Sandsiger Security Assessment v3

To optimize the integration of your network logs into a machine learning program for risk prediction, we would like to gather information on key aspects of your network infrastructure.

—------------------------------------------------------------------------------------------------------------------

Please provide details on the following:

**1. Network Logs:**

What types of network logs are available for analysis in our machine learning program?

Are logs generated for authentication, network traffic, firewall events, application activities, endpoints, and user activities?

**2. Privileged Data:**

Identify the privileged data within your network.

Where is this privileged data stored, and what is the pathing of this data within the network?

**3. Firewall Configurations:**

Reviewing from the firewall perspective, does the firewall have configurations for rules other than "deny all"?

Can you provide insights into specific firewall rules and configurations in place?

**4. Packet Sniffing:**

Are packet sniffing activities monitored and logged within the network?

What measures are in place to detect and respond to unauthorized packet sniffing?

**5. Deviation from Baseline:**

How is the baseline for normal network behavior established?

What mechanisms are in place to identify and respond to deviations from this baseline?

**6. Data Protection:**

What measures are in place to protect sensitive data?

How is data encryption implemented for data in transit and at rest?

Is there a process for secure data disposal when no longer needed?

**7. Security Awareness Training:**

Is there a mandatory security awareness training program for employees?

How often is security training provided, and what topics are covered?

Are phishing simulations conducted to assess employee awareness?

**8. Physical Security:**

What physical security measures are in place to protect server rooms and data centers?

Is there a system for monitoring and controlling physical access to critical infrastructure?

**9. Compliance:**

How does the company ensure compliance with relevant industry regulations and standards?

Is there a process for auditing and validating compliance on a regular basis?The information gathered will help us define the scope and understand the general log data available within your network.

—------------------------------------------------------------------------------------------------------------------

This will enable us to tailor the machine learning program to predict risks based on these logs.

If you have additional information or specific concerns, please feel free to share. We appreciate your cooperation in enhancing the security of your network infrastructure.

* The Sandsiger Team