NETOGRAPHY

Threat Hunting with Netography Fusion®

What is Threat Hunting?

The practice of searching for advanced threats missed by security controls to mitigate risk.

The Challenge

Whether initiated by an attack that has already happened against an organization or third-party intelligence about a new threat potentially targeting their organization, security teams engage in threat hunting to mitigate risk. Any effective threat hunting tool needs to be a flexible and capable detection platform first. This provides threat hunters with a starting point to test theories and creates proactive, actionable signals for specific use cases in their environment. These detection capabilities may include:

- Lateral movement
  - Using machine learning to help identify "loud" hosts
  - Looking for anomalous destinations and times of day on a per-host basis
- Command and Control
  - Detecting communications with C2 hosts
  - Responding vs. alerting to stop communication when detected
- Data accumulation
  - Using machine learning to identify data staging anomalies
- Data exfiltration
  - Detecting files being transferred to cloud hosting providers using machine learning to identify baselines and act when detected
- Abnormal activity
  - Analyzing traffic which is abnormal
  - Establishing a baseline and spotting anomalies with little to no user interaction
- Verifying zero-trust policies
  - Detecting and acting on policy violations

Individually, these capabilities are extremely helpful in finding traces of anomalous activity and indicators of compromise and closing gaps in security controls. However, when used in combination, they can provide a complete picture of the attack path to accelerate response and reduce the impact of an attack. For example, in the case of ransomware, threat hunters can combine visibility into abnormal activity with lateral movement and act to alert/block activity across the enterprise network and limit the blast zone.

Threat hunting is particularly challenging for modern enterprises with Atomized Networks, meaning they are dispersed, ephemeral, encrypted, and diverse. Threat hunters struggle to get the network visibility and control they need when networks are composites of multi-cloud, hybrid-cloud, and on-premises infrastructure and are extremely fluid. The pervasive use of encryption is blinding traditional network detection and response (NDR) tools that rely on deep packet inspection (DPI), and each environment has its own set of tools for monitoring and security with very little overlap which adds further complexity to the threat hunter's job. This is where Netography Fusion takes the lead.

How Netography Fusion Meets the Threat Hunting Challenge

Netography's SaaS-based architecture enables rapid and low friction deployment to deliver real-time visibility, detection, and response capabilities when and where they are needed, across the entire Atomized Network – multi-cloud, hybrid-cloud, and on-prem infrastructure.

We do this by taking cloud flow logs from all the major cloud providers—Amazon Web Services, Google Cloud, IBM Cloud, Microsoft Azure, and Oracle Cloud—as well as on-prem network flow logs. We aggregate and normalize that disparate data to have a consistent and simple language, Netography Query Language (NQL). We use an API-driven, bi-directional conduit to integrate with specific data sets for intelligence and with tools like an organization's SIEM, SOAR, and EDR. This allows us to enrich flow logs with context at the time of ingestion to add meaning right away, with no additional work required. It also allows us to send context-rich signals back to an organization's existing operational infrastructure for remediation.

Netography Fusion provides a single pane of glass and intuitive UI, so operators have an easy way to get the answers they need about what's on their network, what it is doing, what's happening to it, and what actions to take. Threat hunting teams can create individual dashboards for their environment and the specific issues they want to search for using NQL.

This could include:

- **Misconfigurations that could lead to other issues. For example, EC2 instances in an AWS environment that allow far too many holes inbound from everywhere on the Internet, or finding DNS misconfigurations.**
- **Evidence into anomalous behavior as it happens. For example, visibility into suspicious IPs in one office and pivoting quickly to search and match those IPs to a cloud instance in order to stop malicious activity in its tracks.**
- **More advanced hunts. For example, conducting additional analysis of the suspicious IP with visibility into data from honeypots, log management tools, and servers, and filtering out data that isn't relevant to tie detections together and identify the guilty server. Using time series charts of inbound and outbound server traffic to isolate a timeframe for the activity. Finally, using NQL to pivot into IP reputation data and geo activity to see the origination point for the IP connection, block the ingress point, and conclude the hunt.**

Supercharge Your Threat Hunting Program

With Netography, threat hunting teams benefit from a single source of truth, the enrichment of flow logs, and the power of having context for their entire Atomized Network. With gap-free network visibility, flexible data retention policies and custom, granular searches to investigate incidents and understand the attack path, teams can implement proactive measures to reduce attacker dwell time and prevent future intrusions.

About Netography

Netography® has created the first network-centric platform that reconstitutes capabilities disrupted by the combined impact of encryption and Atomized Networks across the security world. Netography Fusion® is for enterprise security operations center (SOC) and cloud operations teams that need scalable, continuous network visibility across the Atomized Network – legacy, on-premises, hybrid, multi-cloud, and edge environments.

Learn more at netography.com.

NETOGRAPHY