Glossary.

SOC (Security Operations Centre)

A SOC (Security Operations Centre) monitors computer and network activities in an organisation. Log information from applications and devices in the corporate network is collected and examined for abnormalities. The log information can come from servers, firewalls, web applications, antivirus software and even industrial control systems. It is therefore relevant information about the security of all systems and devices. All information leads to an understanding of how secure the network, systems and hardware and software are functioning in the organisation.

HIDS (Host-based Intrusion Detection System)

HIDS (Host-based Intrusion Detection System) identifies possible threats based on the log files of servers. These are analysed against so-called use case definitions, where a positive match leads to an alert to be investigated.

NIDS (Network-based Intrusion Detection System)

NIDS (Network-based Intrusion Detection System) provides for the detection of suspicious network traffic. This option can only be deployed on local (on-premise) networks. NIDS can analyse the behaviour of hackers so that you can take measures before the hacker succeeds.

EDR (Endpoint Detection & Response)

EDR (Endpoint Detection & Response) takes care of the analysis of suspicious changes on files, executables (.exe) or registries. EDR can be installed on all kinds of endpoints, such as servers, laptops or PCs. An endpoint can have two meanings (see also this list).

NGAV (Next Generation Anti-Virus)

NGAV (Next Generation Anti-Virus) is anti-malware software that can be installed on most endpoints. NGAV analyses the content of files and mail for suspicious links or code. The main difference with traditional anti-malware is that NGAV also analyses unknown threats, which makes it possible to take measures before the malware becomes active.

Appliance

An appliance is a ready-to-use device with an operating system and the necessary software installed, so that it can be connected to a network without further instructions. The device is thus immediately ready for use.

NUC, Next Unit Computing

An NUC stands for Next Unit Computing and is a full-fledged desktop computer developed by Intel. A NUC is small, quiet and very stable and can directly monitor the servers and possibly the network (see NIDS) with the pre-installed Local Data Collector from OpenSIEM.

Use case

A use case is a description of the behaviour of a system. A use case responds to a certain request or action. In the case of OpenSIEM, the defined use cases react to certain log rules. This is how we recognise a DDOS attack, an SQL injection or an attempted break-in.

Endpoint

An endpoint can have two meanings:

An endpoint can be a device connected to the company network (i.e. internal) that accepts network traffic. This can be a switch or a modem, but of course also a laptop, PC or server. A printer or a VOIP telephone also belong to endpoints, because they also accept network traffic.

The second meaning refers only to all devices that can make contact with the company network "from outside" (i.e. from outside to inside). This is a more limited group of devices, i.e. only laptops, mobile phones or tablets that are allowed to connect to the company network.

Honeypot

A honeypot is a computer system that is installed with the purpose of attracting hackers to study their activities. It sounds scary, but a honeypot is completely isolated from the "real" network. Hackers are therefore unable to penetrate beyond the honeypot itself.

Files

Files is the English name for a file. An executable is a start-up file, typically with the extension .exe. For example, there is a file called word.exe. It is used to start the Microsoft Word application. A registry file is a file that holds all the specific settings and options of the systems that run on the computer or server. Registry files are typically linked to Microsoft applications.