Security Reports

Every InfoSec Professional Should Monitor

There is no shortage of data from the various security solutions deployed at your organization. How do you wade through it all to find the valuable information that can truly help you keep your enterprise secure and alert you when there is a problem you need to address? If you are responsible for cybersecurity, here are 10 reports you should be monitoring on a routine basis.

riverbed®

01: New Services on Sensitive Hosts

You know which hosts in your organization are sensitive and require extra protection. You developed policies and procedures to ensure that only ports, protocols, and services with validated business needs are running on each system. However, 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 is an indication that something unusual is occurring and you need to know about it.

02: Successful SSH Connections from Outside the Network

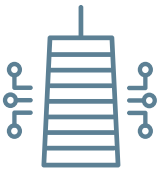
There is no doubt that SSH is a useful protocol. However, it also comes with risks. In fact, according to CSO, unmanaged, orphaned SSH keys remain a serious risk. Organizations need a process to protect SSH keys and passwords from misuse, but because SSH keys can be used to gain access to enterprise systems while remaining hidden, you should also monitor successful SSH connections from outside the network on a regular basis to quickly identify and act on rogue SSH connections. Worms often resort to random scanning to find other systems to penetrate.

03: Outbound Communication with Bad IPs

There are lots of known bad or suspicious IP addresses/spaces out there.
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.

04: 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.



05: Top External Connectors

Not all bad IPs are known. You want to be able to identify connections from certain sources even if they are not currently on a blacklist. At any given moment, there will be any number of connections made to your network from external sources. Monitoring where multiple external connection attempts are initiated — by country, by autonomous system, and IP address — can help identify hacker attempts to access the network.

Many organizations do business only in certain geographic areas. Identifying traffic coming from outside those regions is an effective way to detect threats. If a utility provider in the western United States experiences significant traffic from Eastern Europe or Asia, it could be a sign of threat activity.

06: Top External Consumers of Data

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

07: Large and/or Long Outbound Flows

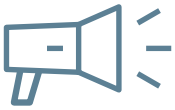
Network flow traffic provides information about the behavior of applications and systems on the network. Looking at the size, duration, and behavior of outbound flows can also help you identify data exfiltration attempts. Examining the outbound flows by duration and flow size can help you identify any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

08: Total Traffic and Connection Volume on Network Segments

While you want to monitor traffic and connections between sensitive systems and suspicious external parties, a well-orchestrated DDoS attack could fly under the radar. You also need to monitor total traffic and connection volumes on the network segments that lead to your revenue-generating or other mission-critical assets, such as Web servers, content servers, etc. Visibility deep 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.

09: 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 others are probably managing these assets in your organization, those connections could signal potential security issues. For instance, typical access to customer or medical records will be a few dozens to perhaps a hundred per day, per user. If there are unusual spikes of 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 hackers have hijacked these servers. 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 above-mentioned conditions are met—can help InfoSec directors stay vigilant and keep the network safe. To get this information without being inundated with nonessential 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 and stores it for forensic analysis. While network managers have long used this data for network management, it also offers huge value for cyber security. You want to make sure that you are working with un-sampled flow records so that you have complete information to investigate fully any potential issue.

- **Network security analytics.** A tool with machine learning or anomaly detection that watches for abnormal changes in behavior that could indicate a security breach. An example is a new host contacted or an ordinary partner contacted on a new port. The anomaly detection process creates a statistical profile of individual IP connections to identify individual sessions as abnormal.

- **Blacklist detection.** You want to be able to scan incoming network sessions individually and match them against a list of known bad 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 at specified intervals. Ideally, each connection to a blacklisted IP or CIDR block should proactively generate an alert.

Click below for more information on how you can better secure your organization using Riverbed SteelCentral network security analytics.

LEARN MORE

riverbed®