The Future of Risk Management: Continuous Monitoring

Matt Cooper, Sr. Manager, Privacy, Risk & Compliance, Vanta
Rob Picard, Security Lead, Vanta

ISACA VIRTUAL SUMMIT

Today's Speaker

Matt Cooper

Sr. Manager, Privacy, Risk & Compliance

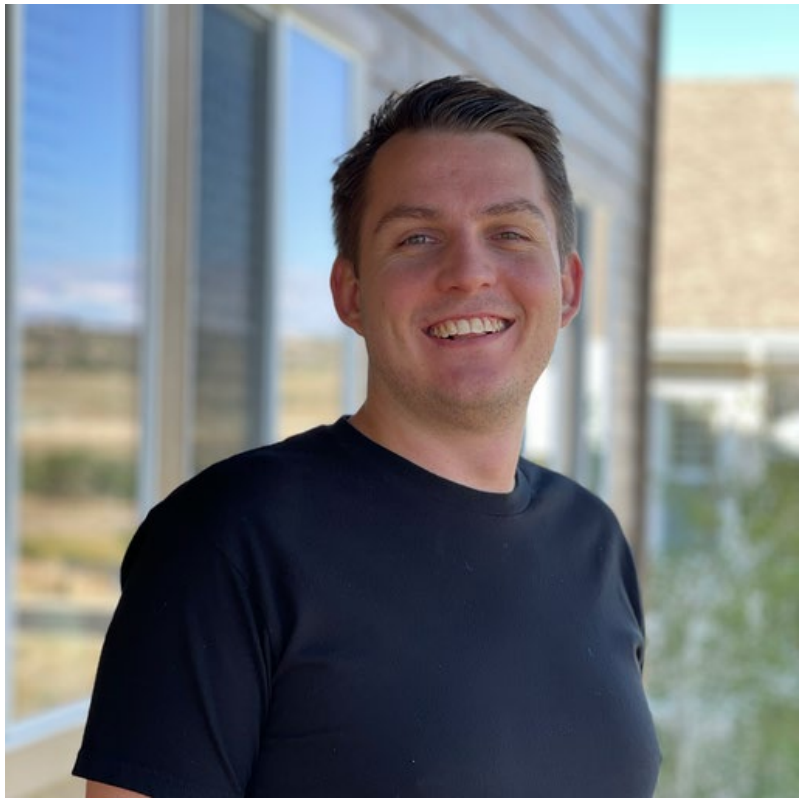
CPP, CISSP, CCSP, CISA, ISO 27001 LA,

CIPM, CIPT, CIPP/US, CIPP/E

Vanta

ISACA VIRTUAL SUMMIT

Today’s Speaker



Rob Picard

Security Lead

Vanta

Agenda

- Definitions
- Code security
- IaC
- CI/CD
- Vulnerability management
- Capacity and performance management
- Logging and alerting
- IAM
- CSPM
- Device and MDM
- Email and phishing
- Vendor and supplier security
- Compliance automation
- Privacy operations
- Reporting and metrics
- Questions

Key Learnings

- What are the risks with point-in-time assessments?
- What does continuous monitoring and automation really mean?
- How can an organization enhance their security posture and gain trust with automation?

Automation & Continuous Monitoring

Definitions:

Automated security monitoring

Use of automated procedures to ensure security controls are not circumvented or the use of these tools to track actions taken by subjects suspected of misusing the information system.

Information security continuous monitoring

Maintaining ongoing awareness to support organizational risk decisions

Now we are going to walk through the common cybersecurity and compliance automation and monitoring domains.

For each domain we will discuss:

- The control activity which can be automated and its security objective
- Risks the controls address
- Discussion of the use cases

Code security

Control(s)

- Identifying and remediating vulns, enforcing code standards, code security testing

Risks

- Introduction of new vulnerabilities into production
- Introduction of misconfigurations
- Errors or malicious insider actions

Use cases

- **Linting:** code base uniformity and cleanliness, optimized for readability, enforce patterns (i.e. no print statement)
- **Unit & Integration:** Unit testing tests the code (how much code is tested is called “coverage”). Integration testing: holistic testing of the running application.
- **DAST/SAST:** Finding vulnerabilities in code before and after it reaches production. “Shift-left”

Infrastructure as Code (IaC)

Control(s)

- Configuration management, change management, SDLC, BC/DR

Risks

- Introduction of new vulnerabilities into production
- Introduction of misconfigurations
- Errors or malicious insider actions (indirect)
- Unavailability of services (indirect)

Use cases

- Automation enabler
- Build consistent configurations
- Apply change management (e.g. peer review) to infrastructure
- Enable easy deployment and CI/CD

Code deployment (CI/CD)*

Control(s)

- Configuration management, least privilege access

Risks

- Introduction of new bugs requiring “roll back”
- Errors or malicious insider actions (indirect)

Use cases

- Continuously deploy code and infrastructure changes
- Reduce opportunity for errors or malicious actions by limiting human access to production environments

Vulnerability management

Control(s)

- Detect and remediate vulnerabilities

Risks

- Exploit of vulnerabilities leads to breach, data corruption or downtime

Use cases

- External, Internal, Application, Container
- Ensure timely remediation of important security issues
- Universal compliance requirement
- Fundamental pillar of a security program

Capacity and performance monitoring

Control(s)

- Capacity planning, performance monitoring (incl. errors), incident response

Risks

- Unavailability or poor performance of services

Use cases

- Ensure sufficient processing capacity (i.e. CPU, memory, disk)
- Ensure system integrity and availability
- Log review and alerting
- Intrusion detection re: anomalous performance issues

Logging and alerting (SIEM)

Control(s)

- Log review, monitoring and alerting, incident detection and response, IDS

Risks

- Breach, intrusion, or exploit not detected (IoC)
- Violations and anomalies not detected or alerted
- Slow and/or ineffective incident response

Use cases

- Infrastructure, application, SaaS logging and alerting
- Cross-enterprise intrusion detection
- Infrastructure control plane
- Application activity (failed logins, privilege escalation)
- SaaS account activity
- IAM activity
- Endpoint security
- Version-control system audit logs
- Rule-based detection of anomalous activity
- Automated triage using business-specific logic

Identity and Access Management (IAM)

Control(s)

- SSO, least privilege, secure logon, authentication factors (MFA)

Risks

- Account takeover
- Access is not authorized (compliance risk)
- Accounts not deprovisioned within SLA
- Intrusion or breach

Use cases

- Automated access workflows
- Enforce MFA
- Detect/block access based on conditions (e.g. suspicious geolocation)
- Manage access groups / elevated privilege
- Offboarding automation

Cloud Security Posture Management (CSPM)

Control(s)

- Configuration hardening and management, continuous security monitoring and alerting, prevent unauthorized access, incident detection and response

Risks

- Misconfiguration leads to intrusion or breach

Use cases

- Monitor secure configurations for cloud platforms
- Limit blast radius manual, human errors
- Reduce window of opportunity for intrusions/breaches
- Detect and alert on anomalous activity

Physical device and endpoint management (MDM)

Control(s)

- Hard disk encryption, AV, Screen lock/timeout, remote lock/wipe

Risks

- Ransomware
- Malware
- Hacker foothold in enterprise leads to breach
- Loss or theft of device leads to breach
- Lack of secure data deletion leads to breach

Use cases

- Monitor and manage device security status
- Automated offboarding
- Remotely manage devices
- Manage / monitor blocked software installation

Email security and phishing

Control(s)

- Incident detection and response, fraud prevention, account security

Risks

- Phishing
- Malware
- Ransomware

Use cases

- Prevent phishing attacks from leading to compromise
- Limit the blast radius of phishing attacks
- Reduce the risk of email-base malware attacks

Vendor & Supplier Management

Control(s)

- Vendor risk assessment, vendor compliance monitoring

Risks

- Supply chain attack
- Noncompliance (i.e. privacy, certification, HIPAA, etc.)
- Supplier breach

Use cases

- Use trustworthy vendors for your most sensitive data and access
- Understand the risks associated with a given supplier
- Visibility into the public footprint of a vendor
- Automate workflows for ongoing review
- Automated discovery of shadow IT

Compliance Automation

Control(s)
- Internal and external audit, certification

Risks
- Exceptions and non-conformities
- Inefficiency and waste

Use cases
- Control mapping & contextualization of security monitoring tests
- Policy update and acceptance
- Evidence and artifact maintenance
- Training completion
- Vulnerability remediation timelines
- Data retention and deletion
- Avoid audit findings

Privacy operations

Control(s)
- Legal and privacy compliance

Risks
- Noncompliance and violations
- Lawsuits and fines

Use cases
- Cookie and tracker management
- Data Inventory / ROPA
- SAR / data deletion
- Privacy program metrics

Reporting and metrics

Control(s)

- Board cyber-risk reporting,
- Management review, understanding and tracking security maturity across domains, reporting to leadership and the board, translating technical risk into the business context to enable decision making

Risks

- Poor governance
- Underperformance
- Lack of visibility or transparency

Use cases

- Measure progress over time, communicate it with stakeholders
- Make better informed decisions regarding resourcing of your security and privacy program

Key Learnings - Recap

- What are the risks with point-in-time assessments?
- What does continuous monitoring and automation really mean?
- How can an organization enhance their security posture and gain trust with automation?

Questions?

ISACA
VIRTUAL SUMMIT


ISACA
VIRTUAL SUMMIT
THANK YOU FOR ATTENDING

ISACA®

VIRTUAL SUMMIT