Overview of detection tools

Previously, you explored **intrusion detection system** (**IDS**) and **intrusion prevention system** (**IPS**) technologies. In this reading, you'll compare and contrast these tools and learn about **endpoint detection and response** (**EDR**). As a security analyst, you'll likely work with these different tools, so it's important to understand their functions.

Why you need detection tools

Detection tools work similarly to home security systems. Whereas home security systems monitor and protect homes against intrusion, cybersecurity detection tools help organizations protect their networks and systems against unwanted and unauthorized access. For organizations to protect their systems from security threats or attacks, they must be made aware when there is any indication of an intrusion. Detection tools make security professionals aware of the activity happening on a network or a system. The tools do this by continuously monitoring networks and systems for any suspicious activity. Once something unusual or suspicious is detected, the tool triggers an alert that notifies the security professional to investigate and stop the possible intrusion.

Detection tools

As a security analyst, you'll likely encounter **IDS**, **IPS**, and **EDR** detection tools at some point, but it's important to understand the differences between them. Here is a comparison chart for quick reference:

Capability	IDS	IPS	EDR
Detects malicious activity	✓	✓	✓
Prevents intrusions	N/A	✓	✓
Logs activity	✓	✓	✓
Generates alerts	✓	✓	✓
Performs behavioral analysis	N/A	N/A	✓

Overview of IDS tools

An **intrusion detection system** (**IDS**) is an application that monitors system activity and alerts on possible intrusions. An IDS provides continuous monitoring of network events to help protect against security threats or attacks. The goal of an IDS is to detect potential malicious activity and generate an alert once such activity is detected. An IDS does *not* stop or prevent the activity. Instead, security professionals will investigate the alert and act to stop it, if necessary.

For example, an IDS can send out an alert when it identifies a suspicious user login, such as an unknown IP address logging into an application or a device at an unusual time. But, an IDS will not stop or prevent any further actions, like blocking the suspicious user login.

Examples of IDS tools include Zeek, Suricata, Snort®, and Sagan.

Detection categories

As a security analyst, you will investigate alerts that an IDS generates. There are four types of detection categories you should be familiar with:

1. **A true positive** is an alert that correctly detects the presence of an attack.
2. **A true negative** is a state where there is no detection of malicious activity. This is when no malicious activity exists and no alert is triggered.
3. **A false positive** is an alert that incorrectly detects the presence of a threat. This is when an IDS identifies an activity as malicious, but it isn't. False positives are an inconvenience for security teams because they spend time and resources investigating an illegitimate alert.
4. **A false negative** is a state where the presence of a threat is not detected. This is when malicious activity happens but an IDS fails to detect it. False negatives are dangerous because security teams are left unaware of legitimate attacks that they can be vulnerable to.

Overview of IPS tools

An **intrusion prevention system** (**IPS**) is an application that monitors system activity for intrusive activity and takes action to stop the activity. An IPS works similarly to an IDS. But, IPS monitors system activity to detect and alert on intrusions, *and* it also takes action to *prevent* the activity and minimize its effects. For example, an IPS can send an alert and modify an access control list on a router to block specific traffic on a server.

Note: Many IDS tools can also operate as an IPS. Tools like Suricata, Snort, and Sagan have both IDS and IPS capabilities.

Overview of EDR tools

Endpoint detection and response (**EDR**) is an application that monitors an endpoint for malicious activity. EDR tools are installed on endpoints. Remember that an **endpoint** is any device connected on a network. Examples include end-user devices, like computers, phones, tablets, and more.

EDR tools monitor, record, and analyze endpoint system activity to identify, alert, and respond to suspicious activity. Unlike IDS or IPS tools, EDRs collect endpoint activity data and perform *behavioral analysis* to identify threat patterns happening on an endpoint. Behavioral analysis uses the power of machine learning and artificial intelligence to analyze system behavior to identify malicious or unusual activity. EDR tools also use *automation* to stop attacks without the manual intervention of security professionals. For example, if an EDR detects an unusual process starting up on a user’s workstation that normally is not used, it can automatically block the process from running.

Tools like Open EDR®, Bitdefender™ Endpoint Detection and Response, and FortiEDR™ are examples of EDR tools.

Note: Security information and event management (SIEM) tools also have detection capabilities, which you'll explore later.

Key takeaways

Organizations deploy detection tools to gain awareness into the activity happening in their environments. IDS, IPS, and EDR are different types of detection tools. The value of detection tools is in their ability to detect, log, alert, and stop potential malicious activity.

Revision #1
Created 6 September 2023 11:06:54 by naruzkurai
Updated 1 November 2023 01:10:46 by naruzkurai