BANDURA®

Smart, Simple, Scalable. Everywhere.

Benefits

- Strengthen network defense Strengthen network defense by taking action at scale with TI to prevent inbound and outbound connections to malicious IPs and domains
- Reduce staff workload by automating IP and domain block listing at scale
- Maximize TI ROI by making it actionable. Increase the ROI and efficiency of existing next-generation firewall (NGFW) investments

Features

- Bandura integrates TI from ThreatSTOP and other sources to block up to 150 million known malicious IPs and domains before they hit your network
- TI and policies from ThreatSTOP are automatically updated in the Bandura platform, ensuring always-current network protection and reduced manual workloads
- TI-driven context from the network edge via the Bandura platform enhances the value of ThreatSTOP TI with increased visibility into malicious IP and domain activity on your network

BANDURA® + ThreatSTOP

Bandura Cyber and ThreatSTOP have partnered to make threat intelligence (TI) actionable at a scale that far exceeds what can be done with existing network security controls. This powerful integration enables organizations to strengthen network defense by proactively using TI from ThreatSTOP in the Bandura platform to block IP and domain-based threats before they hit your network.

The ability to take action on TI at scale is critical to protecting networks from threats and maximizing the value of threat intelligence. However, many organizations experience significant challenges achieving this due to the significant limitations existing security controls have integrating TI. For example, most firewalls have limited capacity to integrate third-party TI indicators of compromise (IOCs). This forces organizations to operate with a limited subset of available TI resulting in suboptimal protection. It also leads to additional downstream effects including increased time and effort spent curating and managing external blocklists.

Bandura Provides Smart, Simple, & Scalable Network Security Everywhere

Bandura blocks known bad traffic at scale using a combination of simple, innovative technology and best-in-class threat intelligence. We provide tens of millions of “out of the box” threat indicators from the world's best sources and offer over 50 point-and-click integrations and connectors: ISACs, ISAOs, Threat Intelligence Platforms (TIPs), SIEMs, SOARs, or any other IP or domain-based source.

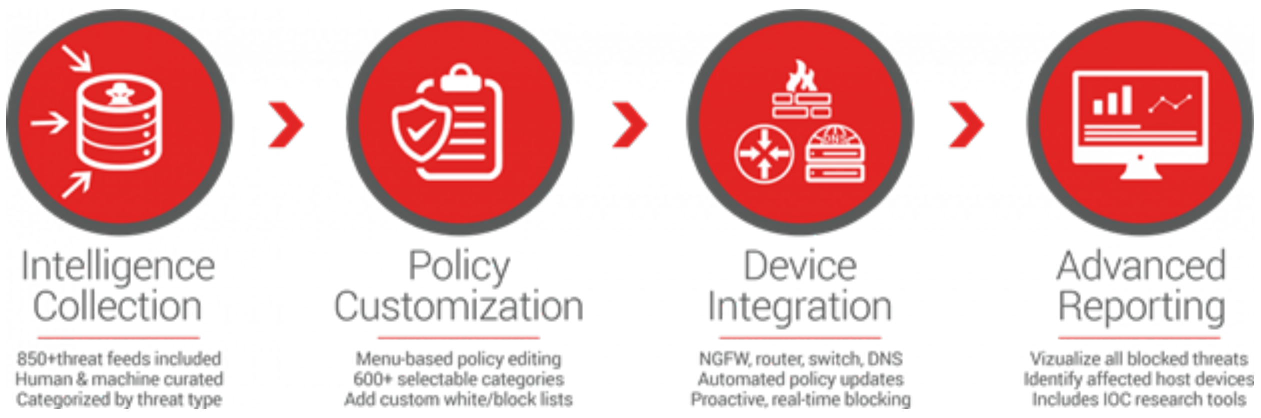
Policy enforcement and blocking is handled by our ThreatBlockr appliances, which can block up to 150M threat indicators in real-time with no latency. ThreatBlockr inspects inbound and outbound traffic and makes simple, policy-based allow or deny decisions based on threat intelligence (IP reputation, block lists, allow lists), GEO-IP, and/or Autonomous System Number (ASN). ThreatBlockr can be flexibly deployed on physical, virtual or cloud appliances, as a cloud-based service or any combination of these. Regardless of deployment, we can protect your users and networks everywhere and our cloud-based management portal gives you a central point of visibility and control.

As data flows through ThreatBlockr appliances, the Bandura platform generates a significant amount of data that helps you analyze your security posture, identify and remediate threats in real time, and easily solve for false positives. Non-PII metadata is sent to our cloud-based management portal to allow quick analysis of your security posture and detailed data is sent to any SIEM, Syslog server or security analytics tool of your choice for further detailed analysis.

ThreatSTOP Platform Overviews & Features

ThreatSTOP is a cloud-based automated threat intelligence platform that converts the latest threat data into enforcement policies, and automatically updates network security controls (firewalls, routers, DNS servers, Threat Intelligence Gateways) and endpoints to stop attacks before they become breaches.

The ThreatSTOP platform blocks unwanted traffic and attacks by preventing connections, both inbound and outbound, with threat actors. This approach means ThreatSTOP can neutralize a broad range of threats including ransomware attacks, DDoS, phishing attempts, and botnets.

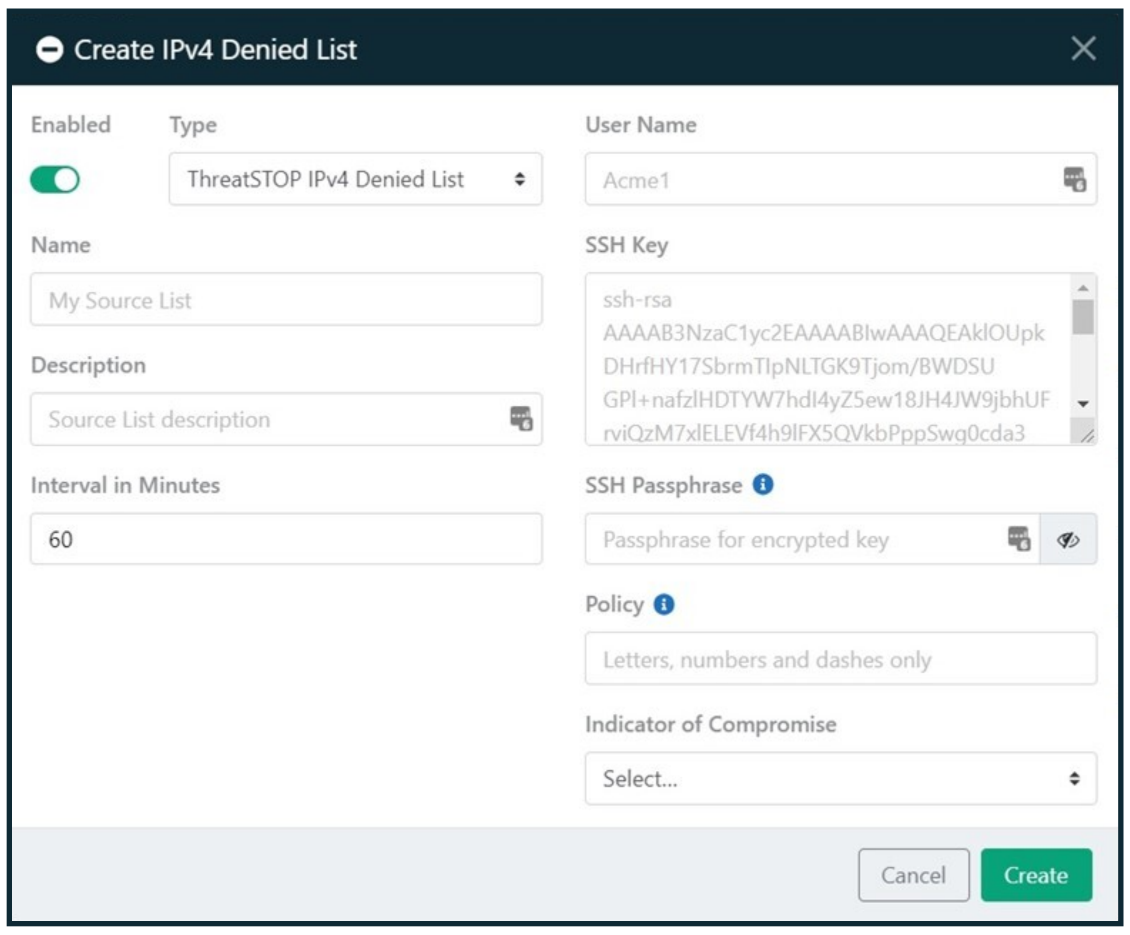

Intelligence Collection
850+threat feeds included
Human & machine curated
Categorized by threat type
Policy Customization
Menu-based policy editing
600+ selectable categories
Add custom white/block lists
Device Integration
NGFW, router, switch, DNS
Automated policy updates
Proactive, real-time blocking
Advanced Reporting
Vizualize all blocked threats
Identify affected host devices
Includes IOC research tools

Threats are continuously discovered by our security researchers, tracked by the 800+ feeds we integrate into our platform, and automatically shared as policy updates for your network and security devices.

- Attacks are prevented by blocking connections with attack infrastructure, stopping new inbound attacks and neutralizing existing infections
- Advanced reporting provides full visibility into blocked connections, and identifies impacted machines, allowing for efficient and accurate remediation
- 100% Cloud-based Security as a Service
- Deploys in under an hour via an online portal on devices you already own
- Custom, user-defined policies are easy to create and manage

The Bandura-ThreatSTOP Integration — Stop Threats At Scale Using Operationalized Threat Intelligence

The Bandura platform can easily integrate and take action using threat intelligence from ThreatSTOP blocking connections to/from known malicious IPs and domains before they hit your network. The integration enables users to create automated Denied and Allowed lists in the Bandura platform using IP and domain-based Policies from ThreatSTOP. IP and domain-based indicators associated with ThreatSTOP policies and the Denied and Allowed lists are automatically updated in real time.



Enabled ●

Type: ThreatSTOP IPv4 Denied List

Name: My Source List

Description: Source List description

Interval in Minutes: 60

User Name: Acme1

SSH Key: ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAklOUpk DHrfHY17SbrmTIpNLTGK9Tjom/BWDSU GPI+nafzIHDTYW7hdI4yZ5ew18JH4JW9jbhUF rviQzM7xIELEVf4h9IFX5QVkbPppSwg0cda3

SSH Passphrase: Passphrase for encrypted key

Policy: Letters, numbers and dashes only

Indicator of Compromise: Select...

The integration of the ThreatSTOP and Bandura platforms strengthens network security, reduces manual workloads, and maximizes threat intelligence ROI by making it actionable.

For more information about Bandura's solutions contact us at 1.855.765.4925 ext 3, or by email at sales@banduracyber.com.