## ISACA MÁSODIK SZERDAI ELŐADÁS

**Dirk Schrader** (CISM/CISSP) SOC2 Compliance – Challenging TSPs and how to get there

2024. szeptember 11.

Az ISACA Magyarországi Egyesület által szervezett Második Szerdai előadásokon bármilyen eszközzel történő kép- vagy hangrögzítés tilos. (Idetartozik a mobiltelefonokkal készített kép- vagy hangfelvétel is). A jelen szabály be nem tartása szerzői- és szomszédos jogi jogsértés jogkövetkezményeit vonhatja maga után.



Confidential. For internal use only.

# 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.





## SOC2 Compliance – Challenging TSPs and how to get there

**Dirk Schrader** VP of Security Research / Field CISO EMEA Netwrix



01SOC 2, Quick Facts02SOC 2, Who cares03SOC 2, The Five Trust Service Principles (TSPs)04Q&A05SOC 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

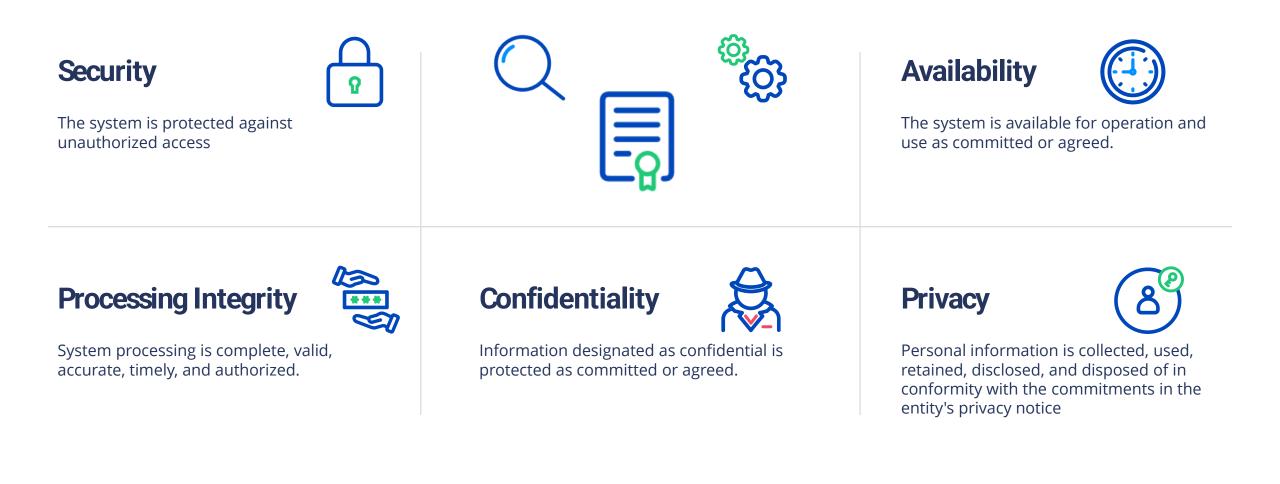
### Why is important?

- 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)**



## 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

#### **Enterprise Overview**



### **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 realtime.
- Ensure system integrity by monitoring changes and configurations.
- Generate audit-ready reports to demonstrate compliance.

### netwrix

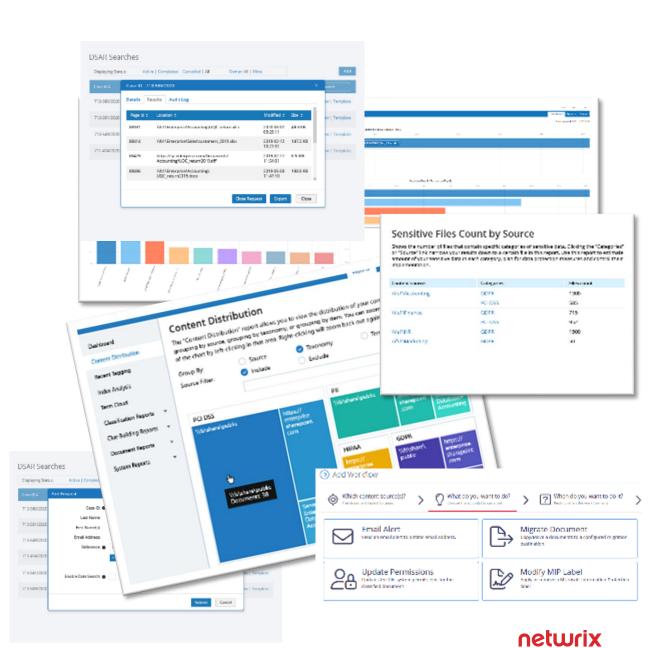
## **Data classified**

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.

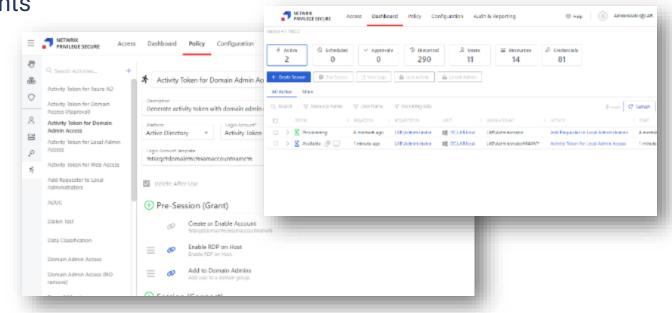


## **Privileges Secured**

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
- Purge Kerberos Tickets Pre/Post File Comparison

**Endpoint Orchestration** 

Dynamic SMB Shares

Enable/Disable RDP

- Custom PowerShell
- Dvnamic sudoers

#### $\neg$ CONFIDENTIAL

### neturix

## **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.

Dashboard	« Device Control - Global Rights	Rights					
Device Control							
Dashboard	Unknown Device	Deny Access 🔻					
Devices Computers	USB Storage Device	Deny Access 🔻					
Users	Internal CD or DVD RW	Deny Access					
Groups	Internal Card Reader	Deny Access 🔻					
<u>Global Rights</u> Global Settings	Internal Floppy Drive	Deny Access					
File Whitelist	Local Printers	Deny Access					
Custom Classes	Network Printers	Deny Access 🔻					
Content Aware Protection	Windows Portable Device (Media Transfer Protocol)	Deny Access					
eDiscovery	Digital Camera	Deny Access 💌					
	BlackBerry	Deny Access 🔻					
Blacklists and Whitelists	Mobile Phones (Sony Ericsson, etc.)	Deny Access 💌					
Enforced Encryption	SmartPhone (USB Sync)	Deny Access					

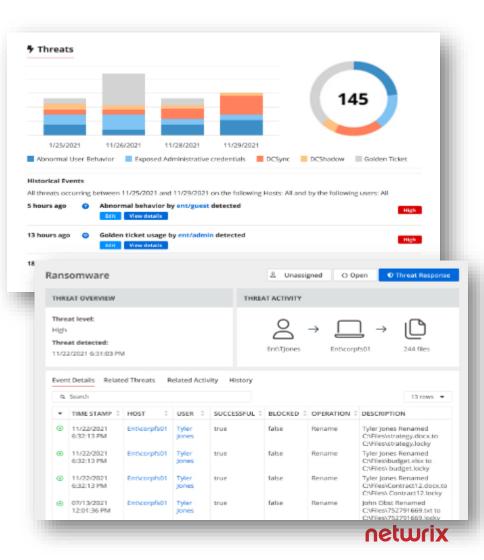
## **Threats identified**

**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

ORD SA	FE										
0	zoom	🔒 asana	Instagram	fo	cebool	0   1455	WORD SAFE	: Q			
fy	J Google Analytics	Google Analytics statista Sprout social		🗳 Hootsuit							
•	Linked in	,X,Confluence	e 🖌 smartsheet		tsheet Spotify		-	-			
n	() Pinterest	Coffice 365	//. monday	XING <sup>X</sup>							
A.N	Alipaiswo Diserch	⇒ ° ck	君 Jira		todois	<u>a</u> =	_				•••
	Adobe Fativelier	-			-	. <b>. </b> =(	Đ			All First	130 loghook entri
	a, Valueter		Deeper column fiscalize from the group ( ip the When I fame	1997	beri .	Fare	Paters	Computer aper	Computer name	Climityse.	Desciption
	ankisah/		htty 12, 2271, 62 . Automotion to Dr.	\$ Line	<ul> <li>Logged in</li> </ul>	Relation to The	343361025			Reidleri	
	a relation		Nov 12, 2011, 12. Schmitt-Addance.	& tar	Logged sub	Scheidt 4 oftender.				WebClarg	
		-	hov 10, 2211, 52. Adveste malance.		A Logged in	tarenit Hotanie.	14/06/01/25			ReiCeri	
	A AGL	-	NOV 16, 2019, 401. Administration, IR.,	& use	Logged out	administration, Thu		VN-00400-04	MI-DIMORT	58.987	
	AOL Visborist		Nov R. 221, 17. Adventures, Th.,		<ul> <li>Loganit in</li> </ul>	namesus, Tu-	1100.114.200			Reichers	
	Apple		Nov.3, 2023, 935 Administrator, Th.,		Coggod not	Administrator, Ph.		VM-084001040	MI-3(\$M001	Server	
	Trabaellen		No.3, 1913, 318	Present & User	@ Diale	Romerus, TL.	10.00104204			Relicien	Reld. Record
		-	Nov1,201,211. Administrative Bu- Nov1,191,721. Administrative Bu-	& there	<ul> <li>Logged is</li> </ul>	Administrator, Tr.	10254		Mi-BIMOOT	Willer	
	Aroan		Nov'l, 1917, 2017. Administration, Terr. New'l, 2017, 2017. Compari, Marcin C.	© Uner	<ul> <li>Loged od</li> <li>Loged od</li> </ul>	Administration, Thu- Energymi, Marcine) -	102.14	main	Mil-COMOOF	WORL	
	Tel: solar		Nov'L (2011, 1011, Conpart, Marvil C.	& tee	<ul> <li>Loged in</li> </ul>	Depen, Merrico,	10214	main	MI-DIMORT	Withert	
	Auguburger Alika	mellikh (k. 1	Nov C2011, 101. Cospan, Naryer C. Nav 1, 2011, 101. Mayer, Prost (Mr.	8 liter	<ul> <li>Logent or</li> </ul>	Maye: Park (8).	102.14	misale	Mar DEMODE	WEDer	
	Regionarger Hall	inpresto (v	Nov'LifeL W1. Mays read pt.		<ul> <li>Loged in</li> </ul>	Maye: Failt 201.	102.14	moeden	MI-DAUDT	Witten	
	/	-	hey 1,2021, 102	E Law	<ul> <li>Logged nat</li> </ul>	Tath, Sincer (Clat		misaim	Mil DIMON	Willeri	
	There are more paraverts exi- depleted. Use the second	o ding them	Nov'Libil Wil. Roth Streen Stot.		<ul> <li>Logent in</li> </ul>	Refs. Stover pilot.	102.54	mpedm	MA-DOMOGE	WEDers	
			his/1,2221,123. Wareh, East-12.	8 Uaw	<ul> <li>Logged cat</li> </ul>	Ramity Grant (E.,	102.14	missim	Mil CIERCOI	WOrld	
	****-		Nov 1, 2003, 105. Wanth, Sarah S.	& teer	di Logget in	Aventy Serah (5.)	102.54	mpedin	Mil-20M001	WEGert	
			No. 1, 2011, 10.1. Edwards, Maggi.	8 Une	1 Logard out	D/www.ite; Maggi	103.14	musim	Mil-DIMODI	WRDel	
	Decitor	17.8097	Nov'l, 2024, 101. Schooler, Maggi.	& tise	di tregget in	Schusseller; Mappi	102.14	miseón	MALERIADOR	WEDer	
	- Remarked	nilladi Adaptatid	No. 1.101. 101. Infection Maga-	8 Univ	The Logard and	Interester Maggi-	103.14	missim	MI-DIMON	WRDeri	
		i desi imalai	Nov'l, 2011, Will. Schronter, Maggi	& User	di tragest in	Sriveado: Mappi	102.14	misadin	MI-DOMOGE	WEDer	
		e-center fair dwark	Ny LIEL TJ., Sheat scheme.	S User	Lipperd and	tahendi Hollande.	10.0.1.4	miledm	MH-DIMON	INPICIALS	
	Invalue	e-cententiari directi normy intrall ng-away trian	Nov 1.2011.102. Scheede Hullerie. 1000000 Laport entite Institutes 12 m	8 tear	<ul> <li>Logged and</li> </ul>	tahendi Hollande.	10214	miseon	Mil-DIMOUT	MPDell	



## KÖSZÖNÖM A FIGYELMET!