

7/19/23

Real-time, Continuous Risk-Management for macOS

Brandon Mesa

- Principal Solutions Engineer @ Qmulos
- in/brandonmesa
- bmesa@qmulos.com

Joseph Becker

- Splunk Engineer @ Qmulos
- in/joseph-d-becker
- jbecker@qmulos.com



Objectives

- Understand macOS Risk Management
- Understand the value of auditing your macOS systems
- Understand the importance of a high-fidelity audit policy

Agenda

- Auditing
- Synthesize an Audit Policy
- Threat Detection
- Operational Compliance
- System Configuration Audit
- Q&A

MacOS devices under threat as data shadows

Updated on: 10 July 2023

NEWS 31 MAY 2023

New "Migraine" Flaw Enables Attackers to Bypass MacOS Security

Dangerous Password Attacks Targeting Windows, macOS, and Linux Software Developers

Japanese Cryptocurrency Exchange Falls Victim to JokerSpy macOS Backdoor Attack

Lazarus Subgroup Targeting Apple Devices with New RustBucket macOS Malware

Researchers Discover New Sophisticated Toolkit Targeting Apple macOS Systems

How is it happening?

- Software Supply Chain Attacks
- Phishing
- Adware

Threat Landscape

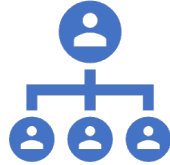
- Increase in malware compatibility
- Sophisticated threat actors with advanced tactics and techniques



Risk Management



Endpoint
Security

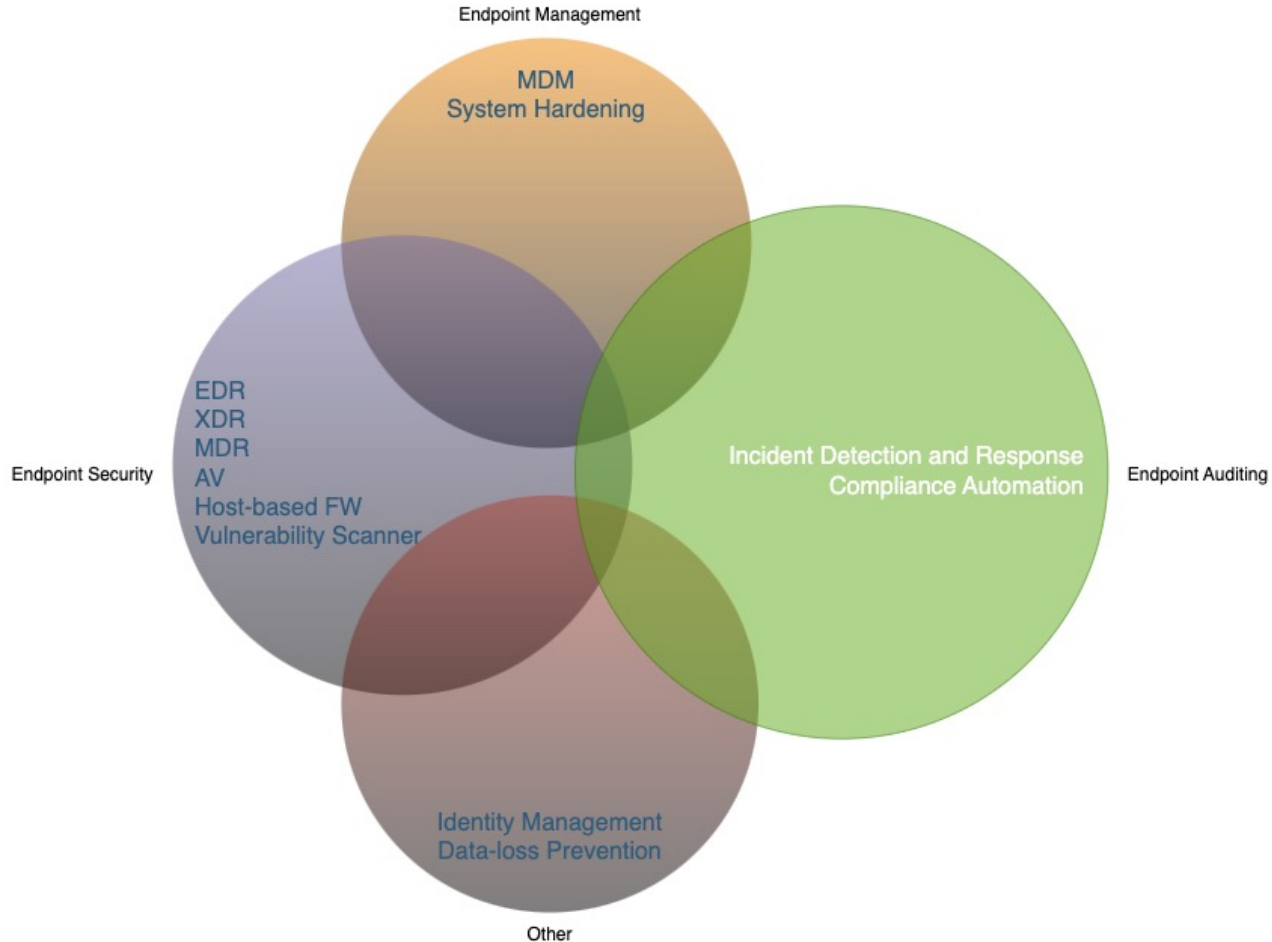


Endpoint
Management



Endpoint
Auditing

Risk Management Overview



Why audit if I already have...

- Endpoint Security
- Endpoint Management

System Auditing

What is system auditing?

**Why audit
macOS?**



How to audit macOS?



What is a System Event?

- Any activity that occurs on a macOS asset, typically carried out by users or processes

macOS APIs

Open-Source Tools

The icon for eslogger consists of a dark blue rounded rectangle with a light blue rounded rectangle inside it, slightly offset to the top-left.

eslogger

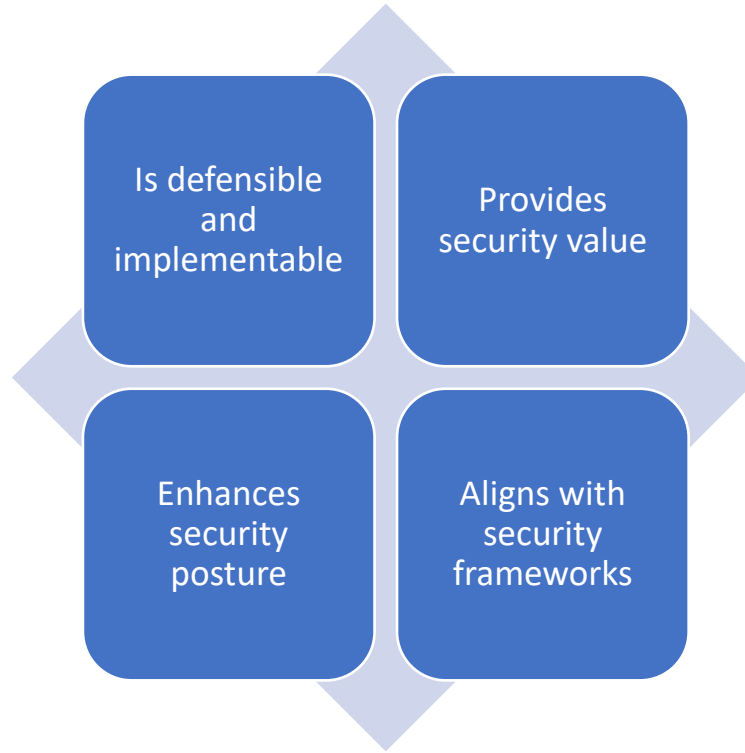
The icon for osquery consists of a dark blue rounded rectangle with a light blue rounded rectangle inside it, slightly offset to the top-left.

osquery

The icon for mSCP consists of a dark blue rounded rectangle with a light blue rounded rectangle inside it, slightly offset to the top-left.

mSCP

A strong audit policy...



Synthesizing an Audit Policy

Synthesizing an Audit Policy

- Federal Guidance:
 - OMB M-21-31

Activity of Interest

User Access to OS
Components and
Applications

System
Performance and
Operational
Characteristics

System
Configuration

File Access

Host Network
Communications

Command-Line
Interface

Firmware

User Access to OS Components and Applications



File and Object
Access



Audit Log Access



System Access and
Log Off



Remote Terminal
Access and Log Off

System Performance and Operational Characteristics



Resource
Utilization



Process Status



System Events



Service Status
Changes



Service Failures
and Restarts

System Configuration



Changes to Security
Configurations



Audit Log Cleared



Changes to Accounts



User or Group
Management Changes



Scheduled Task Changes

Data Exfiltration

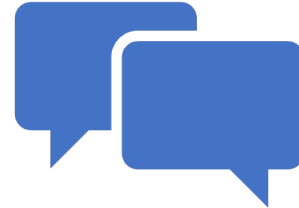


Transfer of data to external
media or remote hosts

Host Network Communications



Listening Network Port and IP
Address



Active Network Communication
with Other Hosts

Command-Line Interface



System Logs



Analytics Data



Wi-Fi Log



System
Application Logs



System Reports



User Application
Logs



User Reports



Audit Logs

Firmware



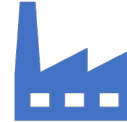
Version



Created Date



Installed Date



Manufacturer



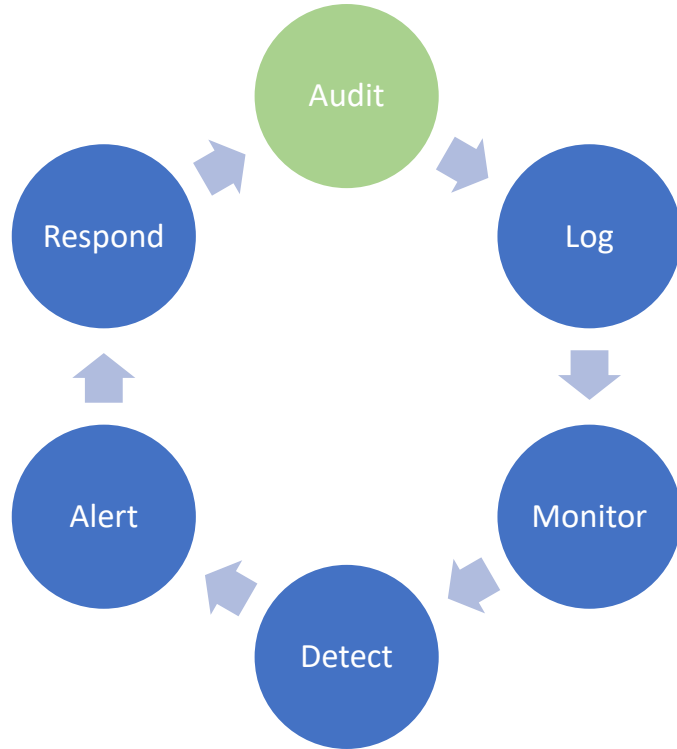
Security Use Cases

Security Use Cases

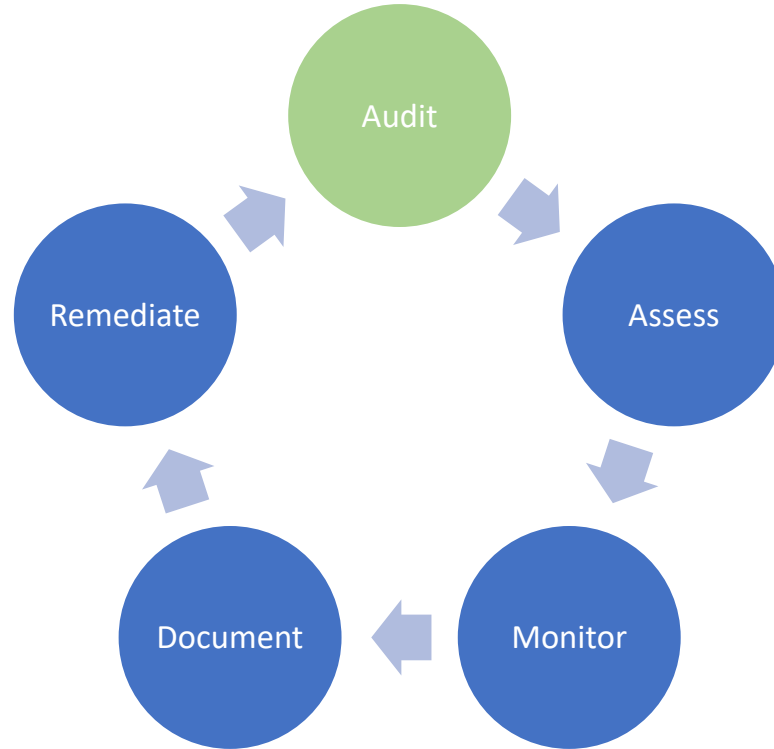
- Incident Management
 - Threat Detection
- System Compliance
 - Technical Controls
 - System Configurations



Incident Management



System Compliance



Monitoring, Detecting, Alerting

Monitoring

- Continuously assess the state of your macOS system
- Typically accomplished with a log management platform

Detection & Alerting

- Identify anomalous, unauthorized, or malicious activity
- Alert when:
 - Assets are not compliant
 - Malignant activity
 - Anomalous system performance

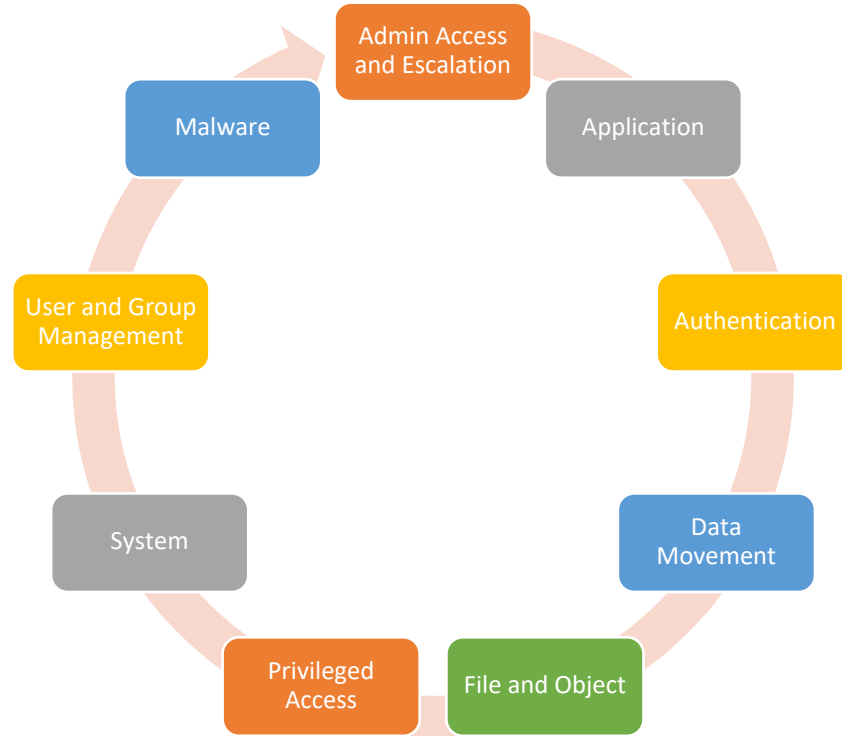
Open-source Log Management

- ELK
- Grafana + Loki
- Graylog



Threat Detection

Threat Detection



Monitoring and Detecting Threats

Admin Access and Escalation – Security Objectives

- Audit and monitor privileged accounts and processes to ensure that they haven't been compromised or misused

Admin Access and Escalation – Monitoring Capabilities



Identify privilege
escalation attempts



Identify privileged
authentications



Identify privileged
system events

Admin Access and Escalation – Data of Interest

- Operating System logs
 - Logd
 - Endpoint Security
 - Authentication
 - Process
 - Su
 - Sudo

In Practice - eslogger

```
% eslogger authentication exec su sudo | tee -a privileged_access.log
```

* must run as a privileged process with Full Disk Access

Admin Access and Escalation – What to Monitor?

Top Users by
Privileged
Executions

Top Processes with
Privileged
Executions

Privileged Access
and Executions
(Successful and
Failed)

Anomalous
Privileged
Escalation and
Access

Failed Privileged
Executions by User

Recent Privileged
Events

File and Object – Security Objectives

- Monitor file access activity to ensure users and processes are accessing authorized files and directories

File and Object – Monitoring Capabilities



Monitor file ownership, permissions,
and status



Identify user or process attempting file
operation to establish accountability

File and Object – Data of Interest

- Operating System logs
 - Endpoint Security
 - Access
 - Clone
 - Copy
 - Close
 - Create
 - Open
 - Rename
 - Write
 - Unlink

In Practice - eslogger

```
% eslogger create unlink access | tee -a file_management.log
```

* must run as a privileged process with Full Disk Access

File and Object – What to Monitor?

File permission
changes by
user

File ownership
changes by
user

File deletions
by user

Anomalous file
changes

Failed
operations by
user

Application - Security Objectives

- Identify unauthorized processes running on hosts

Application – Monitoring Capabilities

- Monitor application execution throughout the environment
- Assess hashes to monitor for malicious processes

Application – Data of Interest

- Operating System logs
 - Endpoint Security
 - Process Execution

In Practice - eslogger

```
% eslogger exec | tee -a process_activity.log
```

* must run as a privileged process with Full Disk Access

Application – What to monitor?

Top Off-Profile
Application
Executions

Top Hosts with
Applications
Executed in User
Folders

Application
Initializations

Anomalous
Application
Initializations

Recent Application
Initializations

Recent Off-Profile
Application
Initializations

Recent Watchlisted
Application
Initializations

macOS Endpoint Security API

- https://developer.apple.com/documentation/endpointsecurity/3228936-es_events_t

Alerting on Threats

Security Objectives

- Efficiently alert on threats and indicators of compromise
- Optimal time to detection enhances time to response

Alerts of Interest

Unauthorized local
device access

Unauthorized local
executable

Unauthorized
privileged access

After-hours
privileged access

Anomalous system
restarts/shutdowns

Defense evasion

Malicious code
detection

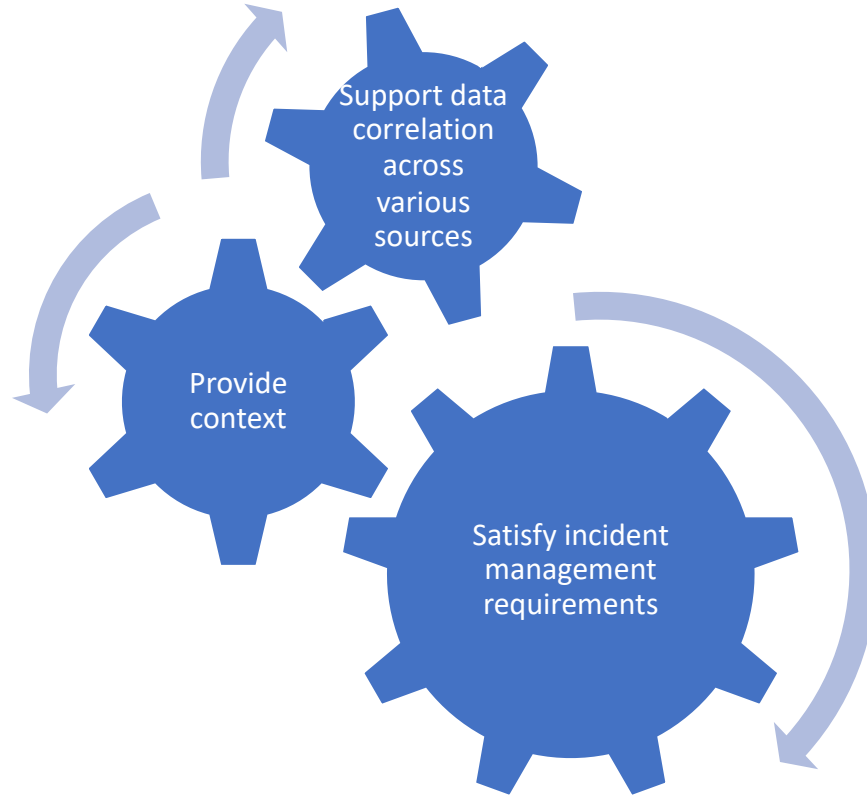
Malware
installation

Printing to local
devices

Uploading from
local devices

Downloading to
local devices

Alerting on Threats should...



How is threat alerting accomplished?



EDR/MDR/XDR/AV

Log Management
Platforms

SIEMs

Threat Detection Resources for macOS

- Sigma
 - <https://github.com/SigmaHQ/sigma>
- Atomic Red Team
 - <https://github.com/redcanaryco/atomic-red-team>
- MITRE ATT&CK Matrix
 - <https://attack.mitre.org/>

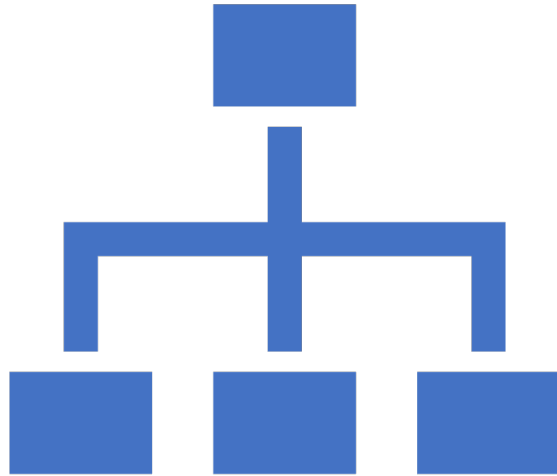
Compliance

Compliance

- Why compliance?
- Risk Management
- RMF overview
- Control libraries
- Continuous monitoring
- Secure configuration guidance with NIST SP-800-219



Why Compliance?



What is a Risk Management?

Common Risk Management Frameworks

NIST RMF

NIST CSF

COSO

ISACA's Risk
IT Framework

OCTAVE

FAIR

TARA

ISO/IEC
31000

NIST Risk Management Framework

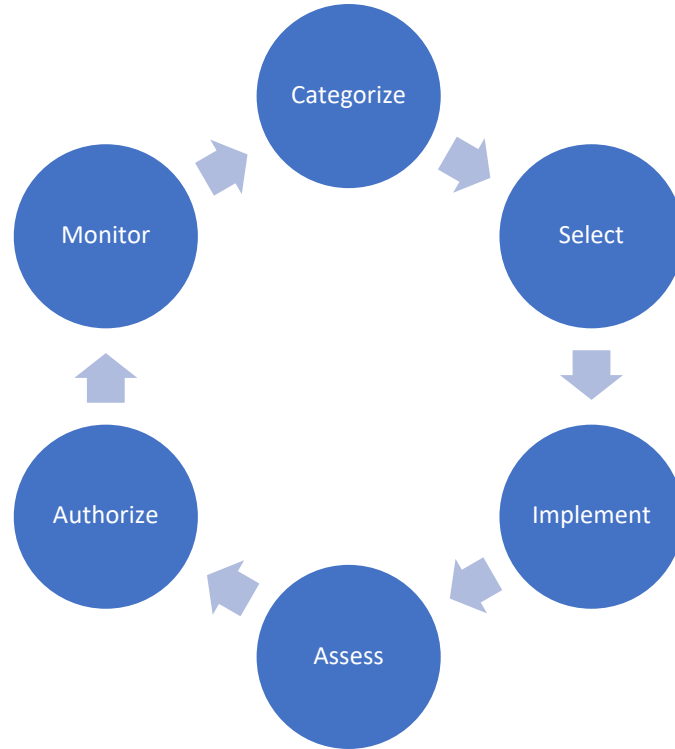
About NIST RMF

- A guideline for monitoring, assessing, and resolving risk
- Dictates how systems must be architected, secured, and monitored
- Provides a process to integrate and maintain security, privacy, and supply chain risk management activities into the system development life cycle
- Provides a risk-based approach to control selection and specification

About NIST RMF

- Consists of six phases to be continuously performed throughout the life of the organization
- Intended as process to identify and respond to threats
- Exercising it will establish a security infrastructure and an ongoing improvement of the environment's security posture

RMF Phases



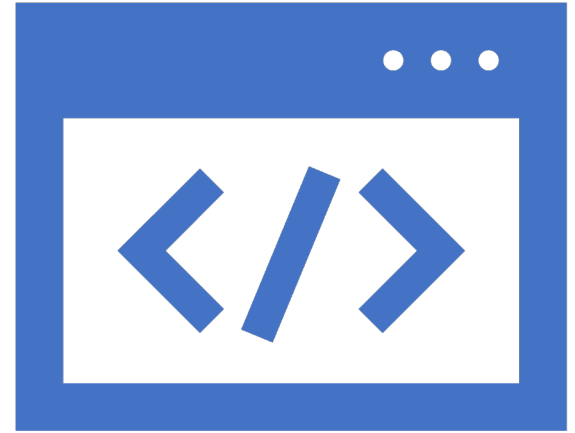


RMF – Categorize

RMF – Select



RMF – Implement

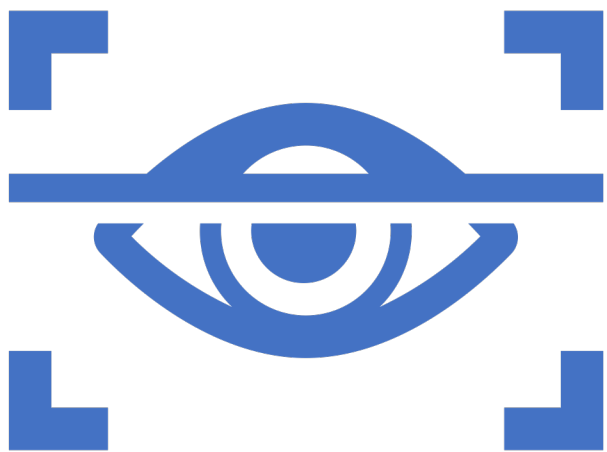


RMF – Assess



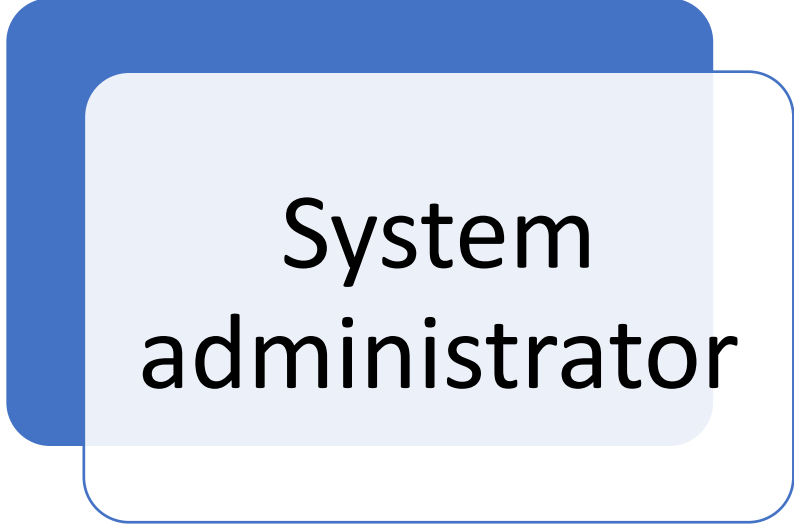
RMF – Authorize



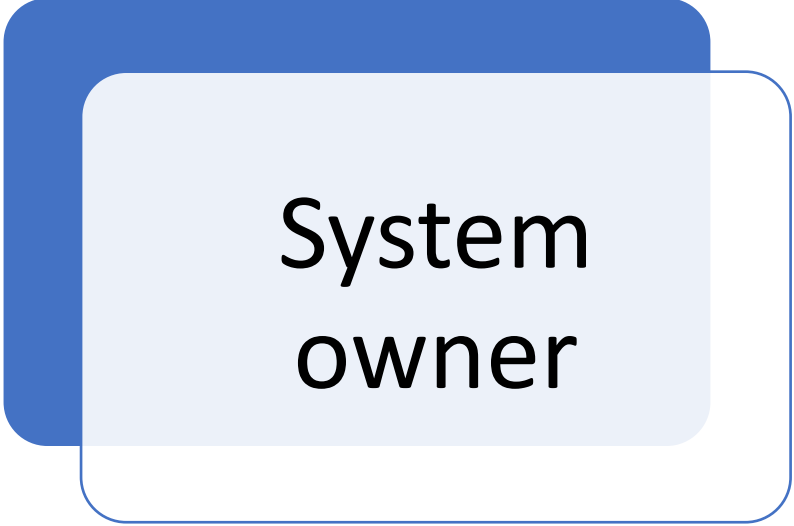


RMF – Monitor

RMF – Your responsibilities as a...



System
administrator



System
owner

Now that we have a framework for risk management...

- How do we track security and privacy for information systems at a granular level?

Control Libraries

NIST 800-53, CIS, ISO 27001, COBIT

System security and privacy is managed via controls

- What is a control?
- Where do they come from?

Continuous System Monitoring

Continuous System Monitoring

- Maintain ongoing situational awareness about the security and privacy of the system to support risk management decisions

Continuous System Monitoring - Outcomes

- Ongoing assessments of control effectiveness
- Output of continuous monitoring activities analyzed and responded to
- Process in place to report security and privacy posture to management
- Ongoing authorizations conducted using results of continuous monitoring activities

Continuous System Monitoring - Tasks



- Ongoing Assessments
- Ongoing Risk Response
- Security Privacy and Reporting



Secure Configuration Guidance

NIST SP 800-219 – macOS Security Compliance Project

What is NIST SP 800-219?

- Secure configuration guidance for macOS using mSCP
- Secure and assess macOS system security in an automated fashion
- Leverages security baselines to establish configuration requirements
- Atomic in nature

Closing Thoughts

- Define and implement a high-fidelity audit policy
- Support organizational security initiatives
- Monitor for anomalous activity across your assets
- Minimize risk by continuously assessing the security posture of your system against technical controls
- Assess the configuration state of your devices against baselines

Q&A

Feedback

- Leave us a session review @ <https://bit.ly/psumac2023-124>



Thank You!