Manage Security Operations

Dr. Lyron H. Andrews

CISSP/CCSP/SSCP/CRISC/CISM/CCSK

https://www.profabula.com/whyprofabula

Overview

Define the standards for establishing and maintaining a security operations center

Review and demonstrate how to configure cloud security monitoring

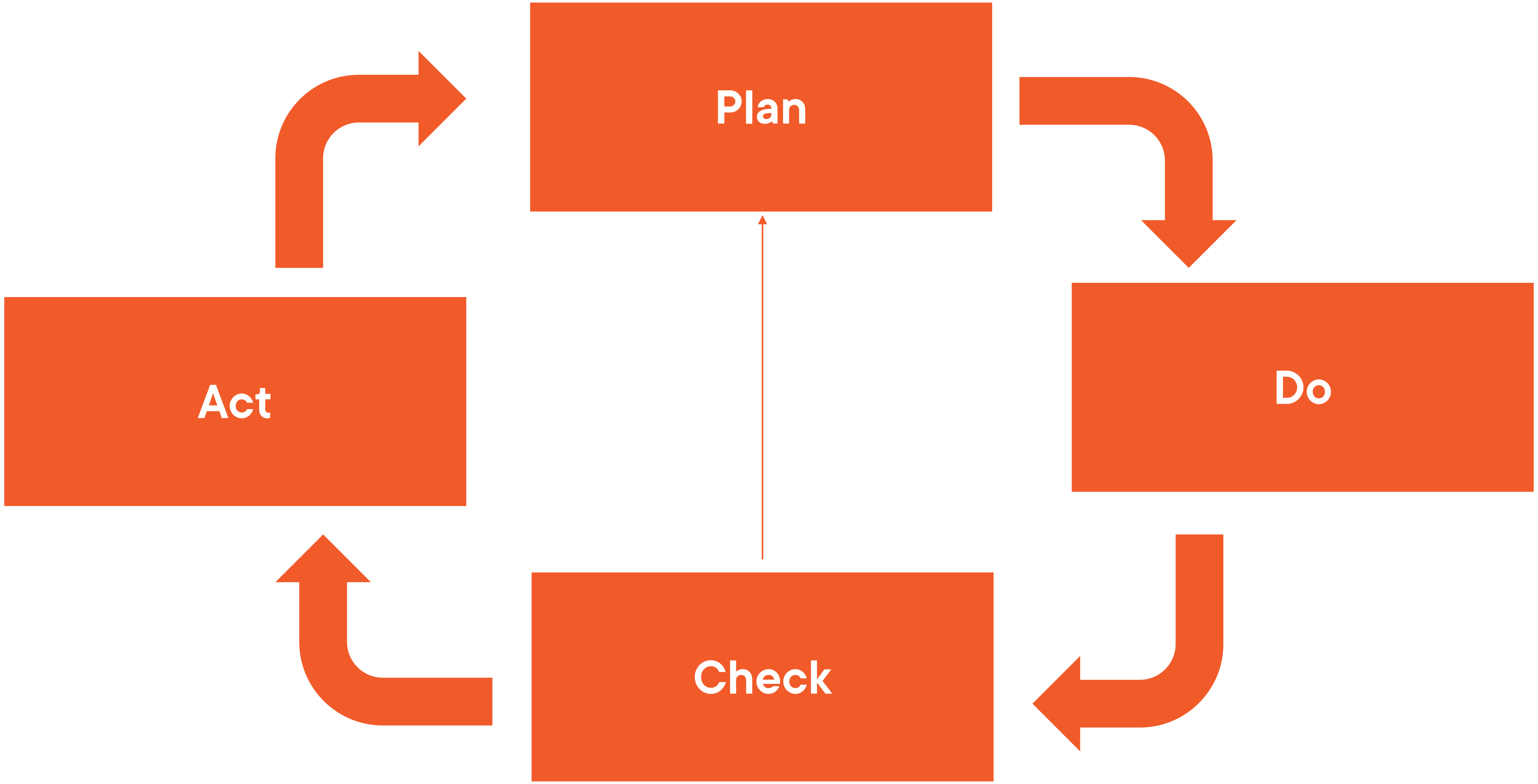
Establish a plan for digital forensics

Security Operations Center Standards

ISO/IEC 18788-2015, Management Systems for Private Security Operations

- Business and risk management for security operations
- Designed for problematic facilities
- Assess and manage impact
- Accountability to law and human rights
- Matches organizational mission

Operational by Plan, Do, Check, Act (PDCA)



Plan

Do

Check

Act

Policy of SOMS

Management commitment

Human rights

Continuous improvement

Resources

Risk assessment

Legal requirements

Objectives to achieve

Strategic programs

Risk management strategies

Planning of SOMS

Operational control

Resources and roles

Competences

Documentation

Prevention

Implementation and Operation of SOMS

Monitoring

Compliance evaluation

Testing

Correction

Audit

Performance Evaluation of SOMS

Effectiveness

Needed changes

Improvement

Management review of SOMS

Intelligent Monitoring of Security Controls

Information security continuous monitoring (ISCM) is “maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.”

NIST SP 800-137 Information Security Continuous Monitoring

Risk management

Measurable

Effective controls

Verifies compliance

ISCM strategy

Supports visibility

Maintains change control

Maintains awareness

ISCM strategy

Implementing Log Capture and Analysis

Guide to Computer Security Log Management

Logs

Event record

Security

Many sources

Elements of Log Collection

Regulatory

Accountability

Performance

Real-time alerts

Event correlation

Incident response

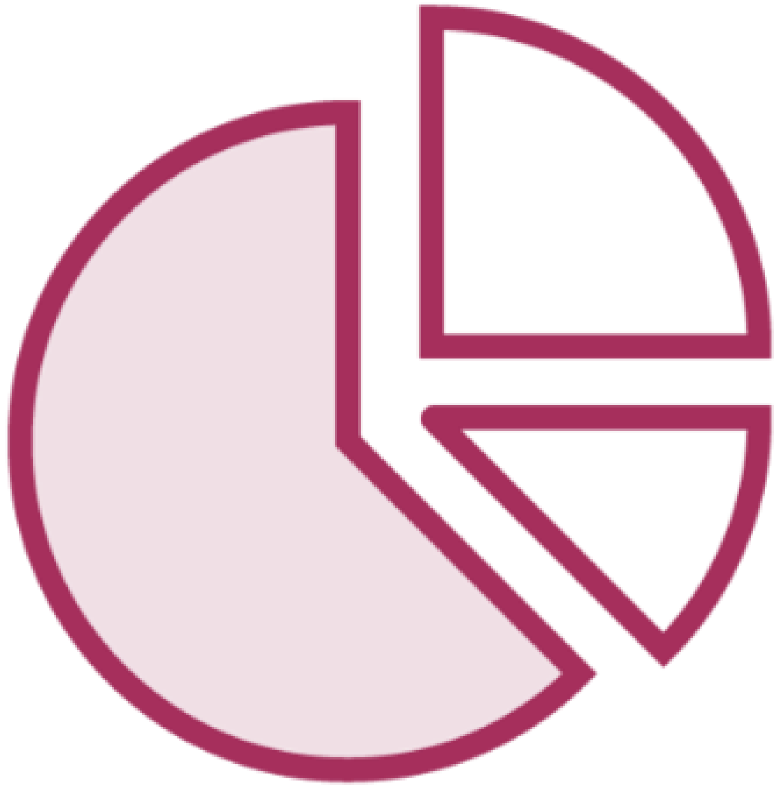
Log Management Process

Define requirements

Develop policies

Develop processes

Factors Influencing Log Design



Cost

Volume

Bandwidth

Storage

Security

Resources

Security Concerns for Logs

Logging status

Log rotation

Patch application

Synchronized time

Reconfiguration

Operational

Security Information and Event Management (SIEM)

Raw data

Aggregation

Normalized

Analyzation

Alerting

SIEM Characteristics and Benefits

Locally hosted

Externally hosted

Hybrid

External storage

DR support

Privilege users

Next Generation Log Management

Offering from providers

UBEA driven

Growing usefulness

Cloud Monitoring

Cloud Monitoring

Inordinate data flows

Varied services

Must meet goals

Multi-cloud capabilities

Demo

We will log into the AWS and configure monitoring

We will use CloudTrail and CloudWatch

- It is important to understand all the API accesses
- We will set up monitoring for changes made to the security group.

Support Digital Forensics

Digital Forensics Guidance

ISO/IEC 27037

Step 1: Prioritization plan to acquire data

- Value
- Volatility
- Effort

Digital Forensics Guidance

ISO/IEC 27037

Step 2: Acquire data

- Use of forensics analysis and duplication tools
- Local capture preferred but may not be feasible

Digital Forensics Guidance

ISO/IEC 27037

Step 3: Verify integrity of data

- Proof of untampered copy
- Use tools to compute digests

Forensics Complications in the Cloud

Privacy

Provider Dependencies

Competent Actors

Location of Physical Data

Trustworthiness of Evidence

Evidence Management

Keep detailed log of steps

Take a photograph of environment

Single person should be custodian

Document, document, document

Maintain Chain of Custody

Chronological documentation highlighting

- Seizure
- Custody
- Control
- Analysis
- Disposition

Summary

What risks can be addressed by means of your cloud monitoring program?

How do the items that you monitor line up with your business requirements?

What areas of physical and logical cloud security deserve your greatest attention?