Detect Threats Early and Follow Attacker Movement Across the Network

Leveraging Rapid7 Network Traffic Analysis (NTA) in InsightIDR

InsightIDR offers the complete approach to threat detection and response. By combining the most impactful components of technology and service, we’re able to analyze extensive event data from across modern environments and transform it into actionable insights and detections.

The addition of Network Traffic Analysis to InsightIDR means teams have all of their critical security data in one place. By eliminating blind spots—including those traditionally in the network edge and perimeter—InsightIDR helps teams work more effectively and focus their talent on the threats that matter most.

Get Up and Running Quickly with the Insight Network Sensor

InsightIDR boasts the best deployment times in the industry, and this commitment to immediate time to value continues with NTA. The Insight Network Sensor is easily downloaded and deployed, either on-premises or on a virtual VMware network. The sensor collects all network traffic metadata for analysis and observation on the central management portal, without interacting with other devices or impacting network performance. This network traffic data is passed to InsightIDR and aggregated with other critical data sources.

Figure 1: An example deployment of the Insight Network Sensor. A SPAN or mirror port is configured at the network core, which allows the capture of any traffic passing through (both north-south and east-west).
Unlock Maximum Visibility with Network Traffic Analysis

Every user and device on a network leaves a trail of traffic data. This data is incredibly valuable for investigations and forensic activities because it’s nearly impossible for malicious actors to tamper with, and it can reveal the steps (or even location) of attackers in real time.

The Insight Network Sensor collects network flow metadata that details this rich traffic information in human-readable metadata, attributed to specific users and devices. Think of it as a closed circuit television, providing real-time visibility and monitoring across your network. With flow data, you can see inbound and outbound traffic outside of your headquarters country, inbound Remote Desktop Protocol activity from external clients, active server ports that may reveal unknown or unwanted systems on the network, and more. Most importantly, this data can help retrace the steps of an intruder in your network—making it invaluable for investigations and forensic activities.

Detect Threats Early and Reliably

Network traffic offers a new axis for attacker detection. This happens through Intrusion Detection System (IDS) events and alerting around known bad attacker activity, as well as custom alerting around flow data to recognize unknown threats and unique anomalous activity on your network.

Traditional IDS tools can be incredibly noisy. The Rapid7 MDR team has carefully analyzed thousands of IDS events to curate a list of only the most critical and actionable events to be alerted on. This means when malware, botnets, or other compromises are detected, teams won’t have to go through tedious cycles to determine their validity. Analysts can take action confidently, on reliable, expertly vetted detections.

Reduce Complexity with InsightIDR

With the data transformation, attribution, analysis, and detection in InsightIDR, customers get comprehensive coverage across their environment to find threats early—without creating more work for security teams. All InsightIDR and MDR customers have free access to the Insight Network Sensor, IDS events, and DNS and DHCP data captured by the Sensor included in their subscription. For a small add-on, InsightIDR and MDR Elite customers can also access the advanced visibility and monitoring capabilities that flow data unlocks.

About InsightIDR

InsightIDR cuts through complexity and noise to accelerate detection and response with reliable alerts, high-context investigations, and automation. Powered by insights from our MDR, research, and threat intelligence teams, InsightIDR aggregates and analyzes data sources across logs, users, endpoints, and network to notify teams at the first signs of attack.

To learn more about Network Traffic Analysis in InsightIDR, visit rapid7.com/IDR-NTA

Support

call +1.866.380.8113

Customer Portal

See why Gartner named Rapid7 a leader in the 2020 Magic Quadrant for SIEM. Visit rapid7.com/siem-leader

©RAPID7 2020