Continuous Monitoring Of Information Security

> Automated measurement, reporting and alerting can improve the effectiveness of security risk management programs.

Continuous Monitoring Components

- *Automated Measurement:* of the effectiveness of security controls and systems on a continuous basis
- *Reporting tools and dashboards:* Provide instantaneous and trending information on security status
- *Alerting and tracking tools:* that indicate when security controls aren't effective

Active vs Passive scanning

Active scanning can catch only so much because they have been told to look for something in particular, whereas Passive scanning look for a deviation on the norm. They can successfully identify unauthorized activity or obfuscated traffic.

The value of Continuous Monitoring

It sharpens the focus of what is important. The theory of information. If you get a monthly report of the same information, you quickly grow accustomed to it, and disregard it, but if, in the other hand, the monitoring system brings the important information to the top of the list.

This program brings two benefits over standard point-in-time security assessments:

Increased Visibility

- Enables staff to see what is happening as it is happening.
- Enables management to understand a problem at a glance.
- Enables technical team to more efficiently debug a issue or security breach.

Increased Control

- Allow for proactive response to identified threats

Implementing continuous monitoring

The implementation ease will depend on the previous security monitoring technique. If there was already one in place, then, it is only a refinement, but if there is no monitoring in place, the implementation will be much more complicated.

Depending on the previous workflow, the information needed to implement a continuous monitoring system will be duplicated or not.

If a team previously handled one type of alerts but now, this is going to be transfered to the CMS, data will be duplicated.

What to monitor

Do not follow security control guidelines, as that security will be measured by point-in-time audits. This will increase the likelihood of you passing the audits, but it won't improve your overall security at all.

Instead, think in terms of "What can be measured". This will monitor weak points provided by the application/system developers.

Automated Measurement

If continuous monitoring is to be effective, It must be automated.

Staff should be alerted when anything important requires investigation, not required to check for anything important to be investigated.

A good place to start with Automated Monitoring is in **log measurement**. Logs will form a large part of the system, and knowing how to handle them is critical.

Source of Logging Information	Types of Logging Data and Statistics to be controlled
Firewall traffic logs	Allowed network traffic; blocked attempts
Mail security gateway	Level of mail traffic; counts of malware and spam blocked, as well as unscannable traffic
Intrusion prevention/detection systems	Medium and high priority alerts on suspicious and blocked traffic
Network device logs	Switches, load balancers and other devices with SYSLOG capabilities
Server logs	Windows event log or SYSLOG
Trouble Ticket System	Tickets opened, closed and why

Vulnerability analyzers and System integrity checkers are also important parts of a security compliance program. Data may be needed to be parsed out, due to the complexity of the generated report.

Reachability and capacity measurement systems should also be monitored as they form a integral part of the overall system availability.

Source of data	Types of security metric to be generated
Reachability monitors	System availability data; network latency data

Source of data	Types of security metric to be generated
Capacity monitors	Utilization of SANs and disk subsystems; memory of critical systems and devices
Bandwidth monitors	Utilization of critical network LAN and WAN links
Vulnerability analyzer	System vulnerability detection; changes in vulnerabilities detected; changes in open ports and systems; time between detection and mitigation
Integrity checkers	Changes in system security and settings or registry values; changes in sensitive files or directories