BANDURA TIG

BANDURA CYBER

STATE & CITY DATA PROTECTION

How Bandura TIG Aligns to the NIST 800-171 Cybersecurity Framework

Consuming, operationalizing, and sharing threat intelligence is important across the NIST Framework. The **Bandura Threat Intelligence Gateway (Bandura TIG)** enables government organizations of all sizes to easily access, aggregate, and automate threat intelligence and align to the core NIST functions.

5 NIST Framework Functions

Threat Intelligence Gateways & Government Data

The Bandura TIG turns threat intelligence into action, blocking known threats at scale and improving the cybersecurity posture of government organizations. Bandura TIG protects against *millions* of known threats, including ransomware, malware, phishing attacks, and data exfiltration.

Works with existing security investments

The Bandura TIG is typically deployed between the firewall and the router, serving as a first and last line of defense. The Bandura TIG integrates into an existing security environment, working with SIEMs, TIPs, IDS/IPS, and other systems.

Automate MS-ISAC feeds & protect from nation-state actors

By aggregating and automating MS-ISAC and other threat feeds, Bandura TIG identifies and automatically blocks threats from entering and exiting your network with almost zero latency. Automated threat feed updates and policy application means your organization is always protected.

Turnkey solution that reduces workload on staff and firewalls

Bandura TIG reduces the load on next-general firewalls and the workload of security staff—reduce or eliminate the need to manage threat feeds and update firewall rules. The plug-n-play solution can be installed in less than 30 minutes, and requires no technical expertise to set up or to run.

Identify - Internal & external threat intelligence aggregation & automation (MS-ISAC, etc)

Protect - Massive blocking of known IP & Domain threats (such as ransomware, malware, etc)

Detect - Visibility into malicious traffic on network

Respond - New threat indicators rapidly deployed via automation & enforced

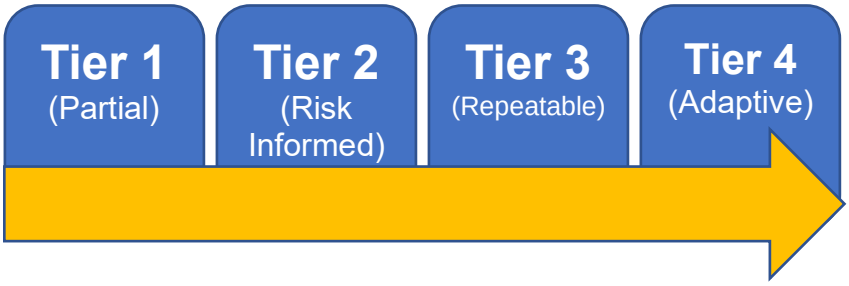
www.BanduraCyber.com
1.855.765.4925 | sales@banduracyber.com

TIGs Promote Alignment with Multiple NIST Key Framework Functions

Framework Function	How a Bandura TIG helps	Category
Identify	Bandura TIG comes pre-integrated with millions of threat indicators from commercial, open source, industry (i.e. MS-ISAC blacklists), and government sources, enabling organizations to better identify cyber risks and threats. With Bandura TIG, you can easily, and cost effectively leverage threat intelligence to gain greater visibility into cyber threats on your network.	• Risk Assessment (ID.RA)
Protect	Bandura TIG operationalizes threat intelligence to threat intelligence with preventive access control to stop unwanted or unauthorized activity from occurring. Bandura TIG blocks the massive volume of known threats before they get to the firewall, protecting organizations' critical data and assets.	• Identity Management, Authentication and Access Control (PR.AC) • Data Security (PR.DS)
Detect	Bandura TIG provides visibility into malicious traffic on your network, enhancing security monitoring efforts. Bandura TIG monitors the traffic attempting to get in/out of your network and works with other security systems to make sure pro-active detection across the perimeter is synchronized across each layer of defense.	• Anomalies and Events (DE.AE) • Security Continuous Monitoring (DE.CM) • Detection Processes (DE.DP)
Respond	New threat indicators can be rapidly deployed in near-real time via automation and enforced by the Bandura TIG, containing incidents and preventing future occurrences.	• Communications (RS.CO) • Analysis (RS.AN)

Bandura TIG & The NIST Framework Implementation Tiers

Bandura TIG can also help organizations progress along the NIST Framework Implementation tiers.



Framework implementation tiers incorporate a progressive use of threat intelligence and information sharing as one goes from Tier 1 (Partial) to Tier 4 (Adaptive).

Because Bandura TIG enables an organization to leverage threat intelligence to identify, protect, detect, and respond to cyber threats it represents a key technology to enable organizations to progress along the NIST Framework maturity spectrum.

For example, at Tier 1, an organization can leverage Bandura TIG to gain greater visibility into cyber threats and risks. As the maturity of a security operation increases, our solution can be leveraged to incorporate more sources of threat intelligence, enable greater intelligence information sharing (i.e. STIX and TAXII support), and enable more dynamic and adaptive threat-intelligence driven protection (i.e. new threat indicator identified by SIEM system; indicator automatically pushed out to Bandura TIG for enforcement).

www.BanduraCyber.com
1.855.765.4925 | sales@banduracyber.com