Recorded Future®

SOLUTION BRIEF

Recorded Future Network Traffic Analysis

Network Traffic Analysis (NTA) involves the monitoring and analysis of network data to identify anomalies, providing insight and context on malicious infrastructure connected to your network. Attackers use these malicious connections to send commands, receive infection updates, and exfiltrate an organization's data. Through NTA, an organization can gain visibility into when the malicious hosts connect to a network and can warn when those connections exfiltrate data from a network. NTA provides real-time, actionable warning intelligence to security teams on adversarial actions and which stage of an attack they are in.

Going beyond traditional NTA, which is based on internal information, Recorded Future leverages external data and is able to identify and analyze activity between a network and external adversary control points. Using proprietary collection and analytics, Recorded Future observes traffic between victim networks and the attacker, identifying an attacker's infrastructure from building, to staging, and the launching of an attack.

Recorded Future's insight into adversary infrastructure is based on a decade of proprietary intelligence data. Recorded Future analyzes volumes of internet traffic data to produce very specific insights into suspicious and malicious behavior based on evidence. Examples of observed network traffic includes, but is not limited to, Botnets, Malware Distribution, DDoS, Scanning, Command and Control, and Exfiltration of Data.

With Recorded Future NTA, clients can monitor, detect, and research adversaries and their malicious activity in real time, enabling them to shut down attacks before damage to an organization is done:

Uncover State-Sponsored Activity
Recorded Future's Insikt Group provides in-depth reporting and analysis of state-sponsored actors that goes beyond the news stories. Insikt Group uses NTA to identify and tag adversary activity, allowing security teams to surface the latest findings and identify current state-sponsored activity.

Identify High-Fidelity Adversary Infrastructure
Eliminate low-confidence and false positive detections with high-fidelity, active infrastructure identification. Insikt Group continually evolves detection rules to classify and improve its proprietary Intelligence Graph. By automating Insikt Group expertise, confidence is generated from context, helping teams expedite detection and remediation.

Track Adversary Group Infrastructure
Security professionals can analyze network traffic from adversary infrastructure, identifying and tracking active attacks against an organization or its supply chain. Using the Recorded Future Threat Intelligence module, security teams can proactively reveal attacks before they're targeted.