NETWORK VISIBILITY TOOL

YOU CAN'T INVESTIGATE WHAT YOU CAN'T SEE

And it's next to impossible to secure what you can't investigate. Enterprise networks are diverse, dynamic and complex, which makes it easy for attackers to obfuscate their tracks once inside. As networks grow and expand, it becomes increasingly difficult for security teams to know that controls and rules are working, security audits are thorough, and alerts and incidents are being effectively validated and responded to.

CLARITY BEGINS WITH VISIBILITY

The Masergy Network Visibility Tool (NVT) provides an actual up-to-the-second record of all network activity over a period of three months and adds context to security events by synthesizing data from multiple network metadata sources and illustrating it across a user-friendly, workflow-driven interface. The attacker's main enabler is the network, and you must be able to visualize where the attacker has been and is going in order to enable your defenses.

By combining and cross-referencing the synthesized data, Masergy's Network Visibility Tool provides network context—a more complete picture that makes responding to security events faster and more effective.

USE CASES

- Identify problems with security controls and firewall rules so they can be fixed
- Deploy simple rules for identifying abnormal connections to critical assets, as well as unusual external dataflows indicative of data exfiltration
- Execute threat intelligence matching on network traffic retrospectively, to overcome time-sensitive nature of intelligence data
- Support threat hunting and other investigations on infected systems with a complete history of related network activity

CONTACT US: USA +1 (866) 588.5885 | UK +44 (0) 207 173 6900 | sales@masergy.com

ACCELERATE

IDENTIFICATION OF MALICIOUS ACTIVITY

IMPROVE

EFFECTIVENESS OF SECURITY INVESTIGATION AND RESPONSE

RESOLVE

CHALLENGING NETWORK AND SECURITY PROBLEMS

NETWORK METADATA WITH TAILORED INSIGHT

Using NetFlow/sFlow, the Masergy Network Visibility Tool collects and stores all up-to-the-second network activity in a centralized, network metadata collector.

NetFlow/sFlow is automatically collected from Unified Enterprise Security (UES) sensors, as part of the Masergy Managed Detection and Response service. Additional NetFlow/sFlow data can be collected from firewalls, switches or any compatible device.

INTUITIVE GUI AND ENHANCED SORTING, RULE CREATION, AND ALERTING

Through a visually intuitive GUI, the security analyst can quickly isolate suspect activity by viewing and sorting network activity by:

- Dates/times
- Source/dest IP – Country
- Ports, protocols, applications
- Usernames
- BGP, DNS, syslog
- and by data transferred

The Network Visibility Policy Manager enables the security analyst to create alert-generating rules for focusing on critical risks or other security-specific use cases. The Network Visibility Tool highly augments the core UES detection and response mission: it delivers complete traffic history for further investigate of security alerts that are generated with the UES machine learning network analytics engine and the Endpoint Detection and Response tools.

FEATURES

Captures NetFlow and sFlow from integrated Unified Enterprise Security network sensors, or other third party network and security appliances, such as firewalls, routers and switches

Integrates with Active Directory for username resolution

Supports custom labelling of Groups, Sites and Subnets for easier management

Enables network alerting with rules configured by the Policy Manager

DEPLOYMENT

NVT DEPLOYS AS A MODULE ON UES CUSTOMER PREMISE EQUIPMENT

SUPPORTS

NETFLOW V5, 6 AND 10 (IPFIX), SFLOW, J-FLOW AND CISCO NSEL

REQUIRES

GOOGLE CHROME OR FIREFOX BROWSER (LATEST VERSION)