Synoligo BIOTECHNOLOGIES
101 Southcenter Court, Suite 800, Morrisville, NC 27560 USA
Phone +1 (919)-650-1014
www.synoligo.com | info@synoligo.com

Synoligo Security Event logging and monitoring

1. Identify the assets to be monitored.

This includes all devices, systems, and applications that contain sensitive data or are critical to the organization's operations. For example, this could include servers, workstations, laptops, mobile devices, firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus software, and web applications.

2. Determine the types of events to be logged.

This includes both security-related events (such as failed login attempts) and operational events (such as system outages). For example, security-related events could include failed login attempts, unauthorized access to files or systems, and suspicious network activity. Operational events could include system outages, application crashes, and database errors.

3. Select a logging and monitoring solution.

There are a variety of commercial and open source solutions available. The solution should be able to collect logs from all of the organization's assets, filter and analyze the logs for suspicious activity, and generate alerts when suspicious activity is detected. Some popular logging and monitoring solutions include: Splunk, LogRhythm, ArcSight, QRadar, IBM Security Event Management.

4. Configure the logging and monitoring solution.

This includes setting up the collection of logs from all of the organization's assets, configuring the filters and alerts, and testing the solution to ensure that it is working properly. Some important configuration settings include:

- The types of events to be logged
- The sources of logs to be collected
- The format of the logs
- The retention period for the logs
- The filters to be used to identify suspicious activity
- The alerts to be generated

5. Monitor the logs for suspicious activity.

This includes reviewing the logs on a regular basis for signs of suspicious activity, investigating any suspicious activity that is detected, and taking steps to remediate any security vulnerabilities that are discovered. Some common methods for monitoring logs include:

- Reviewing the logs manually.

  This involves manually reviewing the logs for signs of suspicious activity. This can be a time-consuming process, but it is a good way to identify unusual patterns or trends that may indicate a security threat.

- Using a SIEM solution.

  A SIEM solution can collect logs from multiple sources, filter and analyze the logs for suspicious activity, and generate alerts when suspicious activity is detected. This can help organizations to identify and respond to security threats more quickly and effectively.

6. Respond to suspicious activity.

When suspicious activity is detected, it is important to take steps to respond to the activity in a timely manner. This may involve:

- Investigating the activity.

  This involves gathering more information about the activity to determine if it is malicious or not. This may involve looking at the logs, talking to users, and running security scans.

- Remediating any security vulnerabilities.

  If the activity is malicious, it is important to take steps to remediate any security vulnerabilities that may have been exploited. This may involve patching vulnerabilities, updating software, and changing passwords.

- Reporting the activity to the appropriate authorities.

  In some cases, it may be necessary to report the activity to the appropriate authorities. This may involve reporting the activity to the local law enforcement agency or to a government agency such as the Cybersecurity and Infrastructure Security Agency (CISA).

7. Document the process.

It is important to document the process for security event logging and monitoring. This documentation should include the following information:

- The assets to be monitored
- The types of events to be logged
- The logging and monitoring solution
- The configuration settings
- The process for monitoring the logs
- The process for responding to suspicious activity

By documenting the process, organizations can ensure that it is followed consistently and that it is effective in protecting the organization's information assets.