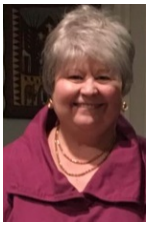
AES aesclever.com

CLEVER® Solutions
Empowering Global Enterprise

Automated mainframe Security Defense - IDS

Greetings!



Laura's Corner

With breaches increasing in frequency, scope and severity, the CISO (Chief Information Security Officer) has one of the most stressful jobs around. So what is on the CISO wish list:

- An end to security silos
- Confidence in the completeness of the overall security strategy
- Movement from a reactive to a predictive security posture Informative, correlated, and complete metrics on security
- Total buy-in by the end user community of their role in securing the business

For most enterprises we are still in a react mode when it comes to identifying a security breach. We still have many breaches that are not discovered until months after the hack begins, and often the enterprise finds out about a breach because of an outside source.

To be successful the following elements need to be defined, implemented, and audited frequently:

- a strategy needs to be defined for the business and all its components,
- implementation coordination needs to occur across all lines of business,
- constant surveillance is required at all levels,
- real-time alerting and alarming is required to central SIEM centers and individual owners, historical reporting needs to be accessible to both owners and global SIEM centers

Server centric intrusion detection is critical and augments network intrusion detection systems. In Laura's Corner we answer questions being posed by clients in these areas.

Impact of End-End Encryption on Network Based Intrusion Detection Systems (IDS)

Question: "Our business is using more and more end-end encryption. How do we need to adjust our mainframe security to avoid any security problems?"

Issue: The rapid increase of end-to-end encryption in network traffic has decreased the effectiveness of using network-based IDS. Network devices don't typically have access to the clear data and can't detect an intrusion based on the data content.

Solution: z/OS IDS is built into the Communication Servers TCP-IP stack, allowing evaluation of the traffic as it first enters the z/OS system and after it has been decrypted. IDS can detect network attacks directed at the z/OS system by evaluating data in context at predetermined points, called attack probes. The traffic content is analyzed against policies defined in z/OS IDS.

Adding a mainframe level of IDS can help you address two trends in network traffic that are putting pressure on network IDS solutions. These trends are the increase in encryption over the network and the increased pace of attacks.

CLEVERDetect® for IDS is a z/OS Intrusion Detection solution providing an effective way to view IDS messages, route these messages to SNMP or SIEM managers, view FTP server logon failures, and issue commands from either a browser or mobile interface. The ability to provide enterprise wide z/OS intrusion details and FTP Logon failures in a crisp, clear, and concise environment allows trend, pattern and anomaly identification. The resulting details provide for more effective decision-making to meet today's dynamic anywhere anytime security environment. IT staff need access to intrusion details from not only their browser desktops, but also their cell phones. With the CLEVER Mobile® for IDS app they have access anytime, anywhere!

Keeping up with Critical Alerts

Question: "I am the lead for our infrastructure trouble shooting team. I need to keep up with critical alerts, but I am in so many meetings now, it is all but impossible. Are there any solutions out there to help me out?

Solution: **CLEVER Mobile® for IDS** empowers IT staff members to provide exceptional service to the business with their mobile devices. The added access capability ensures real-time notification of intrusions leading to increased visibility into potential security breaches. The resulting details provide for more effective decision-making to meet today's dynamic anywhere anytime security environment.

Through their mobile devices IT staff members have access to the monitored information collected by the server solution CLEVERDetect for IDS. With CLEVER Mobile for IDS option implemented, mobile access to monitored metrics provided by IDS Status, IDS Messages, FTP Server Logon Failures, and Commands is essential to understanding the z/OS Intrusion Detection Services health. The real power lies in the ability of CLEVER Mobile for IDS to allow z/OS system-wide system message monitoring, alert notification, z/OS® and TSO command submission, and CLIST and REXX script execution from the mobile device. The powerful alert and command capability with classification is standard on all products in the CLEVER Mobile Advantage family.

We would love to hear from you with your mainframe IDS requirements or other mainframe problem determination questions! Click the box below to send those questions to us in an email.

Learn More about CLEVERDetect for IDS | **Learn More about CLEVER Mobile for IDS** | **Send us your Feedback**

Product Spotlight

AES is pleased to announce:

CLEVERDetect® for IDS v1.2 is a z/OS Intrusion Detection solution providing an effective way to analyze IDS logs and messages, route z/OS messages to SNMP and SIEM managers, track FTP server logon failures, and issue system commands from either a browser or mobile interface. New functions in v1.2 include Dashboard, IDS Analyzer, IDS Policy Explorer, IDS Status and Logview.

CleverView® for cTrace Analysis v8.2 uniquely provides users the ability to generate and analyze IP packet traces across multiple systems concurrently. The expert functions enhance diagnostic efforts accelerating virtualization, cloud, application, security, and IPv6 deployments. **Check out the existing z/OS DATA trace and OSAENTA trace and the support for z/OS IDS trace analysis.**

CleverView®for TCP/IP on Linux v2.9 now offers a new Dashbaord and navigation functions along with our BlockChainView and DockerView support expanding support for microservices and DevOps. With support for connectivity and process monitoring functions unique to a LinuxONE and z

System platform, AES CleverView for TCP/IP on Linux offers extensive Linux monitoring environment without limits.

Want to see these products in action? Request an evaluation copy!

Request an Evaluation Copy

STAY CONNECTED:

Website

1-650-617-2400