NOZOMI NETWORKS

PRODUCT OVERVIEW

OT/IoT Threat Intelligence Feed for Third-Party Security Solutions

Organizations managing OT, IoT and cyber-physical systems (CPS) face increasingly sophisticated cyberattacks that leverage advanced methods, targeted campaigns, and specialized tactics. These challenges demand robust cybersecurity strategies enriched with timely and actionable threat intelligence.

Nozomi Networks offers a specialized OT/IoT Threat Intelligence Feed developed by our expert security researchers. The feed integrates emerging threat data to bolster the cybersecurity posture of industrial and critical infrastructure organizations. The feed provides real-time insights into threats targeting OT, ICS, and IoT infrastructures, enabling proactive defense.

This feed includes Indicators of Compromise (IOCs) in STIX 2.1/ JSON format, hosted on Nozomi's TAXII server. It integrates seamlessly with third-party security platforms and functions independently from the Nozomi Networks platform, offering flexible deployment options.

The Nozomi Threat Intelligence feed delivers critical insights on attacks, including zero-day exploits, malware, and botnets. These feeds enhance incident response, improve security operations, and support the implementation of granular security policies, helping organizations quickly identify and address potential threats.

Supported Users

- **MSSPs & Systems Integrators:** Enhance client protection with integrated threat intelligence.
- **National and Industry CERTs:** Respond effectively to incidents using current threat data.
- **OT/IoT Vendors:** Improve product security and ensure regulatory compliance.
- **Security Technology Partners:** Integrate advanced detection capabilities into existing tools.
- **OT/IoT Asset Owners:** Monitor and safeguard own critical infrastructure.

Key Benefits of the Nozomi OT/IoT Threat Intelligence Feed

Enhanced Threat Landscape Visibility

Strengthen SOC capabilities by providing comprehensive insights into threat actor behaviors, specifically targeting OT, IoT and CPS environments.

Rapid Time-to-Value

The OT/IoT Threat Intelligence Feed integrates quickly and seamlessly into existing cybersecurity systems, significantly improving threat detection and incident response capabilities. It helps minimize operational disruptions associated with cyberattacks while driving revenue growth for OT, IoT and CPS asset owners and security service providers.

Unique Expertise

World-class security researchers and analysts from Nozomi Networks Labs track threat data from numerous public and private sources, leveraging our global network of thousands of threat sensors installed in industrial and critical infrastructure environments.

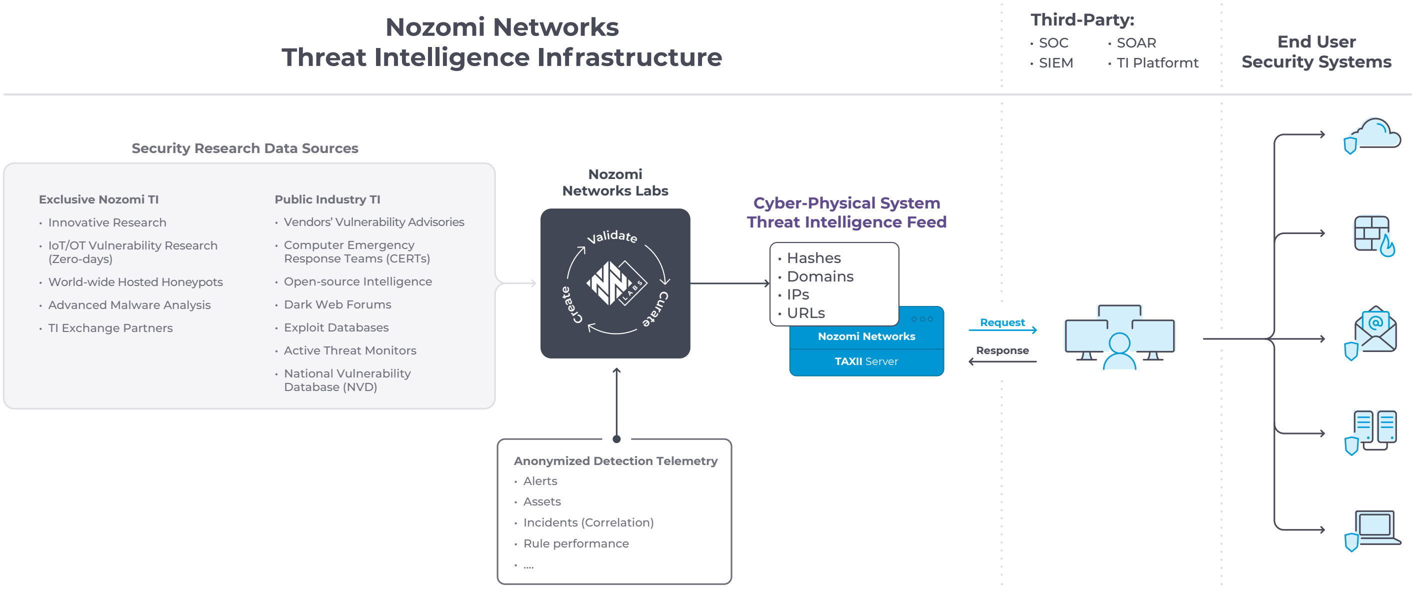
Focus on Cyber-Physical Systems

Unlike traditional IT threat intelligence, the Nozomi OT/IoT Threat Intelligence Feed focuses on threats to ICS, OT and CPS, addressing the attack techniques and vulnerabilities that are specific to these environments.

Regulatory Confidence

Threat intelligence sharing helps ensure compliance with evolving critical infrastructure cybersecurity regulations and frameworks. For instance:

- The NIST Cybersecurity Framework (CSF) 2.0 emphasizes the integration of cyber threat intelligence into organizational risk assessment processes. Specifically, Subcategory ID.RA-02 under the Risk Assessment Category (ID.RA) states: "Cyber threat intelligence is received from information sharing forums and sources."
- EU NIS 2 Directive's preamble 119 states: "With cyber threats becoming more complex and sophisticated, good detection of such threats and their prevention measures depend to a large extent on regular threat and vulnerability intelligence sharing between entities."



Threat Feed Details

- **Focus area:** OT, IoT, Hacking Frameworks, Phishing, Ransomware.

- **Threat intelligence sources**, tracked by Nozomi Networks security researchers:
  - Public: Open-Source Intelligence, Criminal Dark Web Forums, Exploit Databases
  - Private:
    - Global network of threat sensors in industrial and IoT environments
    - World-wide Hosted Honeypots Sensors
    - Innovative Vulnerability, Malware, and Attack Research
    - Threat Intelligence Exchange Partners

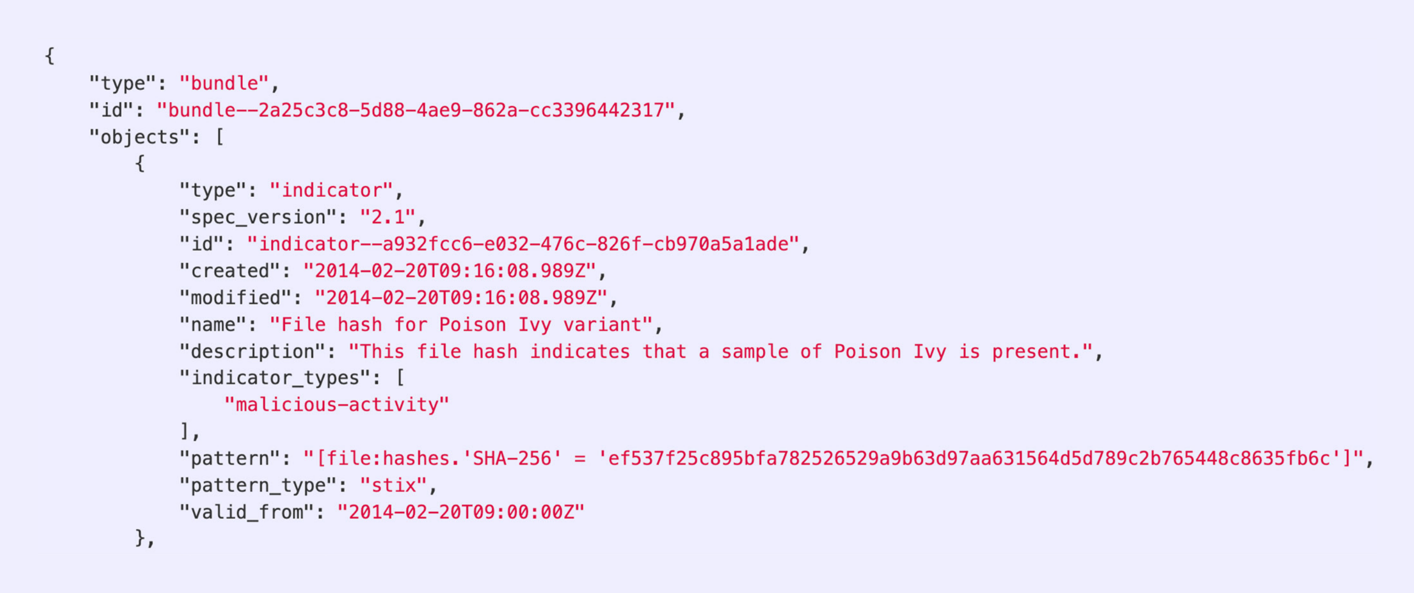
- **Threat indicator format:** Industry-compliant Structured Threat Intelligence eXpression (STIX 2.1/JSON) Objects, Delivered Via TAXII Server Hosted in AWS.

- **Types of indicators:** Malicious URLs, Domains, IP Addresses, File hashes (MD5, SHA1, SHA25).

- **Contextual data:** Each record in the Threat Feed includes actionable details such as threat names, timestamps, and descriptions. By providing context, the feed helps answer critical questions such as 'who, what, where, and when,' empowering organizations to identify adversaries swiftly and take decisive action.

- **Threat feed update frequency:** Indicators are continuously updated, with a minimum frequency of twice per week. This ensures the feed reflects the latest emerging threats and attack vectors, helping organizations stay proactive and ahead of evolving cyber risks.

- **Number of indicators:** Millions of indicators are available, and the dataset is continually and dynamically expanding to address emerging threats.



```
{
    "type": "bundle",
    "id": "bundle--2a25c3c8-5d88-4ae9-862a-cc3396442317",
    "objects": [
        {
            "type": "indicator",
            "spec_version": "2.1",
            "id": "indicator--a932fcc6-e032-476c-826f-cb970a5a1ade",
            "created": "2014-02-20T09:16:08.989Z",
            "modified": "2014-02-20T09:16:08.989Z",
            "name": "File hash for Poison Ivy variant",
            "description": "This file hash indicates that a sample of Poison Ivy is present.",
            "indicator_types": [
                "malicious-activity"
            ],
            "pattern": "[file:hashes.'SHA-256' = 'ef537f25c895bfa782526529a9b63d97aa631564d5d789c2b765448c8635fb6c']",
            "pattern_type": "stix",
            "valid_from": "2014-02-20T09:00:00Z"
        },
```

Supported Security Platforms

The Nozomi OT/IoT Threat Intelligence Feed can **integrate with any solution** designed to ingest third-party threat intelligence, to empower security professionals to automate the initial alert triage process and more effectively hunt for threats in their own data.

It is **compliant with a wide range of security platforms** from security information and event management (SIEM), security orchestration, automation and response (SOAR), threat intelligence platforms (TIP), incident response tools, next-generation firewalls (NGFW) and endpoint detection and response (EDR) systems.

Azure Sentinel, Splunk and QRadar are examples of tools that can **easily import the Nozomi OT/IoT Threat Intelligence Feed**.

Let's get started

Discover how the Nozomi OT/IoT Threat Intelligence Feed can transform your OT, IoT and CPS cybersecurity approach. Connect with your local Nozomi Networks sales team or an authorized partner to learn more and start your journey towards enhanced security.

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