Shield 24x7 NBAD Capabilities

AI-ML Powered Network Behavior Anomaly Detection

Network Behavior Anomaly Detection in 2023

NBAD - or Network Behavior Anomaly Detection has a long history that goes back to the year 2000. At the time, tools like IDS and IPS were growing rapidly and the open-source Snort project was the foundation of many network security programs. The primary deployments and research were being done in the Federal Space.

There was general acknowledgment by the community that signature detection models were great at known exploits, and behavior detection models were great at 0-day exploits, the need to apply anomaly detection models to identify credential abuse was growing and that effort was led by George Tech's Dr. John Copeland's StealthWatch system.

NBAD solutions were first built on packet capture and soon supplemented by NetFlow in 2004. NBAD is widely deployed as a continuous monitoring of a network for unusual events or trends. NBAD is an integral part of network behavior analysis (NBA), which offers security in addition to that provided by traditional anti-threat applications such as firewalls, intrusion detection systems, antivirus software, and malware-detection software.

Today's modern NBAD Solutions can detect the following threats at scale at high speed across billions of network connections

- Deviations in traffic volume, bandwidth use, protocol use, packets, or bytes
- Never seen before internal IP addresses, accounts, or devices
- Login failures, admin activity, inactive accounts, or impossible travel
- Risky IP addresses, locations, devices, or user agents

Shield 24x7's NBAD Capabilities

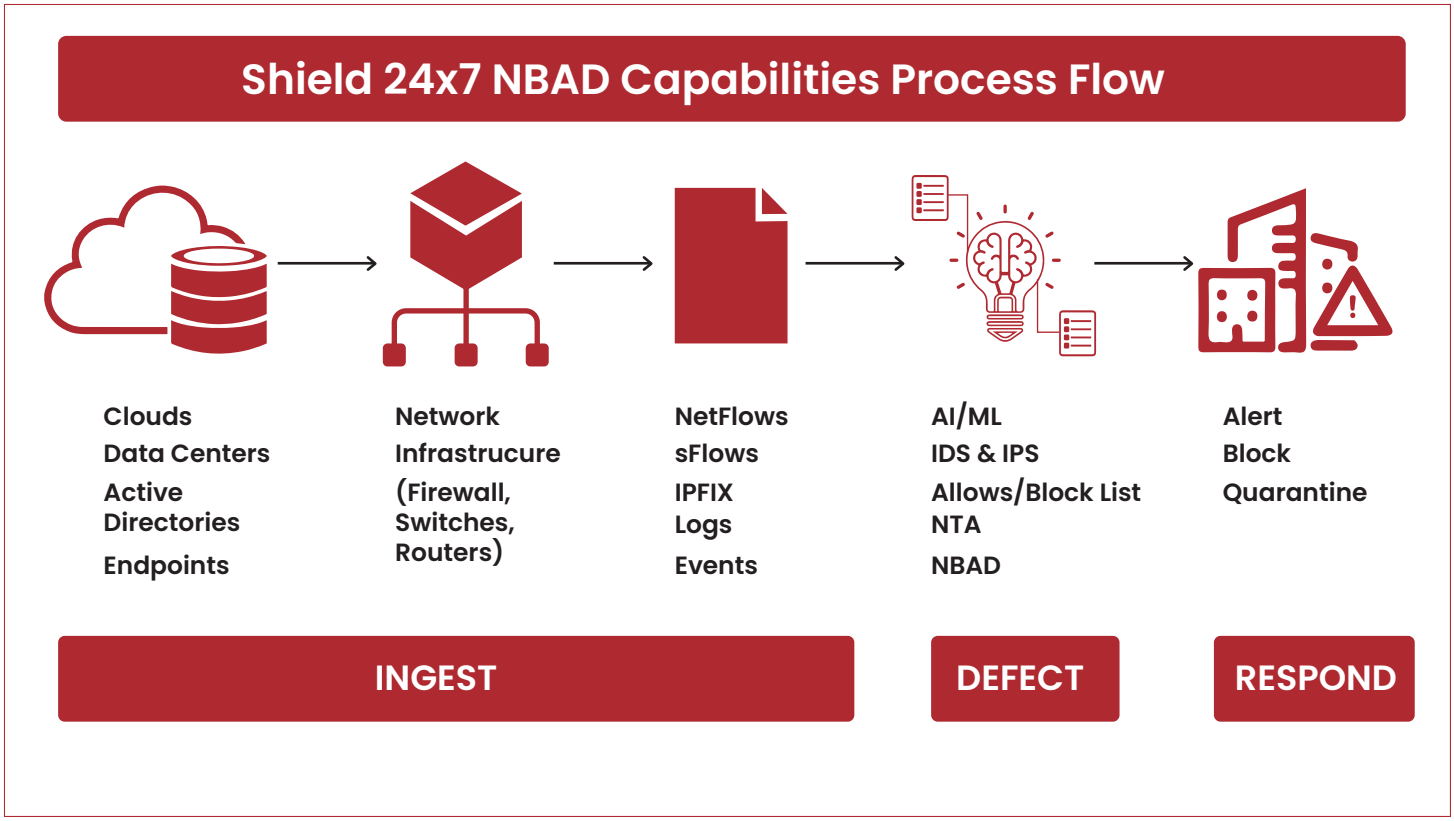
Shield 24x7's aiSIEM and aiXDR threat detection and response platform includes network behavior anomaly detection that integrates network metrics and behavioral data to enable security teams to identify and respond to network threats. It provides analytics and context for each event and shows the details of the compromised assets and actors.

Shield 24x7 network behavior anomaly detection capabilities uses AI and ML to monitor network activity and alert network teams of suspicious events and network behavior anomaly detection complements traditional security tools & fills the gaps in network protection network. Our NBAD capabilities complements your other cybersecurity tools, such as firewalls and network performance monitoring software, by finding hidden threats that they might miss. Seceon's NBAD capabilities can also:

- tracks the behavior of individual network users, depending on the configuration.
- scans the entire enterprise network for threat actors, unlike perimeter, firewall, & endpoint security systems that only cover specific parts of the network

Shield 24x7's NBAD considers three major network properties: traffic flow patterns, passive traffic analysis, & network performance data—from across the network to detect several different types of threats, such as:

- **Inappropriate network behavior** - Unauthorized apps or unusual port usage by known applications are examples of inappropriate network behavior.
- **Data exfiltration** To detect and prevent data exfiltration, network behavior anomaly detection monitors the volume and destination of outbound data transfers in real-time.
- **Hidden threats** - Seceon's NBAD capabilities use AI/ML and a large number of threat intelligence feeds to discover advanced malware, ransomware C&C, and persistent threats to enterprise networks.



How do Shield 24x7's NBAD capabilities work?

Shield 24x7's core design principle has always been to ingest as much data for both the detection systems and to enable context and situational awareness. Shield 24x7 ingests all forms of network metadata from NetFlow, sFlow, and IPFIX to firewall logs, allow/block lists, to cloud and endpoint logs, and events to Active Directory.

Shield 24x7's network behavior anomaly detection capabilities start by creating a baseline of the average user and network behavior, regardless of the network or tool configuration. The baseline is based on behavior data collected over a period of time and the longer the period, the better and more useful the data. Shield 24x7's detection models identify deviations from the 'normal' activities and behaviors in real time.

After detection is made, based on the risk score, Shield 24x7's flexible alerting and response capabilities take over and respond. Protection and response based on automated remediation (based on incident triaging and or prebuilt playbooks) and real-time remediation.

About Shield 24x7

Shield 24x7 reduces cyber threat risks and security stack complexity while significantly improving the ability to detect and block threats and breaches at scale. Shield 24x7's Open Threat Management (OTM) platform enhances and automates security with our AI and ML-powered aiSIEM and aiXDR solutions. The platform provides comprehensive coverage by collecting telemetry from logs, identity management systems, networks, endpoints, clouds, and applications. This data is enriched and analyzed in real-time using threat intelligence, AI and ML models based on behavioral analysis, and correlation engines to generate reliable and transparent detections and alerts. Shield 24x7 supports over 8,000 clients by delivering high-margin, efficient security services with automated cyber threat remediation and continuous compliance.

Learn more about Shield 24x7 NBAD

Schedule a Demo