Inter IIT Tech Meet 12.0

CERT-IN

TEAM - 41

Outline

01. Intro to Controls and Baselines
02. Designing baselines, Vulnerability mitigation
03. Incident Detection and Response integration
04. Auditing solutions
05. Design for an Audit helper application

Outline

01. Intro to Controls and Baselines

02. Designing baselines, Vulnerability mitigation

03. Incident Detection and Response integration

04. Auditing solutions

05. Design for an Audit helper application

Controls and Baselines

- Control: High level description of a feature; not specific to technology/implementation
- Baseline: Implementation of the controls, integrated with business requirements

Why baselines?

- Improved security posture
- Consistent protection measures
- Compliance certainty
- Improved visibility and control
- Flexible baselines: Adapting to changing threats

Outline

01. Intro to Controls and Baselines
02. Designing baselines, Vulnerability mitigation
03. Incident Detection and Response integration
04. Auditing solutions
05. Design for an Audit helper application

Designing and Maintaining Baselines

1. **Classify controls:** Network security, Physical security, Application Security, Data integrity
2. **Define requirements and metrics:** Attack surface metrics, Unencrypted data stores, Default privileges and more
3. **Integrate industry standards:** Compliance checks (GDPR, HIPAA), CIS benchmarks
4. **Create a technical design:** Interfaces between software, Security implementation designs, User authorization
5. **Development methodologies:** Change management, IDS/IPS integration, Risk assessment methods, Code security tests

REFERENCES - CERTIFIED INFORMATION SECURITY MANAGER (CISM): INFORMATION SECURITY PROGRAM
HTTPS://LINKEDIN.COM/LEARNING/CERTIFIED-INFORMATION-SECURITY-MANAGER-CISM-CERT-PREP-2022-3-INFORMATION-SECURITY-PROGRAM/INFORMATION-SECURITY-PROGRAM

Mitigating Vulnerabilities

- **Network security:** Firewalls, Private connections, Logging, NDRs, Access controls, DoS protections
- **Application/Software security:** SAST/DAST implementations, Data protection, Identity management
- **Physical/Hardware security:** Biometric security, Hardware exploit checks, Extensive Logging
- **Security tools training:** Training platforms, Composition Analysis tools, Regular assessments

Minimizing Risks

- Least privileges principle, Data hiding
- Attack surface checks: Individual and Organizational - External modules/API usage assessment
- Regular configuration updates
- Automated backups
- EOL: Data erasure
- Social Engineering: Organization policy training

Outline

01. Intro to Controls and Baselines

02. Designing baselines, Vulnerability mitigation

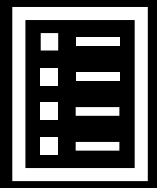
03. Incident Detection and Response Integration

04. Auditing solutions

05. Design for an Audit helper application

Incident Detection and Response

Logging



Continuous monitoring, Standardized logs, Centralized consoles, Contextualization and Redundancies

Automated Detection

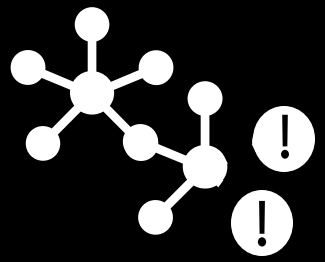
Threat level assessment, Dynamic correlation rules, Ticket management

Automated Threat Hunting

Proactively search for signs of compromise or abnormal behavior

Incident Detection and Response

Contain

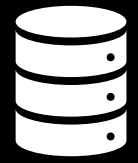


Evidence collection, Isolation, Automated context generation

Eradicate

Strengthening controls, Pace up baseline implementation, Reporting

Recover



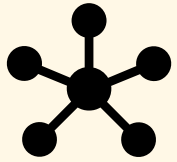
Restoring backups, Resurgence monitoring, Stakeholder communication

Incident Detection and Response

SIEM

Security Information and Ev ent Management

NDR



Network Detection and Response

EDR

Endpoint Detection and Response

Indicators of Compromise

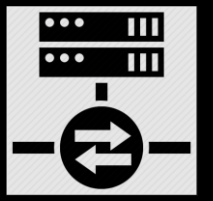
Failed Logins

Multiple failed login attempts might be a sign of a brute force attack

Geolocation Checks

Logging in from multiple locations within a short amount of time

Unusual Traffic



Unusual inbound and outbound network traffic

Extended Detection and Response

- **Intelligence sharing:**
  Shared SIEM, EDR intelligence
- **Analyse:** Uses Reinforcement Learning with XAI and User Behavior Analysis
- **Investigate:** Reactive and Proactive investigation into root cause, Automated risk scoring
- **Respond:** Use SOAR to automate and orchestrate a valid response.

Outline

01. Intro to Controls and Baselines
02. Designing baselines, Vulnerability mitigation
03. Incident Detection and Response integration
04. Auditing solutions
05. Design for an Audit helper application

Elevating Audit Efficiency

- Streamlined adoption process, integration with existing systems, and dynamic interface.
- Integration with existing servers and IAM systems
- Designed solution to enrich the audit process for auditors, auditees, and regulators.
- Empower auditors with features like customizable checklists and automated tasks.
- Facilitates clear and efficient communication throughout the audit process

Outline

01. Intro to Controls and Baselines
02. Designing baselines, Vulnerability mitigation
03. Incident Detection and Response integration
04. Auditing solutions
05. Design for an Audit helper application

AuditApp Functionalities at a Glance

Landing Page

Secure Single Sign-On (SSO) for user convenience and enhanced application security.

Audit Planning and Scheduling

Systematic audit framework (internal and external), compliance notifications

Resources Page and Communication Hub

Training materials for continual professional development, tailored to both auditors and auditees.

Audit Data Collection

Seamless collaboration through Q&A, categorized evidence storage for automated reporting

Audit Data Analysis

Find instances of non-compliance, visualizations

Key Features

- Audit Quality Assurance: Certification and historical records
- Collaboration with regulatory bodies for industry compliance
- Continuous improvement through feedback and updates

AuditApp

Good Morning, Auditee !

- Dashboard
- Schedule
- Adminstration
- Insights
- Connect
- Profile
- Settings

Auditee

Real time CIS benchmark	Vulnerability count	Open tasks	Estimated Score
54%	14	156	53
Wed, Jul 20	Currently testing: 4	98 auditors working	

Compliance history

Months

Audit Checklist

Current | See All

Tasks		Tasks	
Define Risk Assessment Metrics	More	Unknown Vulnerability detection	More
Conduct Gap Analysis	More	Provide necessary documentation	More
Participate in Compliance Check	More	Remediate vulnerabilities	More
Known Vulnerabilities test	More	New Task	More

Compliance

- GDPR
  - Internal 24%
  - External Request An Audit
- HIPAA
  - Internal ✓
  - External 60%
- PCI-DSS
  - Internal ✓
  - External Request An Audit
- FISMA ✓
- SOX 60%

AuditApp

Good Morning, Auditor !

- Dashboard
- Schedule
- Adminstration
- Insights
- Connect
- Profile
- Settings

Auditor

Baseline: CIS | Section: Software | Audit Type: Internal

Task Management
Active: 47/80
Pending: 33/80
Unassigned: 29

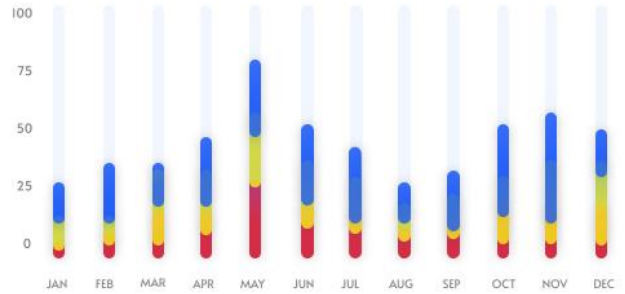
Teams More
Frontend: 5
Networking: 3
Backend: 4

Av. Patch Time
2d 4hr
Av. Patches/day: 17
Av. Patches/tm: 6

Compliance Score History
64%

Risk Heat map
Resilience Score: 3.5

Patch Deployment Frequency Risk Value | Month



Weakest Sections More

- Commercial API Protections — 35% Info
- Deployment and Containerization — 24% Info
- Third Party Dependencies — 17% Info

Strongest Sections More

- Exception Handling — 3% Info
- Secrets Management — 4% Info
- User Privileges & Access Control Checks — 6% Info

Assigned Tasks Latest

- CVE-2023-44228 - Buffer Overflow — Info | Manage 18 ▲
  Jesse Thomas
- [NEW] VN-2023-F81 - Privilege Escalation — Info | Manage -2 ▼

Reports Approval Rate

- Product Delivery Modules - Code Security — View | Manage 12 ▲
  97% Approval rate
- User activity and data retention - Compliance — View | Manage 35 ▲

Thank you

Open For Questions!