AES

CLEVER® Solutions Empowering Global Enterprises

Ransomware has been in the news quite a bit lately, especially after the recent attacks by REvil. While mainframes are generally known for their reliability and security, they are still subject to frequent hacks and malicious attacks. Intruders can strike through unpatched servers or security misconfigurations, but the most common vulnerability is human error, often exploited through the use of social engineering attacks to steal system programmer's credentials and gain access to sensitive data.

AES provides intelligent solutions that will make your mainframe network more secure. In order to detect unusual network activities that could indicate data exfiltration traffic, you must first establish a comprehensive baseline to understand what the normal activity looks like. ***CleverView® for TCP/IP*** keeps track of detailed network activities on the application level, network protocol level, and network interface level, which all can be used to determine the baseline network traffic. Its *Session Log* feature provides an audit trail of all transactions, and will make it easy to pinpoint unusual inbound/outbound network traffic that could be a sign of malicious activities. With visibility into this traffic, you can respond quickly before data is lost or major damage is done.

Unauthorized access to the mainframe has been made possible by the availability of FTP, TN3270 and ssh, as well as the fact that the firewalls protecting the mainframe have been too liberally configured. ***CLEVERDetect for IDS*** complements the z/OS Intrusion Detection Services (IDS) capabilities. It serves as a repository of all IDS, SAF (System Authorization Facility) and subsystems security violation messages. Its *FTP Server Logon Failure* analysis will identify potential attacks to the FTP server. A compromised FTP server not only could be used to exfiltrate stolen data, but also could be used for "blind drop" that allows unauthorized anonymous uploads.

When you need to further diagnose an attack, ***CleverView for cTrace Analysis*** provides the unique capability to correlate an attack or an intrusion with the actual data packets, allowing you to study the flow of the malware and its payload data.

Disaster recovery is the last line of defense against ransomware, but monitoring your networks and systems proactively will help keep it from happening.

Learn More About AES CLEVER Family of Products

Free Trial **Webinar** **Website** **Email**

Applied Expert Systems LLC | PO BOX 50927, Palo Alto, CA 94303