NETWORK SECURITY MONITOR

blësk network monitoring

OBJECTIVE: Constantly monitor for intrusion attempts and suspicious behavior.

A virus or Trojan has managed to bypass the firewall or network of your company. Your IT team is not aware of this intrusion because no alert has been sent. How can your IT team act quickly before expensive damage occurs?

BLËSK Network Security Monitor (NSM) aims to act as a security camera and motion detector on the network by continuously monitoring intrusion attempts and suspicious behavior.

NSM makes use of Open Source tools such as Sguil, Snort, Barnyard2 and OpenVas.

BENEFITS

- Performs real-time traffic analysis and logging of packets over the IP network.
- Protocol analysis.
- Content search.
- Detects probes or attacks.
- Collects, analyzes and escalates indications and warnings to detect and respond to intrusions.
- Analysis and management of vulnerabilities.

BLËSK CAN HELP YOU:

A virus or Trojan will leave a trace on the network. BLËSK detects this and triggers an alert in the NSM dashboard. Increased visibility helps reduce malware damage to the internal environment.

In addition, NSM can scan network devices and perform vulnerability tests. Installed software may have a flaw that is exploitable by a virus. NSM provides a detailed report that will allow you to identify equipment and applications at risk. Recommendations are then formulated to overcome flaws, such as updates to install on these elements. These are key elements of security because they contain fixes that eliminate known vulnerabilities. That's why organizations that have very high security standards, such as financial organizations, use this kind of tool.