FLOWTRAQ

10 SECURITY REPORTS EVERY ENTERPRISE INFOSEC DIRECTOR SHOULD BE MONITORING

There's no shortage of data from the various network security solutions deployed at your organization. How do you wade through it all to find the valuable information that can actually help you keep your enterprise network secure — and alert you when there's a problem that you need to address? If you're responsible for the security of your organization's network and data, here are ten reports that you should be monitoring on a routine basis.

1. NEW SERVICES ON SENSITIVE HOSTS

You know which hosts in your organization are sensitive and require extra protection. And you have policies and procedures to ensure that only ports, protocols, and services with validated business needs are running on each system. But you should also proactively monitor the services on those hosts. When a new service starts up — for example, if a workstation starts acting as a file server — that's an indication that something unusual is going on and you need to know about it.

2. SUCCESSFUL SSH CONNECTIONS FROM OUTSIDE THE NETWORK

There's no doubt that SSH is a useful protocol. But it also comes with risks. In fact, according to a Ponemon Institute survey, three out of four enterprises are vulnerable to root-level attacks against their systems due to their failure to secure SSH keys. Organizations need a process to protect SSH keys and passwords from misuse, but because SSH keys can be used to gain access to enterprise systems while remaining hidden, you should also monitor successful SSH connections from outside the network on a regular basis to quickly identify and take action on rogue SSH connections.

3. OUTBOUND COMMUNICATION WITH BAD IPs

There are lots of known bad or suspicious IP addresses/spaces out there and you want to make sure that your network systems aren't communicating with them. Monitoring communications — especially outbound communications — with blacklisted systems, will help protect you from those known threats. Blacklists will often contain information about known botnet and malware distribution channels; communication with them is a certain red flag.

4. INTERNAL RECONNAISSANCE BEHAVIOR

Most organizations monitor lots of reports about their network borders, but there are many ways for an attacker to quickly and quietly become an insider. You should deploy telemetry and watch carefully what happens inside a network. Attackers will often scan for file shares or other local resources to make their way deeper into your organization.

5. TOP EXTERNAL CONNECTORS

Not all bad IPs are known. You want to be able to identify connections from bad sources even if they aren't currently on a blacklist. But at any given moment, there will be any number of connections made to an enterprise network, including from external sources. Looking at where there are a large number of external connection attempts — broken down by autonomous system and IP address — can help identify hacker attempts to access the network.

6. TOP EXTERNAL CONSUMERS OF DATA

You don't just want to focus on connections; you also want to look at who's consuming the data that is traversing the network. Monitoring top external consumers — broken down by country, autonomous system, and IP address — can help identify data exfiltration in process so that you can shut it down quickly, especially when you consider parts and pieces of your network individually, and focus on their external endpoints.

7. LARGE AND/OR LONG OUTBOUND FLOWS

Network flow traffic provides information about the behavior of applications and systems on the network. Looking at the size, duration, and behavior of outbound flows can also help you identify data exfiltration attempts. Examining the outbound flows by duration and flow size can help you identify any particularly large or long-lived individual flows that could be a sign of a data breach or hacker control channels.

8. TOTAL TRAFFIC AND CONNECTION VOLUMES ON PIPES

While you do want to monitor traffic and connections between sensitive systems and suspicious external parties, a well-orchestrated DDoS attack could fly under the radar of these views. You also need to monitor total traffic and connection volumes on the pipes that lead to your revenue-generating or other mission-critical assets, such as Web servers, content servers, etc. Visibility deeper into your own networks, as opposed to simply monitoring the border, can help you spot many forms of malicious activity, including lateral movement by hackers.

9. TOTAL TRAFFIC AND CONNECTION VOLUMES ON ASSETS

You should also monitor the traffic and connections on the network assets, such as file servers and databases themselves. Even though these assets are likely being managed by others in your organization, those connections could signal potential security issues that you need to be aware of. For instance, typical access to customer or medical records will be on the order of dozens to perhaps a hundred per day, per user. If there are unusual spikes to thousands or more, you may be dealing with a malicious data exfiltration attempt.

10. TOTAL TRAFFIC VOLUMES ON POTENTIAL ATTACK AMPLIFIERS

Some network assets — most notably DNS servers and NTP servers — can be "weaponized" by a third party and used as a DDoS reflection or amplification vector. You want to look at the total volume of traffic to and from these assets to identify unusual activity that could mean these servers are being used to aid hackers. After all, being a good Internet neighbor reduces the amount of attack noise on the Internet, making it harder for attackers to hide in the background.

GETTING THE RIGHT LEVEL OF VISIBILITY

Monitoring these reports on a regular basis — or, even better, being proactively alerted in real time when any of the abovementioned conditions are met — can help InfoSec directors stay vigilant and keep the network safe from intruders. To get this information without being inundated with inessential data, you need the right capabilities. These include:

- **Full-fidelity network flow analysis.** Network flow data — readily available from most routers and switches — provides detailed information about the traffic traversing the network, including source and destination ports, protocol, packets and bytes sent. While this data has long been used for network management, it also offers huge value for network security. You want to make sure that you are **working with un-sampled flow records** so that you have complete information, which is necessary if you need to further investigate a potential issue.
- **Network change detection.** A tool with a network fingerprint generation function watches for changes, such as a new host contacted or an ordinary partner contacted on a new port. The network fingerprinting process creates a statistical profile of individual IP connections in order to identify individual sessions as abnormal. The process is data- and time-intensive — and can be verbose — so it is often deployed with filters tuned to focus on the organization's most critical file servers, email servers, databases, etc.
- **Blacklist detection.** You want to be able to scan incoming network sessions individually and match them against a list of individual IP addresses and CIDR blocks. You should be able to configure a blacklist detector with the URL of a threat list from which it will update in specified intervals. Ideally, each connection to a blacklisted IP or CIDR block should proactively generate an alert.
- **Volume detection.** A volume detector is a powerful general statistical analysis tool that examines long-term traffic history to create baselines for specified network entities — which could be hosts, applications, autonomous systems, or even whole countries — in order to be able to quickly identify unusual volumes in terms of bytes, number of sessions, or unique counts.

ABOUT FLOWTRAQ

FlowTraq provides software and services for high-performance network monitoring, analytics, security and forensics to detect a range of network behaviors, including distributed denial of service (DDoS), brute force attacks, botnets, worms, network scans and other network traffic anomalies. To request a free trial of FlowTraq, visit **www.flowtraq.com/trial**.

FLOWTRAQ

16 Cavendish Court, Lebanon, New Hampshire 03766
Phone +1 (603) 727-4477 | Email info@flowtraq.com