BANDURA®

Smart, Simple, Scalable. Everywhere.

Benefits

- Strengthen network defense by taking action with Anomali threat intelligence to prevent inbound and outbound connections to 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 the Anomali Threat Platform and other sources to block up to 150 million known malicious IPs and domains before they hit your network
- Anomali threat intelligence is automatically updated in the Bandura platform, ensuring always-current network protection and reduced manual workloads
- Threat intelligence-driven context from the network edge via the Bandura platform enhances the value of Anomali threat intelligence with increased visibility into malicious IP and domain activity on your network

BANDURA® + ANOMALI

Bandura Cyber and Anomali have partnered to make threat intelligence more actionable, automated, and scalable. This powerful integration enables organizations to strengthen network defense by proactively using threat intelligence from the Anomali Threat Platform and the Bandura platform to block IP and domain-based threats before they hit your network.

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, and managing external blocklists in firewalls is complex and time consuming.

Bandura Provides Smart, Simple, & Scalable Network Security Everywhere

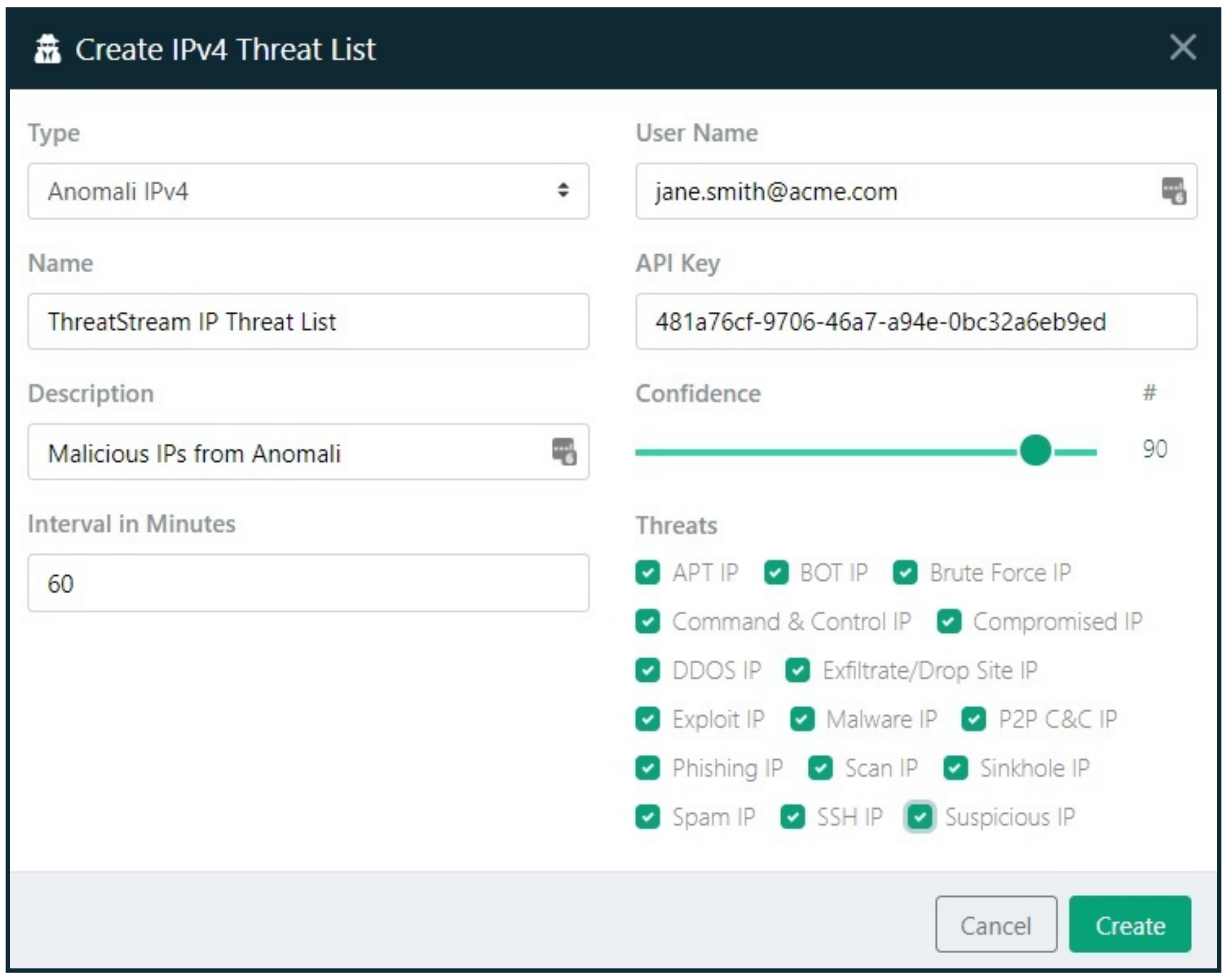
Bandura blocks known bad traffic at scale using a combination of simple, innovative technology and best-in-class threat intelligence. We provide 30 million "out of the box" threat indicators from the world's best sources and offer over 50 point-and-click integrations and connectors: ISACs, ISAOs, Threat 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.

The Bandura-Anomali Integration — Using Threat Intelligence to Proactively Block Threats at Scale

The Bandura platform can easily integrate and take action using threat intelligence from the Anomali Platform blocking connections to/from known malicious IPs and domains before they hit your network. Users can easily create automated IP and domain blacklists based on threat indicators from the Anomali platform. Additionally, using the "out-of-the-box" Anomali plugin available in the Bandura cloud-based Management Portal, users can integrate IP indicators from Anomali into Threat Lists in the Bandura platform. Threat Lists are categorized and scored IP indicators. Users can choose the Categories and Confidence Scores that are integrated into Bandura. Indicators, Categories, and Scores are dynamically updated in real-time.



Create IPv4 Threat List

Type	Anomali IPv4
Name	ThreatStream IP Threat List
Description	Malicious IPs from Anomali
Interval in Minutes	60
User Name	jane.smith@acme.com
API Key	481a76cf-9706-46a7-a94e-0bc32a6eb9ed
Confidence #	90

Threats

☑ APT IP ☑ BOT IP ☑ Brute Force IP
☑ Command & Control IP ☑ Compromised IP
☑ DDOS IP ☑ Exfiltrate/Drop Site IP
☑ Exploit IP ☑ Malware IP ☑ P2P C&C IP
☑ Phishing IP ☑ Scan IP ☑ Sinkhole IP
☑ Spam IP ☑ SSH IP ☑ Suspicious IP

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