Salisbury University

Continuous Monitoring Policy

1. PURPOSE

The Salisbury University Information Technology (SUIT) department is committed to managing the confidentiality, integrity, and availability of information technology assets and information. To provide this level of security within the SUIT Cybersecurity Program, a key component protecting systems and data is the implementation of a continuous monitoring capability.

SUIT is responsible for detecting and identifying anomalies in system and user behavior, ensuring preventive measures are effective and optimized for business and mission functionality, and providing initial response to all cybersecurity incidents.

2. REVISION HISTORY

Date	Version	Approved By:	Policy Update
12/18/2017	1.0	Dr. Dudley-Eshbach	Initial Publication

3. SCOPE

This policy is applicable to all SUIT environments and assets utilized by the University. SUIT will be responsible for continuous monitoring programs in accordance with the requirements in this policy.

4. BASE POLICY AND COMPLIANCE REFERENCES

SUIT policy framework is based upon federal, state, and industry best practices and standards. Below is a listing of the base policy and compliance references from University System of Maryland (USM), Federal, State, and other

organizations. This policy serves as SU's authoritative adaptation of these policies with specific amendments to meet the business and operational needs of the University.

Policy References

- State of Maryland Department of IT - Cybersecurity Policy: http://doit.maryland.gov/Pages/DoIT-Policy-List.aspx
- USM Security Guidelines: http://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf

5. POLICY

An inherent part of a continuous monitoring program's implementation is University identification and mitigation of risk. It is SUIT's mission to ensure proper security integration within the IT infrastructure and to fully implement effective detection and prevention security measures without disrupting the wide range of University mission and business needs.

An operational continuous monitoring program provides SUIT the ability to detect and prevent network and system exploitation by observing real-time traffic flow behaviors and by correlating log events to baseline trends in near real-time. The following subsections describe the policy requirements for event logging, continuous monitoring, incident response, and training and awareness.

5.1 SUIT Continuous Monitoring Program

SUIT will establish and implement a continuous monitoring program to maintain continuous situational awareness of the security posture of the University. The continuous monitoring program will, where possible, implement the functions listed in the table below:

#	Name	Requirement
A	Monitor Events	Use automated tools to aggregate traffic data, syslog and event logs, and application and device alerts and logs. These tools will allow SUIT to observe, correlate, and analyze network and system generated data, store required data for historical and analytical purposes, and document anomalies and deviations.
C	Prevent Suspicious Activity	Tune firewalls, intrusion detection/prevention systems (IDS/IPS), and other boundary devices that interact with inbound traffic, both internally and externally, to ensure risks are mitigated in ways that do not adversely affect mission and business functions of the Enterprise agencies.
D	Detect Potential Outbound Malicious Activity	Design and implement methodologies to identify and monitor outbound traffic for indicators of compromise that include detecting increases in endpoint traffic and outbound connections, increases in data or account access attempts, and other changes in baseline behaviors.
E	Analyze Aggregated Data	Analyze data using baseline comparison, trend analysis, and threat intelligence and implement a medium for documenting alerts and incidents along with maintaining any annotations and corrections made to rulesets or systems.
F	Reporting	Generate and provide tailored reports to SUIT and other relevant personnel or departments.

5.2 Centralized Analysis Tool

To ensure effective monitoring, SUIT analysts must have access to a large amount of network and system data. To parse through that data for threat indicators, an analyst will need to use a centralized logging and analysis capability, such as a System Information and Event Management (SIEM) tool, that allows a comprehensive view of the environment that is efficient and scalable within the network. The table below identifies the functions this tool should be able to perform.

#	Name	Requirement
A	Aggregate Data	Where possible the analysis tool must have a robust data schema to aggregate and normalize data across many different devices; this ensures all data can be ingested by the tool for correlation and tracking.
B	Categorize Events	Configure the tool to parse data into an easily understandable and have the ability to integrate new devices.
C	Correlate Simple Events	Where possible, aggregate events to enable using multiple events to detect otherwise unnoticeable deviations. This allows several events to be correlated and re- evaluated against other alerts.
D	Correlate Multi-Stage Events	Analyze information from a variety of disparate events for any relationship to other events.
E	Prioritize Monitoring and Alerting	Tag, or be able to report on, targeted assets for special scrutiny, based on the risk or mission-relevance of the asset. Any asset containing or processing confidential information, including financial processing, should generate alerts of the highest priority when monitored.
F	Analyze Statistical Data to Detect Anomalous Behavior	Detect events of significance by identifying mathematical deviations as anomalies from normal traffic such as sharp increases in activity on a particular port, protocol, or event type.
G	Maintain Historical Data and Events	Provide historical or forensic information to determine frame of reference and tracing of any incident over time. This will allow the incident investigator or analyst to go through the data history while tracking the incident and the level of compromise. Data can be reevaluated for compromises that may have gone undetected.
H	Correlate Physical and Logical Events	Make correlations between physical access systems and logical security devices, e.g. operating system logs or VPN data. This allows detection of events and incidents that correlate to alerts like a geographic access violation or suspicious physical activity, such as afterhours building access.

5.3 Continuous Monitoring

During day-to-day operations, the continuous monitoring program will identify and monitor key threat indicators for:

- Deviations from established operational baselines
- Unauthorized changes to network and system configurations
- Potential security-control violations to network and system devices and applications

A list of criteria required to effectively monitor a network is identified in the table below, it is not an exhaustive list.

#	Name	Requirement
A	Intrusion Prevention	Monitor network boundaries for intrusion attempts, and: ▪ Analyze inbound network traffic to ensure firewall rules are properly tuned to filter unauthorized connections; analyze dropped outbound packets for attempted invalid connections (this may indicate an adversary attempting to establish a command/control channel through an unmonitored port) ▪ Ensure IDSs are configured to balance issues of false positive and false negative alerts and that firewalls and IPSs are not prohibiting legitimate traffic and impeding agency business functions.
B	Outbound Detection	Monitor outbound connections where possible for: ▪ Data exfiltration ▪ Number and length of unauthorized connections ▪ Unauthorized ports and service access
C	Audit Network and System Events	Review events to detect: ▪ Access control violations, ▪ The creation and deletion of key system and network accounts ▪ Assignments of elevated privilege of key accounts
D	Monitor Endpoint Protection	Monitor alerts from endpoint security tools.
E	Monitor Cyber Threat Intelligence (CTI) Resources	Maintain active engagement and awareness of current and potential threats by monitoring cybersecurity information feeds, fostering relationships with other cybersecurity entities, and utilizing CTI databases through commercial vendors or government organizations.
F	Critical Application Audit Trails	Monitor alerts for modifications to critical applications and administrative level accounts or permission sets.

5.4 Incident Response

SUIT staff responsible for the continuous monitoring program will be familiar with the SU Incident Response policy.

6. EXEMPTIONS

If an exemption from this policy is required, an SUIT Policy Exemption Form needs to be submitted and it needs to clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks associated with this exemption. If the University can accept the risk, an exemption to this policy may be granted**.**

7. DEFINITIONS

Term	Definition
Cyber Threat Intelligence (CTI)	Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.

8. ENFORCEMENT

SUIT is responsible for ensuring the continuous monitoring program for the University. Any systems under the policy authority of SUIT with requirements that deviate from the SUIT Security Program policies are required to submit a Policy Exemption Form to SUIT for consideration and potential approval.

Any attempt by personnel to circumvent or otherwise bypass this policy or any supporting policy will be treated as a security violation and subject to investigation. The results of the investigation may entail written reprimand, suspension, termination, and possibly criminal and/or civil penalties.