralize security actions across multiple tools, reducing the need to switch between platforms.

Benefits

- Automated Network Security: Keep access policies up-to-date and block malicious domains automatically, reducing manual work and enhancing security efficiency.
- Faster Incident Response: Use AI-powered workflows to handle incidents in real-time, ensuring rapid threat identification and remediation.
- Unified Security Operations: Centralize security actions across multiple tools, reducing the need to switch between platforms.
- Enhanced Threat Intelligence: Enrich alerts and actions with context from tools like URLScan.io and VirusTotal, providing deeper insights and faster responses.
- Quick Deployment: Import prebuilt workflows to your Tines tenant for immediate use, reducing setup time and enabling faster time-to-value.

tines zscaler™

Use cases

Automatically Update Security Policies with Latest Data Center Information

Keep access policies effective by automating the update of security zones with the latest active data center IP ranges from Zscaler, ensuring no manual updates are required and that access policies stay current.

Ingest, Enrich, and Remediate Alerts from Detection Tools, Blocking Malicious URLs

Integrate and enrich security alerts from your existing detection tools using automated workflows. Enrich threat data and automatically add suspicious URLs to Zscaler blocklists to prevent future risks.

Use AI to Create Incident Cases and Automate Remediation Steps

Leverage AI to automatically generate cases from security alerts, initiate workflows, and take remediation steps such as blocking access or sending notifications, ensuring real-time response to incidents.

Block Malicious Domains Based on Threat Intelligence

Automatically block access to suspicious or malicious domains by adding them to Zscaler's blocklist. This ensures a proactive approach to blocking potential threats as soon as they are identified.

Enable URL Allowlist Requests with Threat Enrichment

Allow users to request the unblocking of URLs by submitting forms enriched with threat intelligence. This streamlines decision-making and ensures the safety and accuracy of allowlist additions.

Detect Suspicious Activities from Email Threats and Block URLs

Automatically monitor for suspicious email clicks or other activities and escalate incidents. Block any associated malicious URLs in Zscaler to ensure further protection against phishing or malware attacks.

About Zscaler

Zscaler accelerates digital transformation so 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, the SSE-based Zero Trust Exchange is the world's largest in-line cloud security platform.

Learn more at www.Zscaler.com .