Detect Hidden Threats Before the Damage Is Done

Despite new technologies and new policies, cyber criminals continue to find ways to infiltrate government networks. All they need is one vulnerability, and off they go. That's why you can't just focus on prevention — because malicious actors could already be in your environment, hidden by the overwhelming volume of cyber data. **Here's how you can crack the case.**

MALICIOUS ACTORS GO ON CYBER SPREE

Recent studies show that the current surge in cyber threats is not abating. The evidence includes:

56% increase in the volume of malware attacks between 2021 and 2022

21% increase in vulnerabilities found between 2021 and 2022

61% increase in phishing attacks between 2021 and 2022

65% increase in cyberattacks after the Russian invasion of Ukraine

And cyber criminals are getting smarter, thanks to recent advances in the sophistication and accessibility of artificial intelligence (AI), such as the ChatGPT chatbot.

75% of cybersecurity specialists say that AI use in cyberattacks is on the rise

135% is the increase in 'novel social engineering' attacks in 2023 amidst the widespread availability of ChatGPT

The key number to remember:

277

In 2022 it took an average of **207 days** to identify a breach ("dwell time") and another **70 days** to contain the breach.

HOW TO SUSS OUT CYBER THREATS

You need to take active measures to detect those threats as quickly as possible. The solution? Leverage the one advantage you have: You should know your network better than the bad guys. You know...

- Which internal parts of your network often/never communicate with each other
- What normally happens before/after business hours on your network
- Who outside your network you normally communicate with
- What normally happens on weekends

The key is data. Nearly every device on your network creates logs of its activity, providing a wealth of data that could provide clues to nefarious activity — but most of it is never analyzed.

Here's how the AlphaSix Security Analytics Framework helps you put that data to work.

FW Logs
IDS Logs
OS Logs
App Logs
Network Logs
File Hashes

Query | Processing

HPE Ezmeral Data Fabric Software

Hewlett Packard Enterprise

- Visualization Tools
- Customized Visualization
- Search
- Deep Analytics/ML/ Anomaly Detection

DATA SOURCES

Gather log data from all network devices, such as firewalls, intrusion detection systems and routers, as well as applications.

DATA LAKE

Store that data in a data lake. Given the long dwell time of many threats, you need to store not just 30, 60 or 90 days of logs, but years' worth.

ANALYTIC OPTIONS

Provide your experts with tools for searching, analyzing and visualizing that data, including an anomaly detection engine.

This framework supports both short- and long-term analysis:

SHORT-TERM

- A security dashboard highlights possible security events.
- An analyst drills down to get data from system that reports events.
- The data pinpoints traffic that bypassed an official internal DNS server.
- The analyst investigates further to see if the problem is a misconfigured server — or malicious activity.

LONG-TERM

- The anomaly detection engine finds a suspected malicious actor probing your network.
- Further analysis shows that probe happens on multiple ports on-and-off for several days at a time.
- An investigation finds the probing has been going on for more than a year.
- This activity should be treated with suspicion and examined further.

HOW ALPHASIX HELPS

AlphaSix Qato uses machine learning to detect and visualize anomalies in massive data sets, allowing you to sift through data collected over long periods of time. Because Qato is based on an open, scalable architecture, its data is accessible to multiple analytic tools.

Learn more: www.alphasixcorp.com/qato

govloop | AlphaSix | Hewlett Packard Enterprise