5 Ways User Activity Data Improves Security and Compliance

Isaac Kimmel

Justin Sotelo

March 31, 2022

Agenda

- Introduction
- User Activity Data
- 5 Ways to Use It
- Summary and Q&A

Introduction

- **Name**: Isaac Kimmel
- **Role**: Senior Product Manager
- **Email**: ikimmel@securityweaver.com

- Began working with SAP in 2005 as part of a Basis and Security team for a big four consulting firm.
- Over the past decade, worked with many Security Weaver customers all over the world for implementation and training.
- Training class instructor

Introduction

Security Weaver has been in business for 17 years, started as an automated GRC Access Controls software, but has grown into many different offerings around SAP Security & Compliance.

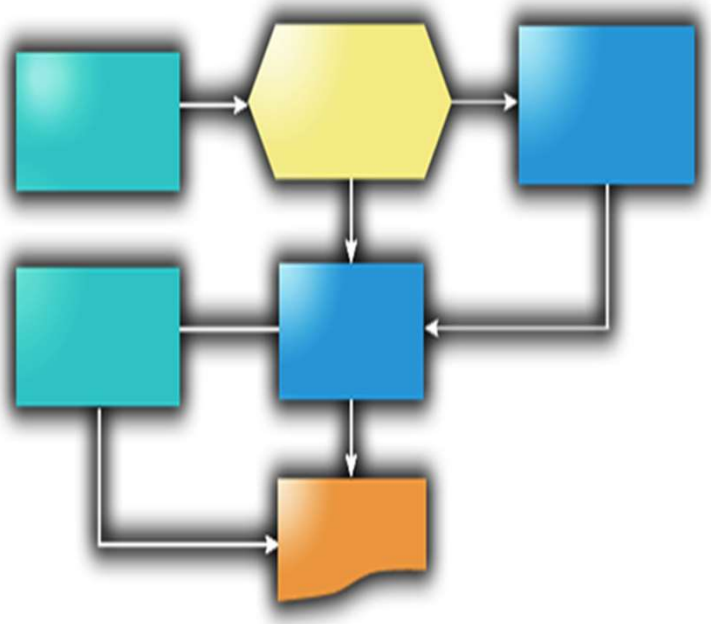
Today we are speaking on something that is relevant to every single organization. Retaining data, specifically SAP data, and analyzing it properly will help you to improve processes, security, employee production, and reduce costs.

Why Care about User Activity Data?

- Account breach identification
- Evidence of misconduct
- Vulnerability analysis and patching
- Irresponsible approvers
- Authorization creep identification
- Role design issues
- Policy flaws
- Provisioning/De-provisioning process issues
- User ID sharing
- Role testing
- Training and evaluation
- Roadmap planning
- Adoption assessments
- Role inventory management
- User risk scoring
- Access re-attestation support
- Backing out configuration errors
- Problem reproduction
- Data breach identification

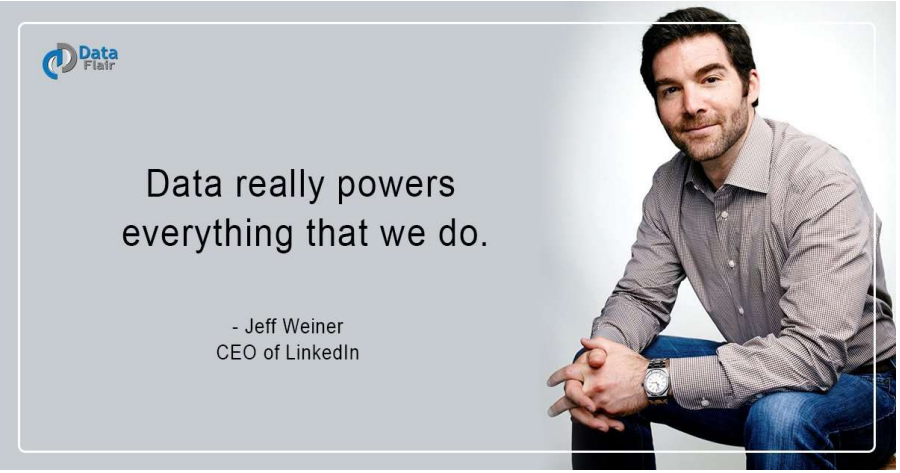
Five Example Use Cases

- Forensic processes
- Excessive access management
- Proper elevated access allocations
- Role recertification
- Segregation of Duties management
- Bonus: End user license allocations



…There are many more, but we don't have all day

Agenda



- Introduction
- User Activity Data
- 5 Ways to Use It
- Summary and Q&A

What Is User Activity Data?

- Historical information on what users are doing in your SAP system.
- This may include information such as the user, date, transaction accessed, and where they logged in from.
- For example, user Obula logged in from Desktop-56FJFFR on April 12, 2020 and ran transaction SE38 (ABAP Editor)

04/12/2020	23:41:56	800	OSEGGIREDDY	DESKTOP-56FJFFR	SE38	Transaction SE38 Started

Where to Find It?

- Standard SAP transactions and tables…You already have it!
- STAD, ST03N (Workload, select Server, Analysis Views – Transaction Profile), SM20 (Security Audit Log)
- Dependent on SAP configuration
- Unless persisted outside of the system, may be limited to summarized data and limited to only the last 45-90 days.
- Can be downloaded, but is not report or analysis friendly
- Over time, storage and incremental security required may become expensive.

How to Manage It?

- Offline
  - Bulky, incremental security, and periodic batch loads
  - Layered analytical tools
- Transaction Archive (TA) from Security Weaver
  - Compressed data, existing ERP security, and near-real time
  - Built in formatting, analytical, and reporting views

Forensics Investigation

- User activity data is critical for investigating an account breach. Without it, there is little to no visibility.
- Leverage any/all available data sources
- For example, if we suspect JDOE's account was compromised from April 1 to April 9 then ideally we'd have all JDOE related user activity available for this time period.
- Useful information includes: User, date, time, transactions used, terminal (PC) used, changes made by the user, audit log records

Forensics Investigation

- Manual approach: Create report in Excel by combining data from whatever sources are available.
- Streamlined approach: Run the *User History* report in Transaction Archive (TA)

User ID	User Full Name	Terminal	Data Type	Tcode or Service	Description
AHARTLEY	Andy Hartley	Lenovo-AH		SM37	Overview of job selection
				ST01	System Trace
				ST03N	Workload and Performance Statistics
				STAD	Statistics display for all systems
				SU01	User Maintenance
				SU01D	User Display
				SU20	Maintain Authorization Fields
				SU21	Maintain Authorization Objects

Forensics Investigation

User ID	Date	Terminal	Time	Tcod...	Report or	Function I	Function Text	Task Name	Change Typ	Table	Key
AHARTLEY	03/15/2020	Lenovo-AH	21:16:11	SU01	SAPMSUU0			Dialog			
		Lenovo-AH	22:20:13		SAPMSUU0						
		Lenovo-AH	22:34:13		SAPMSUU0						
		Lenovo-AH	22:59:54		SAPMSUU0		NetWeaver User Maintenance				
		Lenovo-AH	23:00:07		SAPMSUU0						
		Lenovo-AH	23:00:11		SAPMSUU0		Create				
		Lenovo-AH	23:00:38		SAPMSUU0		Change				
		Lenovo-AH	23:00:45		SAPMSUU0						
		Lenovo-AH	23:01:00		SAPMSUU0						
		Lenovo-AH	23:01:09		SAPMSUU0		Cancel				
		Lenovo-AH	23:01:19		SAPMSUU0						
		Lenovo-AH	23:01:24		SAPMSUU0		Choose				
		Lenovo-AH	23:01:30		SAPMSUU0		Save				
		NOT FOUND	23:01:31				Change Document	Database Change		ADCP	CLIENT=800,ADDRNUMBER
		NOT FOUND					Change Document			ADCP	CLIENT=800,ADDRNUMBER
		NOT FOUND					Change Document			ADCP	CLIENT=800,ADDRNUMBER
		NOT FOUND					Change Document			ADRP	CLIENT=800,PERSNUMBER=
		NOT FOUND					User Master Changes			USR02	AATEST1
		NOT FOUND					User Master Changes			USR02	AATEST1

- Result = Greatly improved visibility into any at risk activities!
- Keep in mind that if no plans are put in place until a breach occurs, then it is too late!

Excessive user access

- Common scenario: Roberto has worked at the company for 7 years and changed positions several times. He has 50 roles assigned in the production system.
- As Roberto changed positions, *authorization creep* has occurred. New roles were added, but old ones were not taken away.
- Current status – Roberto has a lot of excessive access that is neither appropriate nor useful. This causes many SOD conflicts (risks) and critical access violations.

Excessive user access

- ***If*** we have user activity data for Roberto, we can begin to understand what access is actually being used.
- Manual approach: Download available transaction usage data and compare to the user's assigned roles (role content). For example, transaction *ABC* was used which is part of role *XYZ*.
- Streamlined approach: Run *User's Unused Roles* report in TA

User ID	Long name	Company	Department	Interactions	Role	Role name	Last used	Used Days	Used Per.	Used Tcode	Total tcodes
MARY	DeGenius Mary	SWSD		0	/PSYNG/SW_ER_USER	SW: Emergency Repair User		0	0%	0	3
	DeGenius Mary	SWSD		0	SAP_ALL_HR_ONLY	All HR authorizations		0	0%	0	105
	DeGenius Mary	SWSD		0	SAP_FI_AR_BILL_OF_EXCHANGE	Process Bills of Exchange		0	0%	0	11
	DeGenius Mary	SWSD		0	SAP_FI_AR_CHANGE_LINE_ITEMS	Change Customer Line Items		0	0%	0	4
	DeGenius Mary	SWSD		0	SAP_FI_AR_CLEAR_OPEN_ITEMS	Clear Customer Line Items		0	0%	0	3
	DeGenius Mary	SWSD		0	Z.MAINT.CUSTOMER.MASTER.DEMO	Maintain Customer Master		0	0%	0	13
	DeGenius Mary	SWSD		0	Z.SALES.ORDER.DEMO	Sales Orders		0	0%	0	6
	DeGenius Mary	SWSD		0	Z_ALL_SOD_TCODES	Role with all SOD Tcodes		0	0%	0	113
	DeGenius Mary	SWSD		0	Z_SAP_FI_AR_CLEAR_OPEN_ITEMS	Clear Customer Line Items		0	0%	0	2

Excessive user access

User ID	Role	Role name	Interactions	Tcode	Transaction Text	Last used
MARY	Z.SALES.ORDER.DEMO	Sales Orders	0	PFCG	Role Maintenance	
			0	V.23	Release Orders for Billing	
			0	VA01	Create Sales Order	
			0	VA03	Display Sales Order	
			0	VA05	List of Sales Orders	
			0	ZVA01	ZVA01	

- With this information at our finger tips, we can remove the unused (excessive) access from the user. Removal can be done in an intelligent manner which should not impact the user's day to day activities.
- Result = user's excessive unused access is removed which **greatly reduces** the number of SOD conflicts (risks) and critical access violations in the system. User is prevented from performing activities that are no longer appropriate for his/her position.

Infrequently used access

- While reviewing excessive user access, we are likely to discover infrequently used access that is currently permanently assigned to the user (24x7).
- For example, Katie (Basis team) occasionally needs to run certain transactions from a support and troubleshooting perspective. She does not use this access every day.
- Grant (Finance team) performs some specific activities only at quarter end. He does not and should not use this access at other times.
- This causes many SOD conflicts (risks) and critical access violations.

Infrequently used access

- The goal is to identify the infrequently used access and move this access to your emergency access management process. For example, Security Weaver's Emergency Repair (ER) solution.
- Manual approach: Download available transaction usage data and compare to the user's assigned roles (role content). Pay particular attention to the usage dates.
- Streamlined approach: Run *User's Unused Roles* report in TA

User ID	Role	Role name	Last used	Used Days
CBATRA	/PSYNG/SW_DISPLAY	SW: Separations Enforcer Display	03/06/2020	4
KKUESTER	/PSYNG/LM_ADMINISTRATOR	LM: License Management Administrator	03/05/2020	5
DREINSMA	/PSYNG/SW_ER_USER	SW: Emergency Repair User	03/04/2020	1
DREINSMA	ZPSYNG_SW_ER_USER_FA	SW: Emergency Repair User - Allows Future Assignments		1
DITEST	/PSYNG/SW_ER_REVIEWER	SW: Emergency Repair Reviewer		1
DITEST	/PSYNG/SW_ER_USER	SW: Emergency Repair User		1
DITEST	ZPSYNG_SW_ER_USER_FA	SW: Emergency Repair User - Allows Future Assignments		1
AHARTLEY	/PSYNG/SW_ER_ADMINISTRATOR	SW: Emergency Repair Administrator	03/02/2020	2

Infrequently used access

- With this information, we can identify appropriate emergency access use cases.
- Once configured per your emergency access process and solution, the 24x7 access (role assignment to user) can be removed.
- Result = user's infrequently used access is removed which **reduces** the number of SOD conflicts (risks) and critical access violations in the system on a daily basis. When this access is **actually needed**, there is improved visibility and tracking.

Improve role recertification

- User activity data can help improve the role recertification (periodic access review) process.
- Most reviewers simply recertify (retain) all of the user's access (roles). They have limited information and assume the access is used.
- The activity data can be shown to the reviewer to help better inform him (or her). A more educated decision can be made.
- *Why recertify (retain) unused roles?*

Improve role recertification

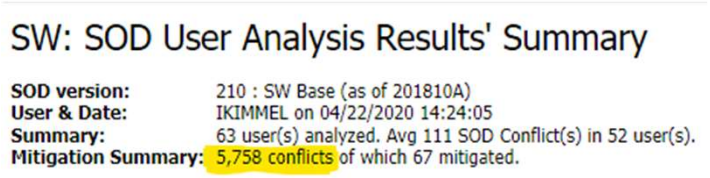
- Manual approach: Download available transaction usage data and compare to the user's assigned roles (role content). Summarize this information and add to your spreadsheet that contains the periodic user access review data.
- Streamlined approach: Utilize Security Weaver's Role Recertification (RR) solution which has a built in integration to TA.

AWILLIE	Z.SALES.ORDER	Sales Orders	DM1800	2016-03-22	9999-12-31	0
AWILLIE	Z_RR_MM_PROCURER	MM Procurer Role	DM1800	2020-03-26	9999-12-31	0
AWILLIE	Z_RR_PS_PROJECT_...	PS Project Manager Role	DM1800	2018-10-09	9999-12-31	0
DFOWLER	/PSYNG/RR_DISPLAY	Role Recertificaiton(TM) : [	DM1800	2016-08-12	9999-12-31	0
DFOWLER	Z.AP.PAYMENTS		DM1800	2014-04-28	9999-12-31	21

Improve role recertification

- Result = Reviewers are better informed. Even a small percentage increase in the number of roles removed during the periodic access review process will positively impact the number of SOD conflicts (risks) and critical access violations in the system.

Prioritize SOD Conflicts


SW: SOD User Analysis Results' Summary

SOD version: 210 : SW Base (as of 201810A)
User & Date: IKIMMEL on 04/22/2020 14:24:05
Summary: 63 user(s) analyzed. Avg 111 SOD Conflict(s) in 52 user(s).
Mitigation Summary: 5,758 conflicts of which 67 mitigated.

- When running an SOD conflict (risk) report on the user community, thousands of issues may be reported.
- *Where to start?* The results can be overwhelming and there is not time to investigate each and every conflict.
- Recommendation is to prioritize high importance conflicts where the conflicting transactions were used by the same user. Known as *executed conflicts*.
- User activity data is needed to provide this insight.

Prioritize SOD Conflicts

- Manual approach: Download available transaction usage data and compare to the user's SOD Conflicts. Look at the conflicting transactions within the SOD conflict. For example, has Mary used transactions FB01 (Post Document) and ME21 (Create PO)? This would fall under the conflict AP PO Invoice and PO Entry.
- Streamlined approach: Utilize Security Weaver's Separations Enforcer (SE) solution which has a built in integration to TA with the *SOD Live* feature. Even when using a different SOD tool, you can utilize the TA reports to speed up the comparison process.

User ID	User Name	Sensitivity	Con ID	SW: Risk Description	Mitigation	Auditor	Valid From	To date	Type	TCD Exe
KREESE	Kyle Reese	LOW	P045	Purchase Order Entry & Vendor Master Maintenance						☑
SCHAUBEY	Oliver Jacobs	HIGH	S028	Sales Order Processing & Clear Customer Balance						☐
		MEDIUM	P041	AP Release PO Invoice & Goods Receipt to PO						☑
			P054	AP PO Invoice & Purchase Order Entry						☑
			S008	AR Cash Application (Payments) & Sales Order Processing						☑
		LOW	P045	Purchase Order Entry & Vendor Master Maintenance						☑

Prioritize SOD Conflicts

- By focusing on important executed conflicts, a company's limited time & resources can focus on SOD conflicts of **actual** importance.
- Result = Time spent more wisely! The higher priority conflicts will be the first to be remediated (cleaned up).

Bonus: Optimize SAP license allocation

- Due to the complexity and vagaries of license types, they are often assigned to users with little rhyme or reason.
- Unfortunately, this is not only inefficient but costly. There is often a large cost difference between license types. For example, a Limited Professional compared to Professional.
- User activity data can help appropriately optimize license allocation in a consistent manner.
- Why pay for an expensive license for a user that does very little in your system?

User License Type	License Type Desc.	Licensed #	Licensed Amount	# Over	Amount Over
01	Operational	50	300,000.00	24	144,000.00
63	SAP NetWeaver Developer	20	140,000.00	0	0.00
64	SAP NetWeaver Professional	10	50,000.00	0	0.00

Optimize SAP License allocation

- Security Weaver's License Management (LM) solution allows you to define license **rules** for users. LM can then automatically apply these rules and update the user license types.
- Result = Licenses consistently allocated, saving time and money!

Sort Order	Rule definition	App	Inst	Instance d	License Ty	License description
10	Has developer key				63	SAP NetWeaver Developer
20	500 Interactions done in last 60 days				64	SAP NetWeaver Professional
30	Used TCode FB01 in last 90 days				64	SAP NetWeaver Professional
40	User group EAST				65	SAP NetWeaver User
50	Used TCode ME28 in last 30 days				64	SAP NetWeaver Professional

Summary and Q&A

- User Activity Data can be used to support a variety of security and compliance processes.
- The data is already available, but how it is managed can be a challenge.
- If a forensic requirement is raised, it's too late to start collecting data, and data not retained is as useless as data not collected.
- User data can help streamline role assignment, role retention, and role recertification decisions.
- Segregation of Duties management processes can be more efficient and mitigations better prioritized.

Announcements

- Contact us to schedule a free demo for any Security Weaver products.
- Join our LinkedIn SWUG group!