Five Steps to Satisfy OMB Memorandum M-21-31 and Improve Security Logging

Capturing security events and processing that information in a timely manner is one of the most important security activities that you can conduct. This activity is fundamental to larger government programs and policies including: CDM, TIC 3.0, NIST 800-53, and the Zero Trust strategy. You need good information, and you need it fast.

This is where a simple five step process can help in setting up a proper security logging architecture as well as achieve compliance with the OMB M-21-31 memorandum of 2021. This memorandum was in response to the Executive Order 14028, “Improving the Nation’s Cybersecurity”, from May 2021.

1

Create a logging and network visibility strategy – your EL0 process

Before you blindly dive in and enable logging on every asset, you should start by verifying your existing assets and determine what your security posture should look like. For many agencies, log data is just the beginning because it’s low-hanging fruit in terms of implementation difficulty, limited disruption, and budget friendly. However, you will be well-served by taking the time to look beyond logging towards a long-term visibility strategy that can reduce risk by removing blind spots in your network.

2

Capture the right packet data to start the EL1 process

Better logging practices start with capturing good data. The first thing to do is to deploy lots of taps across your network. This gives you access to the critical monitoring data that you need and creates visibility into the network. Taps are passive network elements that are quick and easy to deploy. There are versions for your physical on-premises environment as well as cloud-based taps to capture your virtual data. Keysight has the largest range of taps on the market.

3 Decrypt relevant data as part of EL2 compliance

More than 70% of malware may now hide in encrypted packet data. Passive and active TLS decryption allows you to look into those packets and see what's hidden. After that, you can monitor and flag potentially malicious communication. This functionality helps with compliance to the EL2 stage that expressly calls for decryption capability.

4 Process network metadata to enhance EL2 compliance

Network metadata provides another source of crucial information at a fraction of the space of full packet and log data. Metadata (NetFlow, J-Flow, IPFIX, IxFlow, JSON) generated from collected packets creates better network efficiency and is easier for security managers, like SIEMs, to process. This metadata can provide actionable insights.

5 Aggregate, filter, and transmit relevant data to security tools

The last component is to use a packet broker to collect and access the relevant data your security analysis tools need. A purpose-built packet broker uses advanced filtering, deduplication, and packet trimming features to enhance the efficiency of log collector and analysis tools. The data can then be forwarded to your storage solutions. In addition, these data brokers can collect traffic from any segment of the network and perform header stripping so that the data can be tunneled (i.e. GRE) back to a central datacenter. Keysight offers on-premises, virtual (hypervisor and public or private cloud solutions), or a hybrid mixture of both solutions that delivers lossless data capture, aggregation, and filtration of data packets. Keysight also offers a time sync reliability solution, since data logs are useless if the network isn't properly synchronized.

Enhanced logging is a necessary component for any government agency. Whether you are looking to achieve M-21-31 compliance or to enhance your Zero Trust solution, Keysight is here to help: Reach out to us and we will show you how to optimize your logging and security solutions.

Learn more at: www.keysight.com/us/en/industries/government

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at:

www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES