BANDURA®

Smart, Simple, Scalable. Everywhere.

BANDURA® + ThreatConnect™

Bandura Cyber and ThreatConnect have partnered to make threat intelligence more actionable, automated, and scalable. This powerful integration enables organizations to strengthen network defense using curated threat intelligence from ThreatConnect and the Bandura platform to proactively protect your network by blocking IP and domain-based threats.

The ability to take action on threat intelligence is critical to maximizing its value. However, organizations often face challenges integrating threat intelligence into traditional network security controls like firewalls. Most firewalls have limited capacity to integrate third-party threat intelligence indicators Managing external blocklists in firewalls can also be complex and time consuming.

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 30 million "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 Global Management Center 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.

Benefits

- Strengthen network defense by taking action with ThreatConnect threat intelligence to prevent inbound and outbound connections involving malicious IPs and domains
- Reduce staff workload by automating IP and domain block listing at scale
- Maximize threat intelligence ROI by making it actionable and increase the ROI and efficiency of existing next-generation firewall investments

Features

- Bandura integrates threat intelligence from various sources to block up to 150 million known malicious IPs and domains before they hit your network
- Curated, relevant intelligence from ThreatConnect is automatically synchronized to the Bandura platform, ensuring always-current network protection and eliminating manual efforts
- Threat intelligence-driven context from the network edge via the Bandura platform enhances the value of ThreatConnect threat intelligence with visibility into malicious IP and domain activity on your network

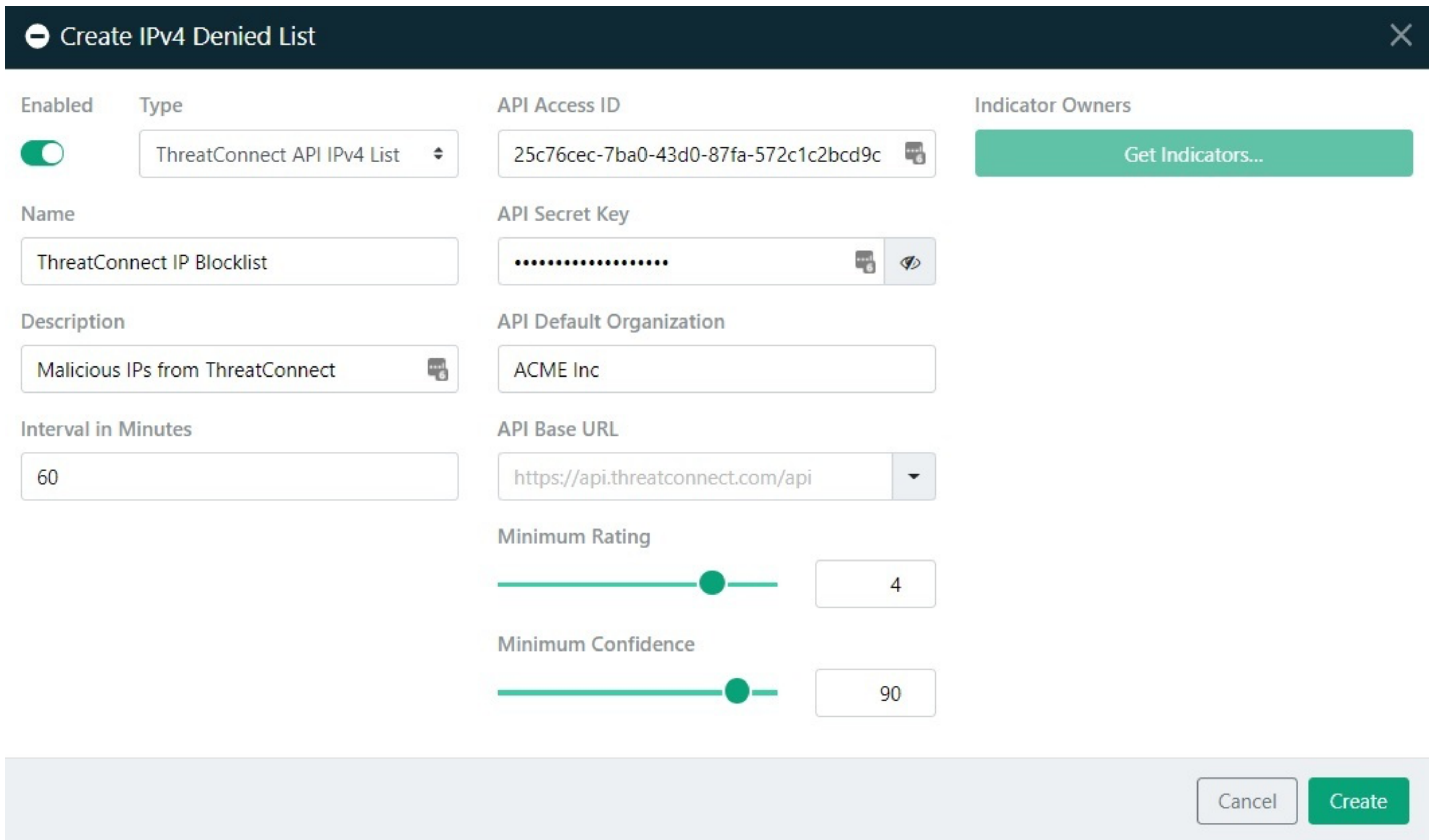
ThreatConnect Platform Overview & Features

ThreatConnect is the place where security comes to work. The only Platform to unite Cyber Risk Quantification (RQ), Threat Intelligence Platform (TIP) and Security Orchestration and Response (SOAR) capabilities, ThreatConnect is a decision and operational support platform that aligns the entire security lifecycle to the goal of reducing risk. Whether used in a standalone fashion, or combined in a single platform ThreatConnect's solutions provide increased accuracy, efficiency, collaboration and automation, enabling a more complete picture of an organization's risks and a better ability to mitigate them.

The Bandura-ThreatConnect Integration — Proactively Block Threats Using Threat Intelligence

The Bandura platform can easily integrate and take action using threat intelligence from ThreatConnect blocking connections to/from known malicious IPs and domains before they hit your network.

Users can easily create automated IP and domain blocklists based on threat indicators from ThreatConnect using the "out-of-the-box" ThreatConnect plugin in the Bandura platform. Blocklists can be configured based on ThreatConnect's Indicator Rating and Confidence Score. Once configured, blocklists are automatically updated.



Create IPv4 Denied List

Enabled	●
Type	ThreatConnect API IPv4 List
API Access ID	25c76cec-7ba0-43d0-87fa-572c1c2bcd9c
Indicator Owners	Get Indicators...
Name	ThreatConnect IP Blocklist
API Secret Key	•••••••••••••••••••
Description	Malicious IPs from ThreatConnect
API Default Organization	ACME Inc
Interval in Minutes	60
API Base URL	https://api.threatconnect.com/api
Minimum Rating	4
Minimum Confidence	90

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