Maintain awareness with network monitoring

Network communication can be noisy! Events like sending an email, streaming a video, or visiting a website all produce network communications in the form of network traffic and network data. As a reminder, **network traffic** is the amount of data that moves across a network. It can also include the type of data that is transferred, such as HTTP. **Network data** is the data that's transmitted between devices on a network.

Network monitoring is essential in maintaining situational awareness of any activity on a network. By collecting and analyzing network traffic, organizations can detect suspicious network activity. But before networks can be monitored, you must know exactly what to monitor. In this reading, you'll learn more about the importance of network monitoring, ways to monitor your network, and network monitoring tools.

Know your network

As you've learned, networks connect devices, and devices then communicate and exchange data using network protocols. Network communications provide information about connections such as source and destination IP addresses, amount of data transferred, date and time, and more. This information can be valuable for security professionals when developing a **baseline** of normal or expected behavior.

A baseline is a reference point that's used for comparison. You've probably encountered or used baselines at some point. For example, a grocery amount for a personal budget is an example of a baseline that can be used to help identify any patterns or changes in spending habits. In security, baselines help establish a standard of expected or normal behavior for systems, devices, and networks. Essentially, by knowing the baseline of *normal* network behavior, you'll be better able to identify *abnormal* network behavior.

Monitor your network

Once you've determined a baseline, you can monitor a network to identify any deviations from that baseline. Monitoring involves examining network components to detect unusual activities, such as large and unusual data transfers. Here are examples of network components that can be monitored to detect malicious activity:

Flow analysis

Flow refers to the movement of network communications and includes information related to packets, protocols, and ports. Packets can travel to ports, which receive and transmit communications. Ports are often, but not always, associated with network protocols. For

example, port 443 is commonly used by HTTPS which is a protocol that provides website traffic encryption.

However, malicious actors can use protocols and ports that are not commonly associated to maintain communications between the compromised system and their own machine. These communications are what's known as **command and control (C2)**, which are the techniques used by malicious actors to maintain communications with compromised systems.

For example, malicious actors can use HTTPS protocol over port 8088 as opposed to its commonly associated port 443 to communicate with compromised systems. Organizations must know which ports should be open and approved for connections, and watch out for any mismatches between ports and their associated protocols.

Packet payload information

Network packets contain components related to the transmission of the packet. This includes details like source and destination IP address, and the packet payload information, which is the actual data that's transmitted. Often, this data is encrypted and requires decryption for it to be readable. Organizations can monitor the payload information of packets to uncover unusual activity, such as sensitive data transmitting outside of the network, which could indicate a possible data exfiltration attack.

Temporal patterns

Network packets contain information relating to time. This information is useful in understanding time patterns. For example, a company operating in North America experiences bulk traffic flows between 9 a.m. to 5 p.m., which is the baseline of normal network activity. If large volumes of traffic are suddenly outside of the normal hours of network activity, then this is considered *off baseline* and should be investigated.

Through network monitoring, organizations can promptly detect network intrusions and work to prevent them from happening by securing network components.

Protect your network

In this program, you've learned about **security operations centers** (**SOC**) and their role in monitoring systems against security threats and attacks. Organizations may deploy a **network operations center** (**NOC**), which is an organizational unit that monitors the performance of a network and responds to any network disruption, such as a network outage. While a SOC is focused on maintaining the security of an organization through detection and response, a NOC is responsible for maintaining network performance, availability, and uptime.

Security analysts monitor networks to identify any signs of potential security incidents known as **indicators of compromise** (**IoC**) and protect networks from threats or attacks. To do this,

they must understand the environment that network communications travel through so that they can identify deviations in network traffic.

Network monitoring tools

Network monitoring can be automated or performed manually. Some common network monitoring tools can include:

- **Intrusion detection systems** (**IDS**) monitor system activity and alert on possible intrusions. An IDS will detect and alert on the deviations you've configured it to detect. Most commonly, IDS tools will monitor the content of packet payload to detect patterns associated with threats such as malware or phishing attempts.
- **Network protocol analyzers**, also known as packet sniffers, are tools designed to capture and analyze data traffic within a network. They can be used to analyze network communications manually in detail. Examples include tools such as tcpdump and Wireshark, which can be used by security professionals to record network communications through packet captures. Packet captures can then be investigated to identify potentially malicious activity.

Key takeaways

Monitoring and protecting networks from intrusions and attacks are key responsibilities of security professionals. You can't protect what you don't know. As a security analyst, you'll need to know the components of a network and the communications that happen on it, so you can better protect it. Baselines provide a way to understand network traffic by uncovering common patterns which help in identifying any deviations from the expected traffic patterns. Tools like intrusion detection systems and network protocol analyzers support efforts in monitoring network activities.

Resources

- If you would like to learn more about network components organizations can monitor, check out network traffic - MITRE ATT&CK®
- Attackers can leverage different techniques to exfiltrate data, should you like to learn more, check out data exfiltration techniques - MITRE ATT&CK®