ISACA MÁSODIK SZERDAI ELŐADÁS

Dirk Schrader **(CISM/CISSP)**

SOC2 Compliance – Challenging TSPs and how to get there

2024. szeptember 11.

ISACA®
Budapest Chapter

FELELŐSSÉG KIZÁRÁSA

Az elhangzott prezentációk tartalmát illetően az ISACA Magyarországi Egyesület nem vállal felelősséget az abban nyújtott információk aktualitásáért, helyességéért és teljességéért.

Az itt elhangzott információk nem feltétlenül egyeznek meg az ISACA Magyarországi Egyesület álláspontjával.

ISACA®
Budapest Chapter

netwrix

SOC2 Compliance – Challenging TSPs and how to get there

Dirk Schrader
VP of Security Research / Field CISO EMEA
Netwrix

Agenda

01 SOC 2, Quick Facts

02 SOC 2, Who cares

03 SOC 2, The Five Trust Service Principles (TSPs)

04 Q&A

05 SOC 2, TSPs vs Netwrix Solutions

SOC 2 (System and Organization Controls 2) is a framework developed by the **American Institute of CPAs (AICPA)** for managing customer data based on five "trust service principles"—*security, availability, processing integrity, confidentiality, and privacy*. It is designed for service providers storing customer data in the cloud, emphasizing security and data protection.

SOC 2 – Quick Facts

What is SOC 2?

- A framework for managing and protecting customer data
- Based on five Trust Service Principles (TSPs)
- Especially relevant for technology and cloud companies

Why is important?

- Builds trust with customers
- Demonstrates commitment to data security
- Can be a competitive advantage

What are the benefits?

- Increased customer confidence
- Improved regulatory compliance
- Enhanced brand reputation

Trust Service Principles (TSPs)

Security

The system is protected against unauthorized access

Availability

The system is available for operation and use as committed or agreed.

Processing Integrity

System processing is complete, valid, accurate, timely, and authorized.

Confidentiality

Information designated as confidential is protected as committed or agreed.

Privacy

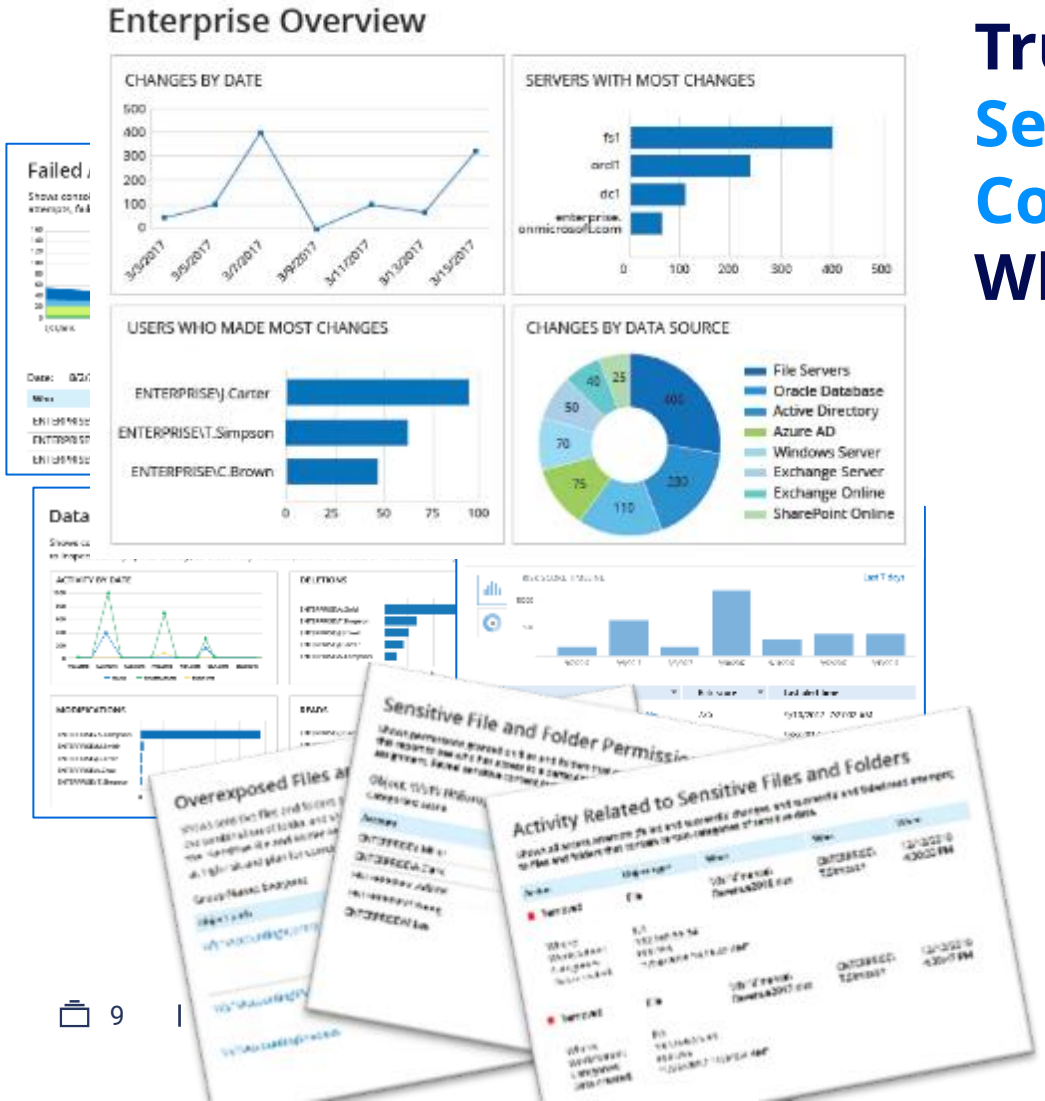
Personal information is collected, used, retained, disclosed, and disposed of in conformity with the commitments in the entity's privacy notice

Steps to Achieve SOC 2 Certification

1. **Define Scope**:
   a) Identify the systems, processes, and data that fall under the scope of the SOC 2 audit.
   b) Determine the relevant trust service principles.
2. **Conduct a Readiness Assessment**:
   a) Assess current policies, procedures, and controls against SOC 2 requirements.
   b) Identify gaps and areas for improvement.
3. **Implement Controls**:
   a) Develop and implement the necessary controls to meet the trust service principles.
   b) Ensure these controls are integrated into daily operations.
4. **Documentation**:
   a) Document all policies, procedures, and controls.
   b) Maintain records of all relevant activities and evidence that demonstrate compliance.
5. **Training and Awareness**:
   a) Train employees on SOC 2 requirements and their roles in maintaining compliance.
   b) Establish a culture of security and compliance within the organization.
6. **Select an Auditor**:
   a) Choose an independent, accredited CPA firm with experience in SOC 2 audits.
   b) Ensure the auditor understands the specific needs and nuances of your business.
7. **Pre-Audit Assessment**:
   a) Conduct an internal review or pre-audit to identify any remaining issues.
   b) Make necessary adjustments based on findings.
8. **Formal Audit**:
   a) Undergo the formal SOC 2 audit conducted by the selected CPA firm.
   b) The audit will include a thorough examination of your controls and processes, as well as testing their effectiveness (for Type II).
9. **Review and Report**:
   a) Review the auditor's report, which will include any findings and areas for improvement.
   b) Address any issues identified in the audit report.
10. **Continuous Monitoring and Improvement**:
    a) Regularly review and update controls to maintain SOC 2 compliance.
    b) Prepare for subsequent audits, especially if seeking SOC 2 Type II certification.

Digital assets audited

Your foundation for SOC 2 compliance



Trust Service Principles:

Security, Availability, Processing Integrity, Confidentiality, Privacy

Why:

- Provide visibility into user activities, system configurations, and data access.
- Help detect and respond to security threats in real-time.
- Ensure system integrity by monitoring changes and configurations.
- Generate audit-ready reports to demonstrate compliance.

netwrix

Data classified

What is there, where

Trust Service Principles:

Confidentiality, Privacy

Why:

- Classify sensitive data to ensure it is properly handled and protected.
- Automate the discovery and classification of personal and confidential information.
- Help enforcing data privacy policies and compliance requirements.

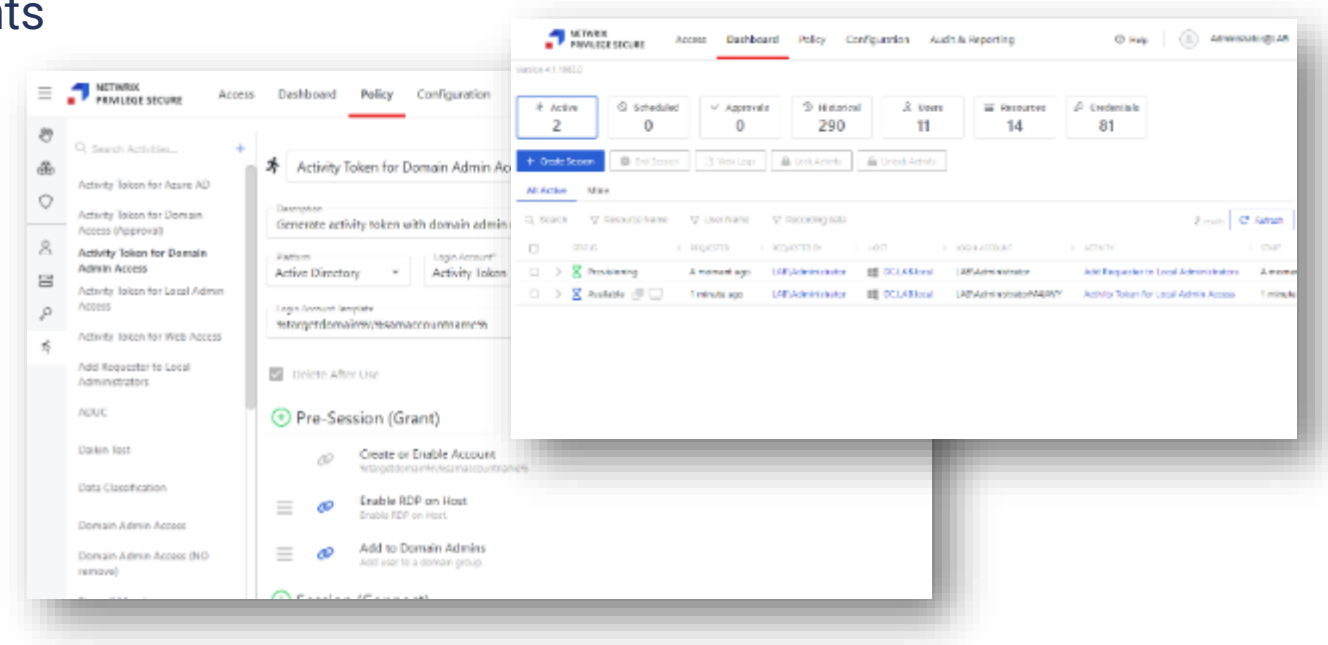
netwrix

Privileges Secured

Thwart cyberattacks by removing privileged accounts

Trust Service Principles:
Security, Confidentiality
Why:

- Manage and monitor privileged accounts and access.
- Provide just-in-time access and real-time monitoring of privileged activities.
- Reduce the risk of insider threats by controlling and auditing privileged access



Just-in-Time Orchestration

Create what you need to accomplish a specific task when you need it, and remove the attack surface when you're not using it.

Identity Orchestration

- Create / Remove Accounts
- Enable / Disable Accounts

Privilege Orchestration

- Add / Remove Permissions
- Enforce Group Membership

Endpoint Orchestration

- Enable/Disable RDP
- Purge Kerberos Tickets
- Pre/Post File Comparison
- Dynamic SMB Shares
- Custom PowerShell
- Dynamic sudoers

netwrix

Protect Endpoints

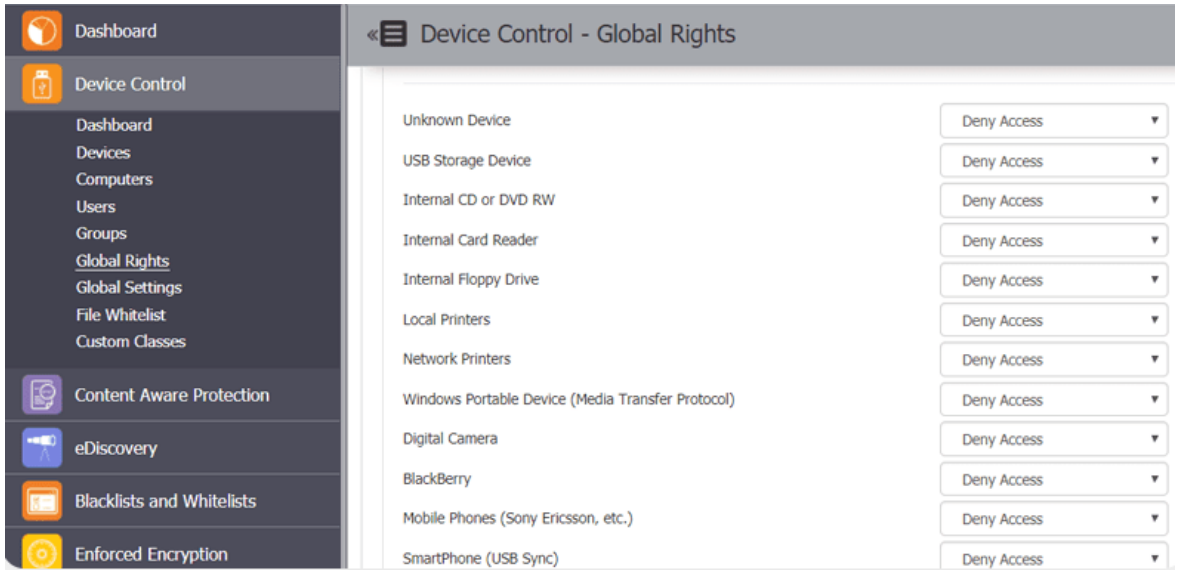
Data Loss Prevention

Trust Service Principles:

Security, Confidentiality, Privacy

Why:

- Prevent unauthorized access and exfiltration of sensitive data from endpoints.
- Monitor and control data transfers, detect and block data breaches, and provide real-time alerts.
- Classify sensitive data, enforce access control policies, encrypt data, and provide detailed compliance reports.



netwrix

Threats identified

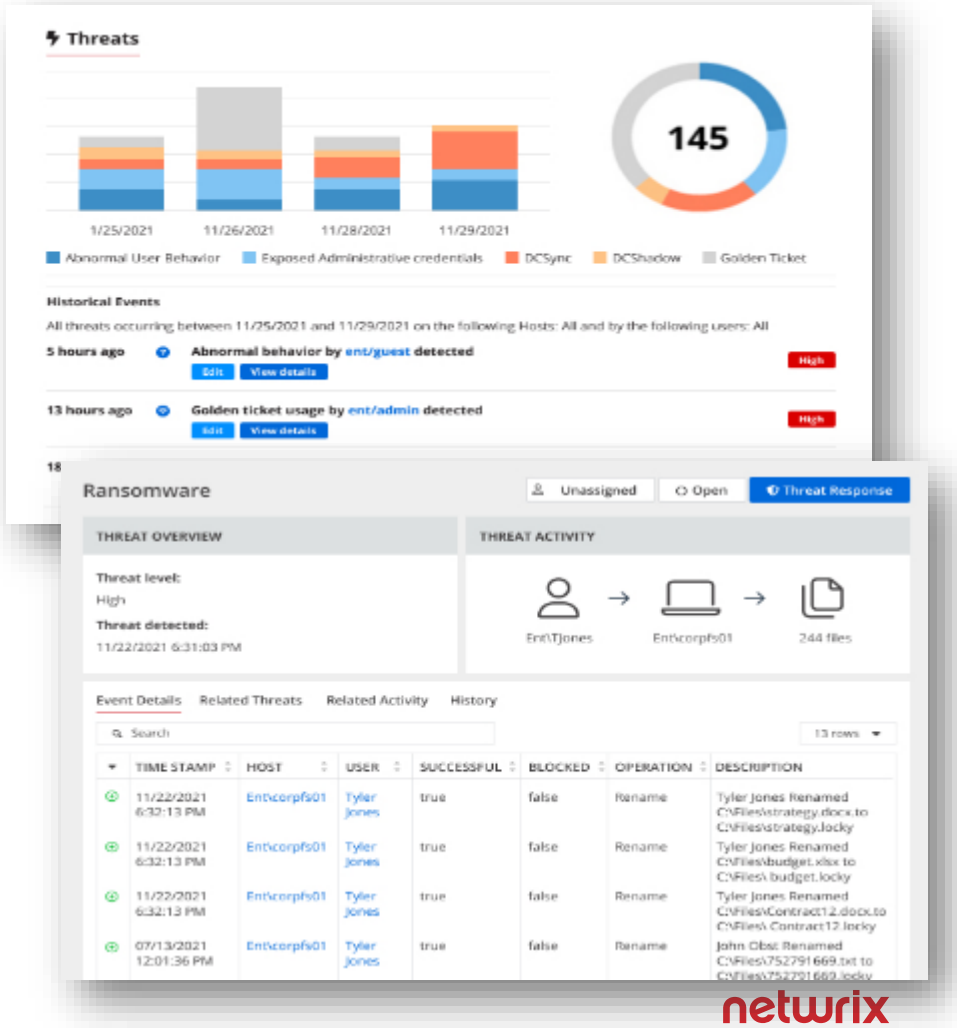
Threat Detection & Response

Trust Service Principles:

Security, Availability, Processing Integrity

Why:

- Provide real-time threat detection and response.
- (Use machine learning to detect abnormal behaviors and potential security incidents.)
- Automate responses to mitigate threats and maintain system integrity



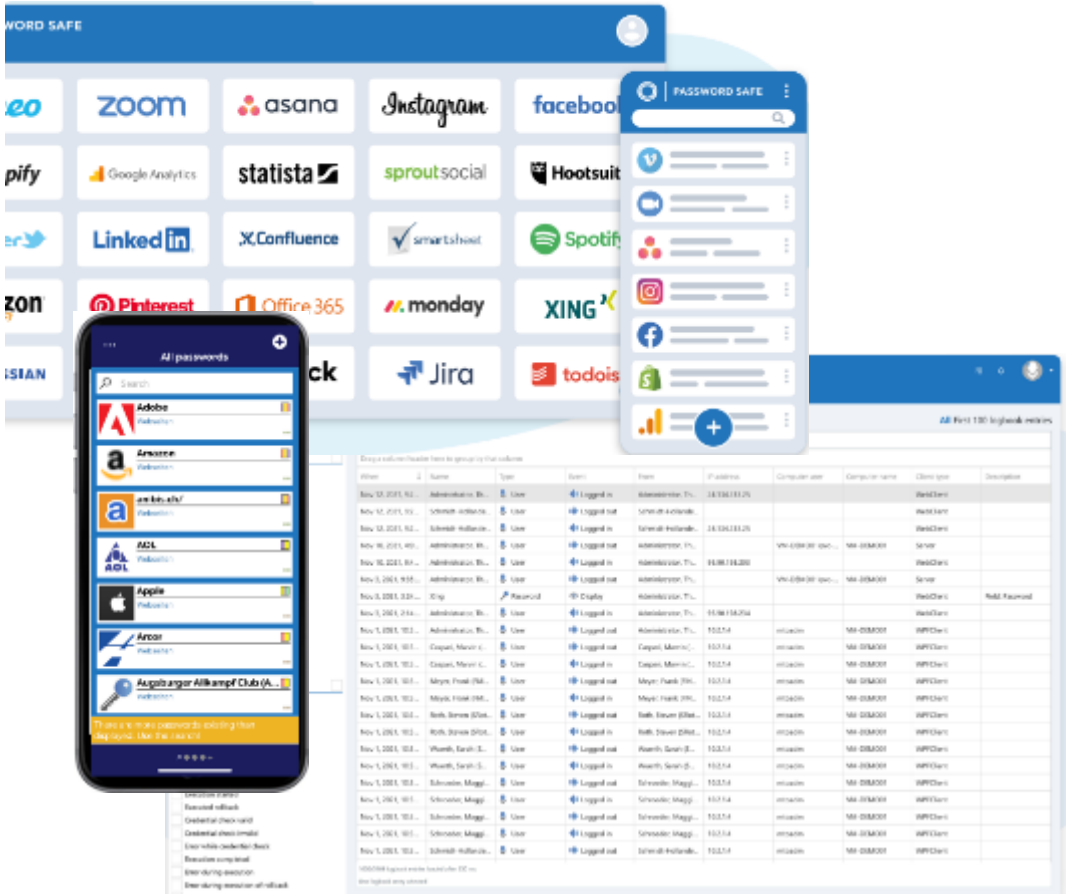
Passwords easy&secure

Protect sensitive credentials and be compliant

Trust Service Principles:
Security

Why:

- Ensure robust password policies and practices.
- Provide password management and self-service password reset to reduce security risks.
- Enhance access control mechanisms



netwrix

KÖSZÖNÖM A FIGYELMET!