

IDS for SAP

Application Based IDS Reporting
in the ERP system SAP R/3

Research Question

How is the performance of this SAP IDS when running with reduction of false positives and anonymization?

Hypothesis

It is possible to make an application based IDS for SAP and increase performance with false positive reduction in anonymized mode.

Goals

- Simplicity
- Automate security monitoring for SLA meetings and Security Audits.
- Effective and Proactive processing of Security Audit Log
- Improve organizational security awareness

SAP R/3 facts

- ERP system (Enterprise Resource Planning)
- Integrated database containing all data and processes for the organization.
- Realtime
- 3-tier (database, application, client)
- Extensive and complicated authorization system.
- Role based access control, (RBAC).

IDS

- Intrusion Detection System: Software that automates the intrusion detection process.
- IDPS – intrusion detection and prevention system
- Purpose [NIST SP800-94]
 - monitoring “...events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices.”
- IDS challenge: False positives and true negatives.
- Optimize false positive reduction, (FPR) without generating true negatives.

Why an Internal IDS for SAP?

- Use for SLA Meetings and Security Audits
- Monitoring and investigating security audit logs for internal security incidents and misuse is time consuming and dull
- Output from IDS will produce more findings.

Performance Considerations

- Why Anonymization?
 - Some information in the reports are internal
- What is Good IDS Performance?
 - Comprehensive
 - Timely
 - Comprehensible
 - Accuracy

Ethical Dilemma

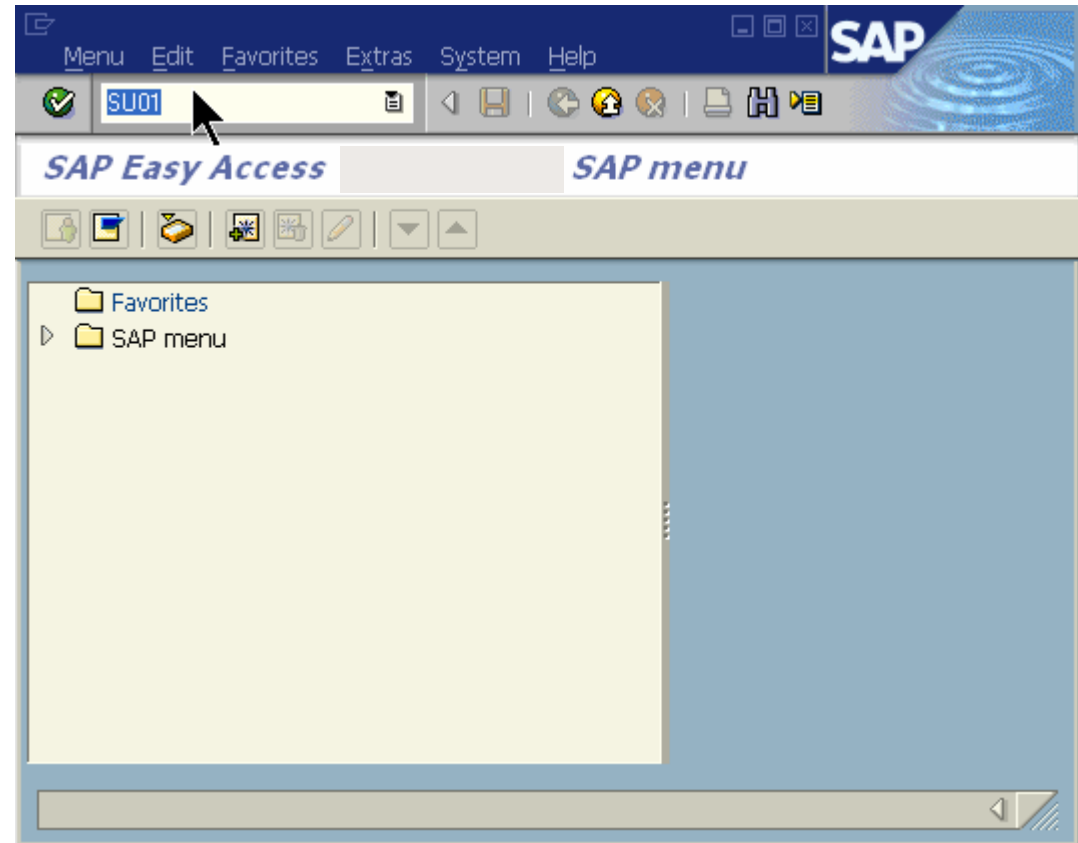
- Security personnel responsible for reporting signs of misuse and abnormal activity
- No time is allocated to work in this area by the employer
- Outsourced IS operations personnel instructed **not** to report problem areas unless service agreement for this type of work is in place

Building Blocks for IDS

- Security Audit Logging
- ABAP programs
- Access Roles
- Authorization User Groups
- SOD Matrix, Virsa Compliance Calibrator
- Customized tables
- SAP standard tables

Transaction codes

- Tcodes for short
- Typically a four letter alpha-numeric code.
- Executes a program or script when entered.



Security Audit Logging


- Stored at OS level (UNIX)
- One file for each 24 hour period on each application server
- Text based file with delimiter for linefeed
- Collect log files for specified time period and populate customized table.

Security Audit Logging


<u>Dialog logon</u>	Non-crit.	<input type="checkbox"/>	User Logoff
	Important	<input checked="" type="checkbox"/>	Logon Successful (Type=&A)
	Important	<input checked="" type="checkbox"/>	Logon Failed (Reason = &B, Type = &A)
	Critical	<input checked="" type="checkbox"/>	Logon Failed (Reason = &B, Type = &A)
	Critical	<input checked="" type="checkbox"/>	User Locked After Incorrect Logon
	Critical	<input checked="" type="checkbox"/>	User lock because of incorrect logon removed
<u>RFC/CPIC logon</u>	Non-crit.	<input type="checkbox"/>	RFC/CPIC Logon Successful (Type = &A)
	Critical	<input checked="" type="checkbox"/>	RFC/CPIC Logon Failed, Reason = &B, Type =
<u>RFC function call</u>	Non-crit.	<input type="checkbox"/>	Successful RFC Call &C (Function Group = &A)
	Critical	<input checked="" type="checkbox"/>	Failed RFC Call &C (Function Group = &A)
<u>Transaction start</u>	Non-crit.	<input type="checkbox"/>	Transaction &A Started
	Important	<input checked="" type="checkbox"/>	Transaction &A Locked
	Important	<input checked="" type="checkbox"/>	Transaction &A Unlocked
	Critical	<input checked="" type="checkbox"/>	Start Transaction &A Failed
<u>Report start</u>	Non-crit.	<input type="checkbox"/>	Report &A Started
	Important	<input type="checkbox"/>	Start Report &A Failed (Reason = &B)
<u>User master change</u>	Important	<input checked="" type="checkbox"/>	User &A Deleted
	Important	<input checked="" type="checkbox"/>	User &A Locked
	Important	<input checked="" type="checkbox"/>	User &A Unlocked
	Important	<input checked="" type="checkbox"/>	Authorizations for User &A Changed
	Important	<input checked="" type="checkbox"/>	Authorization/authorization profile &B Created
	Important	<input checked="" type="checkbox"/>	Authorization/authorization profile &B Deleted
	Important	<input checked="" type="checkbox"/>	Authorization/authorization profile &B Changed
	Critical	<input checked="" type="checkbox"/>	User &A Created
	Critical	<input checked="" type="checkbox"/>	Authorization/authorization profile &B Activated
<u>Other events</u>	Important	<input checked="" type="checkbox"/>	Download &A Bytes to File &C
	Important	<input checked="" type="checkbox"/>	Digital Signature (Reason = &A, ID = &B)
	Critical	<input checked="" type="checkbox"/>	Audit: Slot &A: Class &B, Weight &C, User &D,
	Critical	<input checked="" type="checkbox"/>	Application Server Started
	Critical	<input checked="" type="checkbox"/>	Application Server Stopped
	Critical	<input checked="" type="checkbox"/>	Digital Signature Error (Reason = &A, ID = &B)

Log Collector







Selection of Audit Events from the Audit Files to table ZSALOG



Time restrictions

From date/time	05.09.2007	13:00:00
To date/time	05.09.2007	<input type="text"/> 

Standard selections

Instance name	<input type="text"/>	
Client	<input type="text"/>	
User	<input type="text"/>	
Terminal	<input type="text"/>	
Transaction code	<input type="text"/>	
Program	<input type="text"/>	
Text in the message	<input type="text"/>	

Events

Critical only


Severe and critical

All

Options

Display ALV report

Update Table ZSALOG



Empty Table ZSALOG

Misuse Detection

- Update of own access
 - Incidents where user has changed his own authorizations
- Segregation of Duties, SOD risks
 - Potential for fraudulent gain and misappropriation of funds.
- Dualism
 - Incidents in which a user is running transactions classified as IS operations and business postings.

FPR in Misuse Detection

- Update of own access
 - Actual update of authorization profiles
- Segregation of Duties, SOD risks
 - Illicit use or attempts, i.e. no approval.
- Dualism
 - Exclude privileged users.

Anomaly Detection


- Login Failures
 - Incorrect user name, password, or validity period
- Authorization Failures
 - Attempts to perform unauthorized postings and operations.
- Download Activity
 - Downloading information from system and storing in PC format

FPR in Anomaly Detection

- Login Failures
 - Exclude non-existing user IDs (typos)
- Authorization Failures
 - Exclude non-existing tcodes (typos)
- Download Activity
 - Check enterprisers only

Detection Engine

IDS Report



Misuse Detection

	FPR (False Positive Reduction)	Anonymization
1. <input type="checkbox"/> Update of own access	<input type="checkbox"/> Actual Changes, (Table USH04)	<input type="checkbox"/>
2. <input type="checkbox"/> SOD risks	<input type="checkbox"/> Exclude Privileged/SOD Users	<input type="checkbox"/>
3. <input checked="" type="checkbox"/> Dualism (IS/postings)	<input type="checkbox"/> Exclude Privileged Users	<input type="checkbox"/>

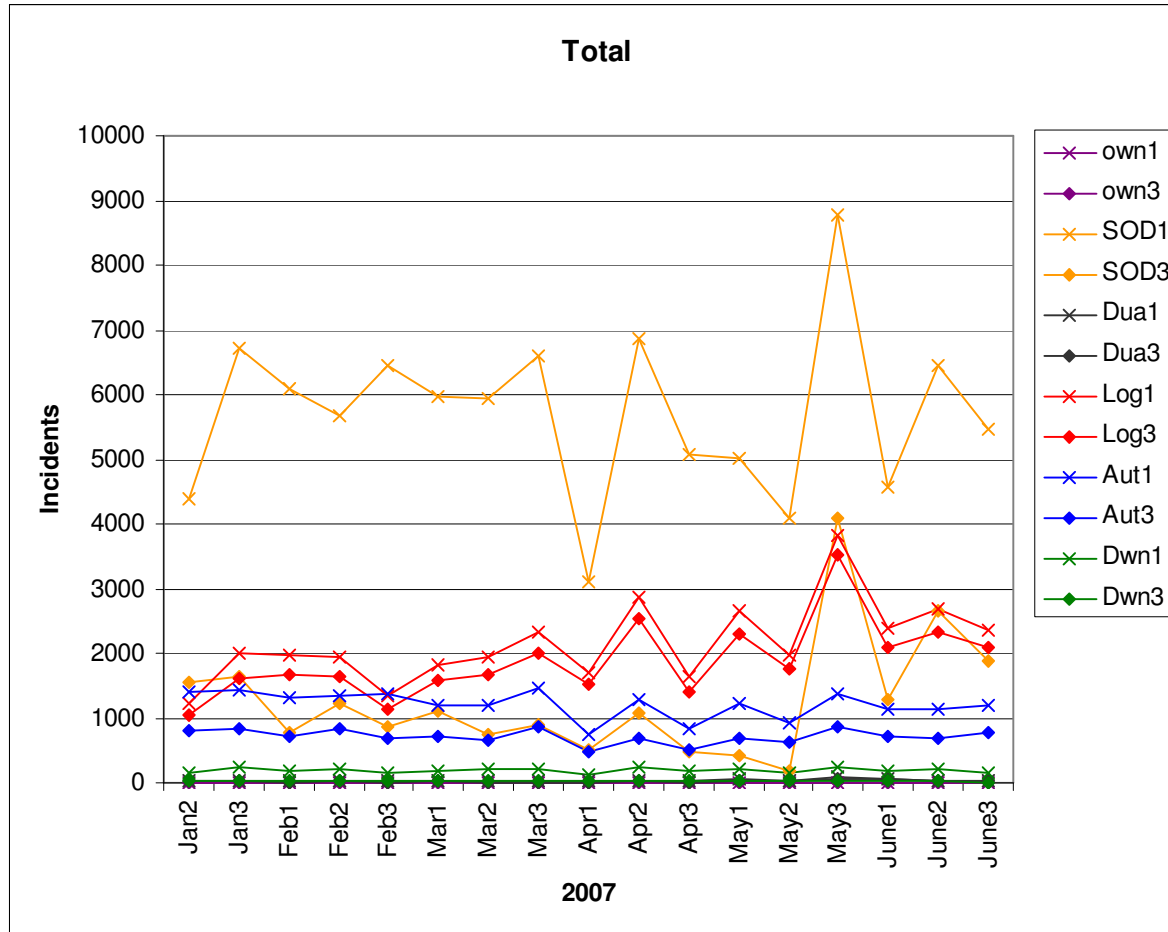
Anomaly Detection

	FPR (False Positive Reduction)	Anonymization
1. <input type="checkbox"/> Failed Logons	<input type="checkbox"/> Valid User IDs only	<input type="checkbox"/>
2. <input type="checkbox"/> Authorization Failures	<input type="checkbox"/> Valid Transactions only	<input type="checkbox"/>
3. <input type="checkbox"/> Excessive Downloads	<input type="checkbox"/> Check Z-users only	<input type="checkbox"/>

Log files

Microsoft Excel - M2 20070511-20 SODFPR&ANON - random example												
File Edit View Insert Format Tools Data Window Live Meeting Help												
	A	B	C	D	E	F	G	H	I	J	K	L
1	12.09.2007								Dynamic List Display			
2												
3	Sod Risk in period	, total :	175									
4	Sod Risk in period	, per user :	13									
5												
6												
7	Report type	User name	Trans.	At	Program	Cate	Me	Terminal	Descriptive text for Securit	Application serv	Date	Time
8												
9	SOD risk- 2 trans c	KSA6SEA	CAPP	3				D0	1 06SJAN\2HK0YKT2CP0 TK33 Y2K	bgo021ilp_P01	14.05.2007	16:17:22
10	SOD risk- 2 trans c	KSA6SEA	CAT2	3	SAPLSMT	D1		D0	1 06SJAN\2HK0YKT2CP0 TK2J Y2K	bgo021ilp_P01	14.05.2007	16:03:40
11	SOD risk- 2 trans c	KSA6SEA	CAPP	W	CATSSHCD			D0	1 06SJAN\HW3PH2 TK2YYLPV Y2KH	bgo021ilp_P01	14.05.2007	16:17:22
12	SOD risk- 2 trans c	KSA6SEA	CAT2	3	SAPLSMT	D1		D0	1 06SJAN\2HK0YKT2CP0 TK2J Y2K	bgo021ilp_P01	14.05.2007	16:03:40
13	SOD risk- 2 trans c	KSA6SEA	CAPP	3				D0	1 06SJAN\2HK0YKT2CP0 TK33 Y2K	bgo075ilp_P01	18.05.2007	12:17:37
14	SOD risk- 2 trans c	KSA6SEA	CAT2	3	SAPLSMT	D1		D0	1 06SJAN\2HK0YKT2CP0 TK2J Y2K	bgo021ilp_P01	14.05.2007	16:03:40
15	SOD risk- 2 trans c	KSA6SEA	CAPP	W	CATSSHCD			D0	1 06SJAN\HW3PH2 TK2YYLPV Y2KH	bgo075ilp_P01	18.05.2007	12:17:38
16	SOD risk- 2 trans c	KSA6SEA	CAT2	3	SAPLSMT	D1		D0	1 06SJAN\2HK0YKT2CP0 TK2J Y2K	bgo021ilp_P01	14.05.2007	16:03:40
17	SOD risk- 2 trans c	KSA6NXU	FB01	3	SAPMSY	D1		D0	1 06SSQE\2HK0YKT2CP0 57AS Y2K	bgo075ilp_P01	14.05.2007	15:21:59
18	SOD risk- 2 trans c	KSA6NXU	F-04	3				D0	1 06SSQE\2HK0YKT2CP0 5-A0 Y2K	bgo075ilp_P01	14.05.2007	12:09:48
19	SOD risk- 2 trans c	KSA6NXU	FB01	3	SAPMSY	D0		D0	1 06SSQE\2HK0YKT2CP0 57AS Y2K	bgo075ilp_P01	14.05.2007	15:22:29
20	SOD risk- 2 trans c	KSA6NXU	F-04	3				D0	1 06SSQE\2HK0YKT2CP0 5-A0 Y2K	bgo075ilp_P01	14.05.2007	12:09:48
21	SOD risk- 2 trans c	KSA6NXU	FB01	3	SAPMSY	D3		D0	1 06SSQE\2HK0YKT2CP0 57AS Y2K	bgo021ilp_P01	18.05.2007	08:56:26
22	SOD risk- 2 trans c	KSA6NXU	F-04	3				D0	1 06SSQE\2HK0YKT2CP0 5-A0 Y2K	bgo075ilp_P01	14.05.2007	12:09:48
23	SOD risk- 2 trans c	KSA6NXU	FB01	3	SAPMSY	D4		D0	1 06SSQE\2HK0YKT2CP0 57AS Y2K	bgo021ilp_P01	18.05.2007	09:20:13
24	SOD risk- 2 trans c	KSA6NXU	F-04	3				D0	1 06SSQE\2HK0YKT2CP0 5-A0 Y2K	bgo075ilp_P01	14.05.2007	12:09:48
25	SOD risk- 2 trans c	KSA6NXU	FB01	3	SAPMSY	D4		D0	1 06SSQE\2HK0YKT2CP0 57AS Y2K	bgo021ilp_P01	16.05.2007	07:49:47
26	SOD risk- 2 trans c	KSA6NXU	F-04	3				D0	1 06SSQE\2HK0YKT2CP0 5-A0 Y2K	bgo075ilp_P01	14.05.2007	12:09:48
27	SOD risk- 2 trans c	KSA6NXU	FB01	3	SAPMSY	D1		D0	1 06SSQE\2HK0YKT2CP0 57AS Y2K	bgo075ilp_P01	14.05.2007	07:50:24
28	SOD risk- 2 trans c	KSA6NXU	F-04	3				D0	1 06SSQE\2HK0YKT2CP0 5-A0 Y2K	bgo075ilp_P01	14.05.2007	12:09:48
29	SOD risk- 2 trans c	KSA6NXU	FB01	3	SAPMSY	D1		D0	1 06SSQE\2HK0YKT2CP0 57AS Y2K	bgo075ilp_P01	14.05.2007	07:50:23
30	SOD risk- 2 trans c	KSA6NXU	F-04	3				D0	1 06SSQE\2HK0YKT2CP0 5-A0 Y2K	bgo075ilp_P01	14.05.2007	12:09:48
31	SOD risk- 2 trans c	KSA6NXU	FB01	3	SAPMSY	D1		D0	1 06SSQE\2HK0YKT2CP0 57AS Y2K	bgo075ilp_P01	14.05.2007	07:50:22
32	SOD risk- 2 trans c	KSA6NXU	F-04	3				D0	1 06SSQE\2HK0YKT2CP0 5-A0 Y2K	bgo075ilp_P01	14.05.2007	12:09:48
33	SOD risk- 2 trans c	KSA6NXU	FB01	3	SAPMSY	D1		D0	1 06SSQE\2HK0YKT2CP0 57AS Y2K	bgo075ilp_P01	14.05.2007	07:50:27
34	SOD risk- 2 trans c	KSA6NXU	F-04	3				D0	1 06SSQE\2HK0YKT2CP0 5-A0 Y2K	bgo075ilp_P01	14.05.2007	12:09:48
35	SOD risk- 2 trans c	KSA6NXU	FB01	3	SAPMSY	D3		D0	1 06SSQE\2HK0YKT2CP0 57AS Y2K	bgo075ilp_P01	14.05.2007	15:23:00
36	SOD risk- 2 trans c	KSA6NXU	F-04	3				D0	1 06SSQE\2HK0YKT2CP0 5-A0 Y2K	bgo075ilp_P01	14.05.2007	12:09:48
37	SOD risk- 2 trans c	KSA6NXU	FB01	3	SAPMSY	D1		D0	1 06SSQE\2HK0YKT2CP0 57AS Y2K	bgo021ilp_P01	18.05.2007	08:05:14

Incidents



Misuse Conclusions, FPR

- Misuse of privileges to gain additional authorizations
 - Good performance, actual changes only
- Misuse with SOD risks
 - Effective with corrective actions
- Misuse with Dualism
 - Effective with corrective actions

Anomaly Conclusion, FPR

- Login failures
 - Some performance improvement, but what about brute force attacks?
- Authorization failures
 - Some performance improvement, but what about 'menu cruisers'?
- Download activity
 - Performance improvement! –but, should account for quantity of downloads

Conclusions, Anonymization

- One to one correlation between FPR only mode and FPR anonymized mode.
- Anonymization does not affect other performance characteristics than comprehensibility.

Experiences & Suggestions

- Consider more than one FPR for each IDS characteristic
- Introduce thresholds
- Incorporate white lists and black lists
- Incorporate alert facilities?
- Check total number of downloads not just number of users, as for the SOD analysis