NOZOMI NETWORKS

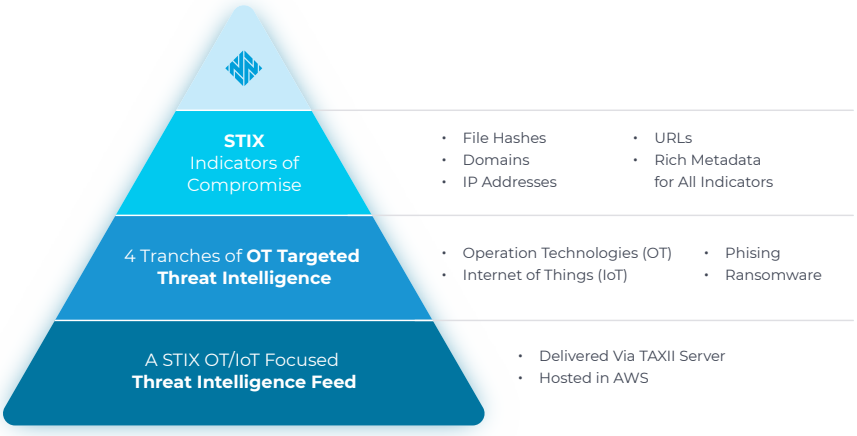
DATA SHEET

Threat Intelligence Feed

Leading OT and IoT Threat Intelligence Data for Third-Party Security Solutions and Platforms

The Nozomi Networks Threat Feed is a data feed of the latest emerging threat data from across the industry that can be used outside or independent of our Guardian and Vantage platforms with other third-party security platforms.

This data feed is comprised of Nozomi Networks' operational technology (OT) Indicators of Compromise (IOCs). It can be used by any security platform that can ingest Industry-compliant Structured Threat Intelligence eXpression (STIX 2.1) Objects. The content is hosted on Nozomi Networks Trusted Automated eXchange of Intelligence Information (TAXII) server in the cloud and can be accessed globally.



Threat Intelligence Feed is broken into several data sources and formats for a range of OT, IoT and ICS threats, source information and IOCs.

Anticipate

Assess risk profiles across assets and sites based on latest indicators of compromise

Diagnose

Identify threat actors, their methods and vectors to gain access to systems

Respond

Disrupt and develop effective strategies for defending against attacks in a variety of platforms

What's in the Threat Feed?

A threat intelligence feed (TI feed) is an ongoing stream of data related to potential or current threats to an organization's security.

TI feeds provide information on attacks, including zero-day attacks, malware, botnets and other security threats. TI feeds are vital components of security infrastructure, which help identify and prevent security breaches. Threat intelligence can be used to implement more granular security policies, as well as to identify potential characteristics or behaviors associated with that threat.

The new Threat Feed is consistent with the Nozomi Networks Threat Intelligence subscription, which is solely for use in Nozomi Networks' own Guardian and Vantage products but allows other platforms to leverage the research and intelligence on recent and emerging threat indicators and how they are spreading. It does not include more sophisticated Nozomi Networks packet rules or YARA rules.

Threat Feed allows other platforms to leverage Nozomi Networks research and intelligence on recent and emerging threat indicators and how they are spreading. The feed delivers a single, unified source of data, including malicious IP addresses or URLs, new indicators of compromise (IOC) signatures, threat sources, malware hashes, and methods and tactics to gain system access, all of which can serve to accelerate incident response and enhance security operations.

Indicators of Compromise (IOC) Classes Included in the Feed

✓ Malicious URL	✓ Malicious MD5
✓ Malicious Domain	✓ Malicious SHA-1
✓ Malicious IP Address	✓ Malicious SHA-256

Supported Security Platforms

The Threat Intelligence Feed is compliant with a wide range of security platforms from Security Information and Event Management (SIEM) tools, next-generation firewalls and endpoint detection and response systems.

Azure Sentinel, Splunk, QRadar are examples of tools that can easily import Nozomi Threat Feed. Additionally, Threat Feed can integrate with any solution designed to ingest third-party Threat Intelligence, to empower security professionals to more effectively hunt for threats in their own data.

Let's get started

For more details on specific product support and deployment options, please reach out to your local Nozomi Networks sales teams or Nozomi Networks partner network.

Contact Us

nozominetworks.com/contact

Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

NOZOMI NETWORKS

nozominetworks.com