IBM Security

A Day in the Life: When “Tip of the Iceberg” is Not a Cliché

Bern Lord
Cybersecurity Specialist
IBM Z Security
balord@us.ibm.com

July 2020

Mike Rich
Cybersecurity Specialist
IBM Z Security
mike.rich@ibm.com

IBM Security / © 2020 IBM Corporation

IBM Security Community

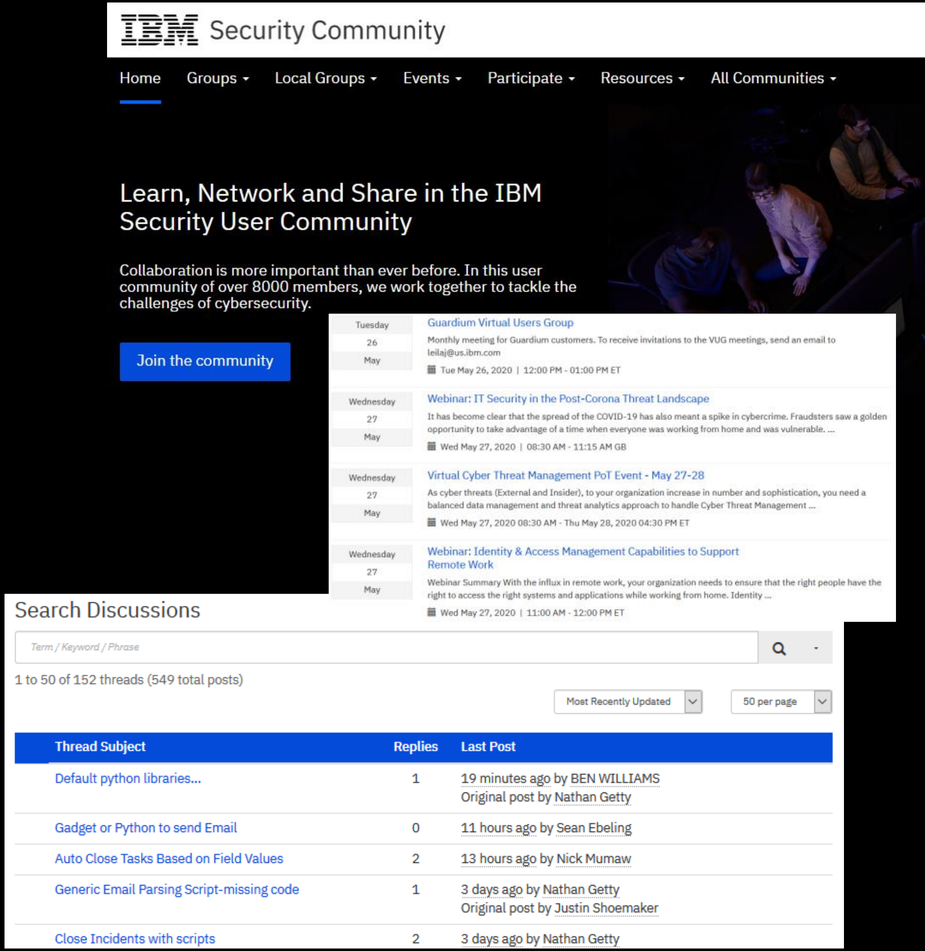
8,000 Members Strong and Growing Every Day!

Sign up: https://community.ibm.com/security

Learn: The indispensable site where users come together to discover the latest product resources and insights — straight from the IBM experts.

Network: Connecting new IBM clients, veteran product users and the broader security audience through engagement and education.

Share: Giving YOU a platform to discuss shared challenges and solve business problems together.



Learn, Network and Share in the IBM Security User Community

Collaboration is more important than ever before. In this user community of over 8000 members, we work together to tackle the challenges of cybersecurity.

Tuesday 26 May — **Guardium Virtual Users Group**
Monthly meeting for Guardium customers. To receive invitations to the VUG meetings, send an email to leilaj@us.ibm.com
Tue May 26, 2020 | 12:00 PM - 01:00 PM ET

Wednesday 27 May — **Webinar: IT Security in the Post-Corona Threat Landscape**
It has become clear that the spread of the COVID-19 has also meant a spike in cybercrime. Fraudsters saw a golden opportunity to take advantage of a time when everyone was working from home and was vulnerable. ...
Wed May 27, 2020 | 08:30 AM - 11:15 AM GB

Wednesday 27 May — **Virtual Cyber Threat Management PoT Event - May 27-28**
As cyber threats (External and Insider), to your organization increase in number and sophistication, you need a balanced data management and threat analytics approach to handle Cyber Threat Management ...
Wed May 27, 2020 08:30 AM - Thu May 28, 2020 04:30 PM ET

Wednesday 27 May — **Webinar: Identity & Access Management Capabilities to Support Remote Work**
Webinar Summary With the influx in remote work, your organization needs to ensure that the right people have the right to access the right systems and applications while working from home. Identity ...
Wed May 27, 2020 | 11:00 AM - 12:00 PM ET

Search Discussions

Term / Keyword / Phrase

1 to 50 of 152 threads (549 total posts)

Most Recently Updated | 50 per page

Thread Subject	Replies	Last Post
Default python libraries...	1	19 minutes ago by BEN WILLIAMS Original post by Nathan Getty
Gadget or Python to send Email	0	11 hours ago by Sean Ebeling
Auto Close Tasks Based on Field Values	2	13 hours ago by Nick Mumaw
Generic Email Parsing Script-missing code	1	3 days ago by Nathan Getty Original post by Justin Shoemaker
Close Incidents with scripts	2	3 days ago by Nathan Getty

Agenda

- ❖ Company Description & Cast of Characters
- ❖ Day in the life story of a data breach
- ❖ How could this have had a different outcome?
- ❖ What are the ways this may have been prevented?
- ❖ Q & A

Bushwood Financial Group

Company Background

- 5,000 employees
- 100,000 customers
- Financial Services Company specializing in Wealth Management

Enterprise Data

- Mission Critical applications running on Z
- Transaction processing, teller applications, trading platform
- Human Resources including payroll

Security Tools (CISO is proud of their 'State of the Art Security')

- SIEM – QRadar
- RACF Administration, audit, and compliance – zSecure Suite
- Guardium for Db2 on LUW, felt MF safe so no need to monitor Db2 z/OS

Jane Thomas

- SOC Team Security Analyst
- Minimal mainframe experience

Bill Lord

ID = LORD1

- Db2 LUW and Z DBA

Sam Thomas

- Guardium Admin
- No Db2 for Z knowledge

QRadar terminology pertaining to Mainframe data

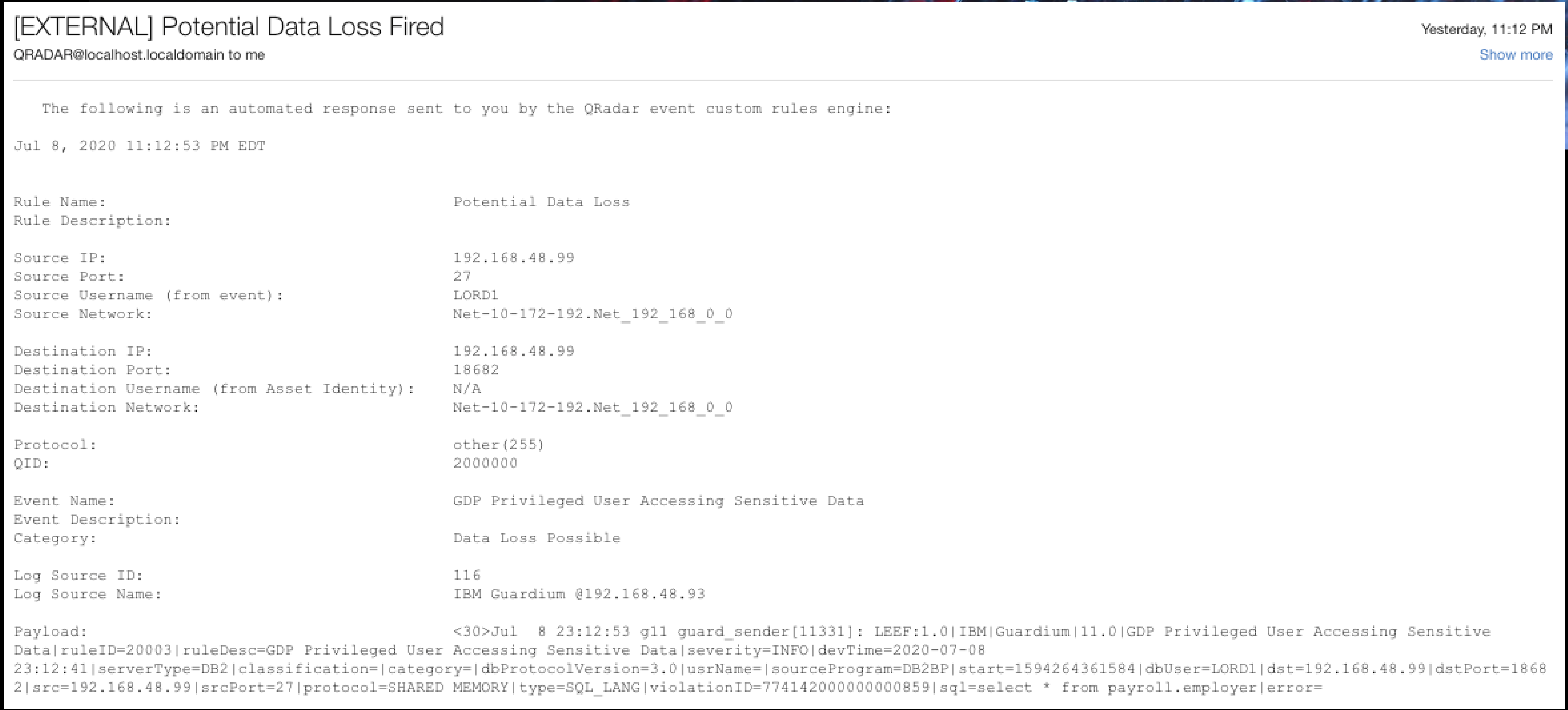
Alerts – Guardium Alert

Events – QRadar streaming events from log sources (Guardium, zSecure Alert, SMF Events, etc)

Rules – Rules are set in QRadar to take action based on the number, type, or time of day an event is received

Offenses – QRadar rules trigger an offense in QRadar

Chapter 1: SOC Team Detects Possible Data Breach – Jane Receives Email



[EXTERNAL] Potential Data Loss Fired

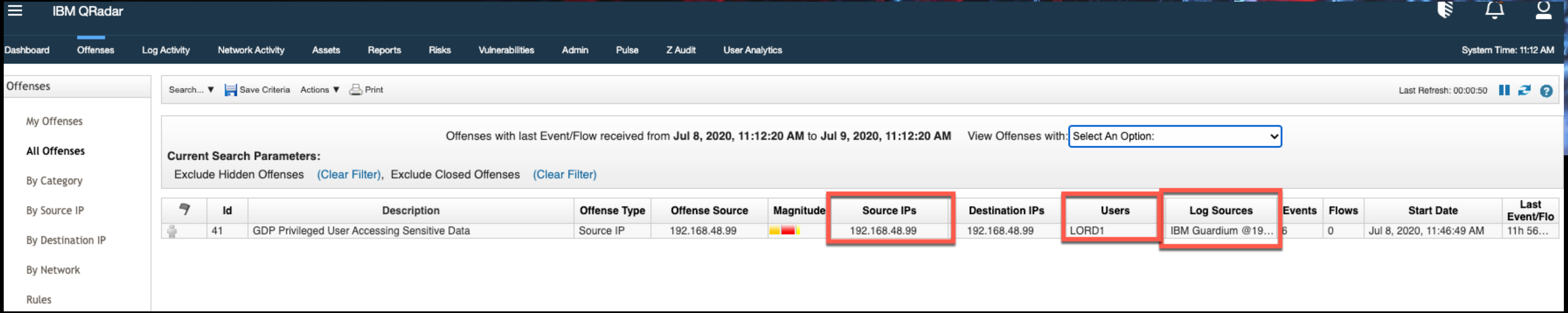
QRADAR@localhost.localdomain to me

Yesterday, 11:12 PM

Show more

```
   The following is an automated response sent to you by the QRadar event custom rules engine:

Jul 8, 2020 11:12:53 PM EDT


Rule Name:                                    Potential Data Loss
Rule Description:

Source IP:                                    192.168.48.99
Source Port:                                  27
Source Username (from event):                 LORD1
Source Network:                               Net-10-172-192.Net_192_168_0_0

Destination IP:                               192.168.48.99
Destination Port:                             18682
Destination Username (from Asset Identity):   N/A
Destination Network:                          Net-10-172-192.Net_192_168_0_0

Protocol:                                     other(255)
QID:                                          2000000

Event Name:                                   GDP Privileged User Accessing Sensitive Data
Event Description:
Category:                                     Data Loss Possible

Log Source ID:                                116
Log Source Name:                              IBM Guardium @192.168.48.93

Payload:                                      <30>Jul  8 23:12:53 g11 guard_sender[11331]: LEEF:1.0|IBM|Guardium|11.0|GDP Privileged User Accessing Sensitive
Data|ruleID=20003|ruleDesc=GDP Privileged User Accessing Sensitive Data|severity=INFO|devTime=2020-07-08
23:12:41|serverType=DB2|classification=|category=|dbProtocolVersion=3.0|usrName=|sourceProgram=DB2BP|start=1594264361584|dbUser=LORD1|dst=192.168.48.99|dstPort=1868
2|src=192.168.48.99|srcPort=27|protocol=SHARED MEMORY|type=SQL_LANG|violationID=77414200000000859|sql=select * from payroll.employer|error=
```

Chapter 1: SOC Team Detects Possible Data Breach – Jane Checks QRadar Offense Panel

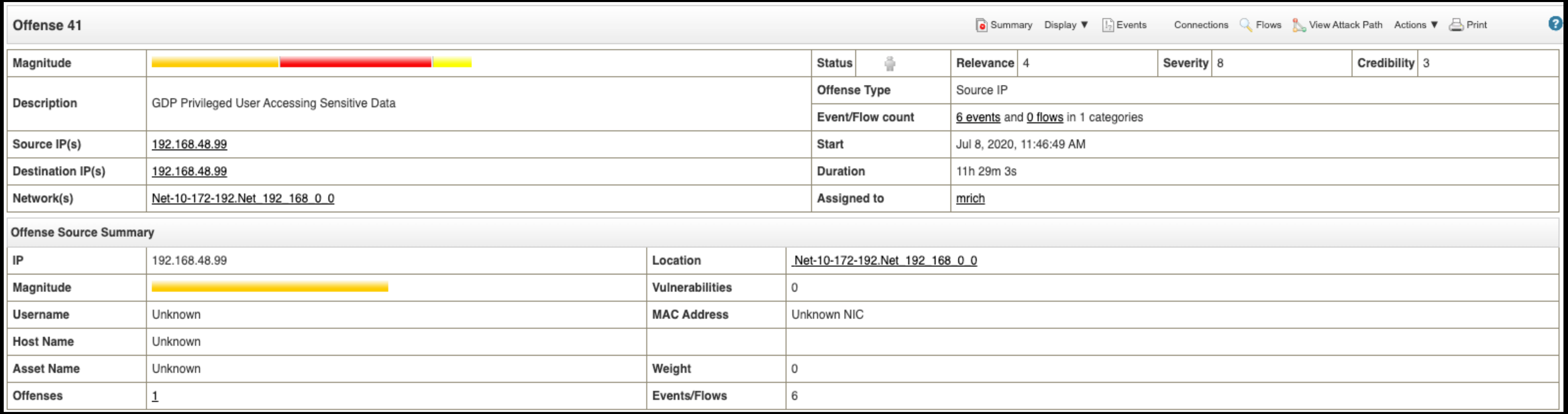


Offenses with last Event/Flow received from **Jul 8, 2020, 11:12:20 AM** to **Jul 9, 2020, 11:12:20 AM** View Offenses with: Select An Option:

Current Search Parameters:

Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

	Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources	Events	Flows	Start Date	Last Event/Flo
	41	GDP Privileged User Accessing Sensitive Data	Source IP	192.168.48.99	🟨🟥🟨	192.168.48.99	192.168.48.99	LORD1	IBM Guardium @19…	6	0	Jul 8, 2020, 11:46:49 AM	11h 56…



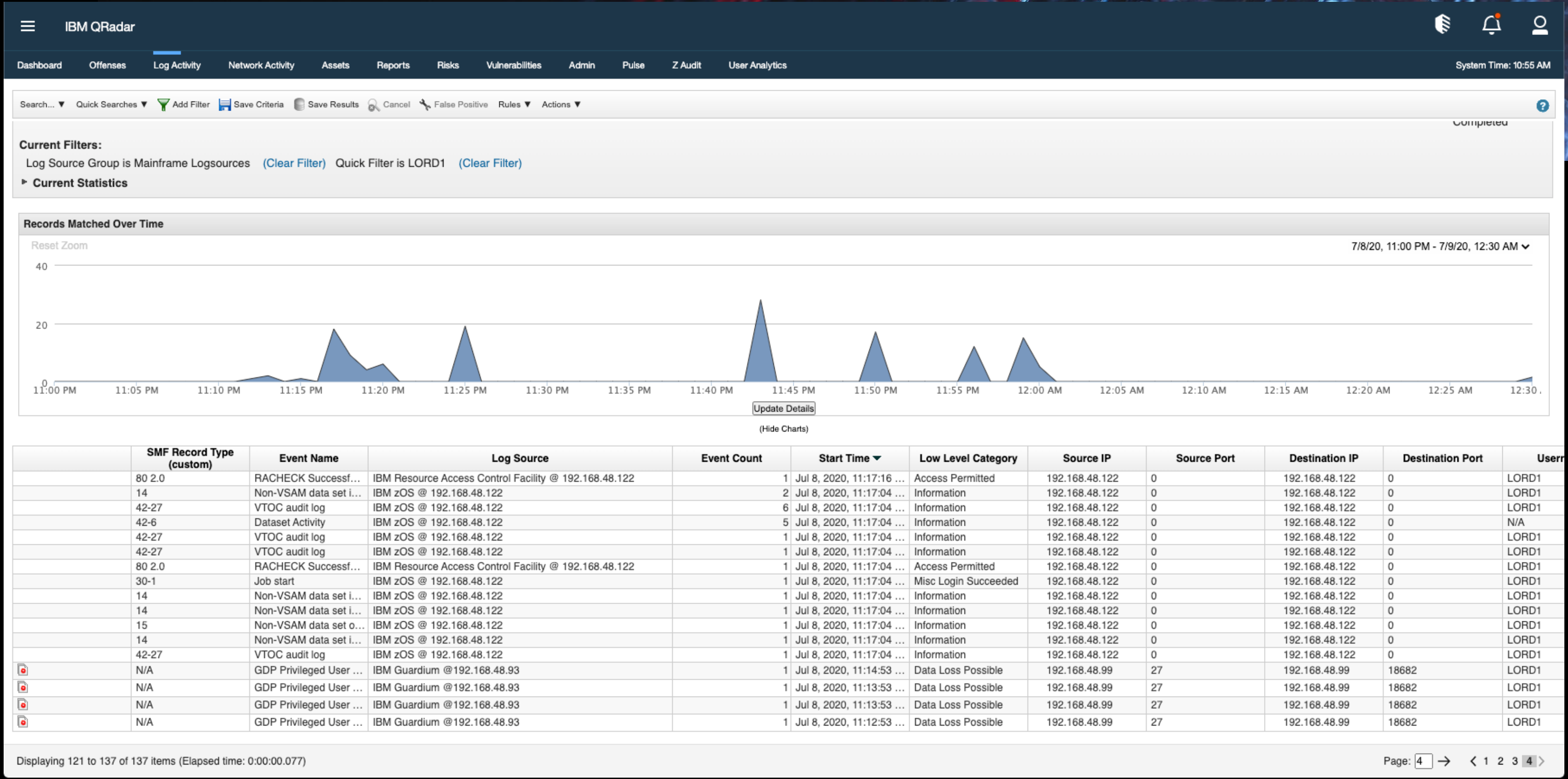
Offense 41

Magnitude	🟨🟥🟨	**Status**		**Relevance**	4	**Severity**	8	**Credibility**	3
Description	GDP Privileged User Accessing Sensitive Data	**Offense Type**	Source IP						
		Event/Flow count	6 events and 0 flows in 1 categories						
Source IP(s)	192.168.48.99	**Start**	Jul 8, 2020, 11:46:49 AM						
Destination IP(s)	192.168.48.99	**Duration**	11h 29m 3s						
Network(s)	Net-10-172-192.Net_192_168_0_0	**Assigned to**	mrich						

Offense Source Summary

IP	192.168.48.99	**Location**	Net-10-172-192.Net_192_168_0_0
Magnitude	🟨	**Vulnerabilities**	0
Username	Unknown	**MAC Address**	Unknown NIC
Host Name	Unknown		
Asset Name	Unknown	**Weight**	0
Offenses	1	**Events/Flows**	6

Chapter 1: SOC Team Detects Possible Data Breach – Jane Filters on LORD1 and Finds z/OS Activity



Current Filters:

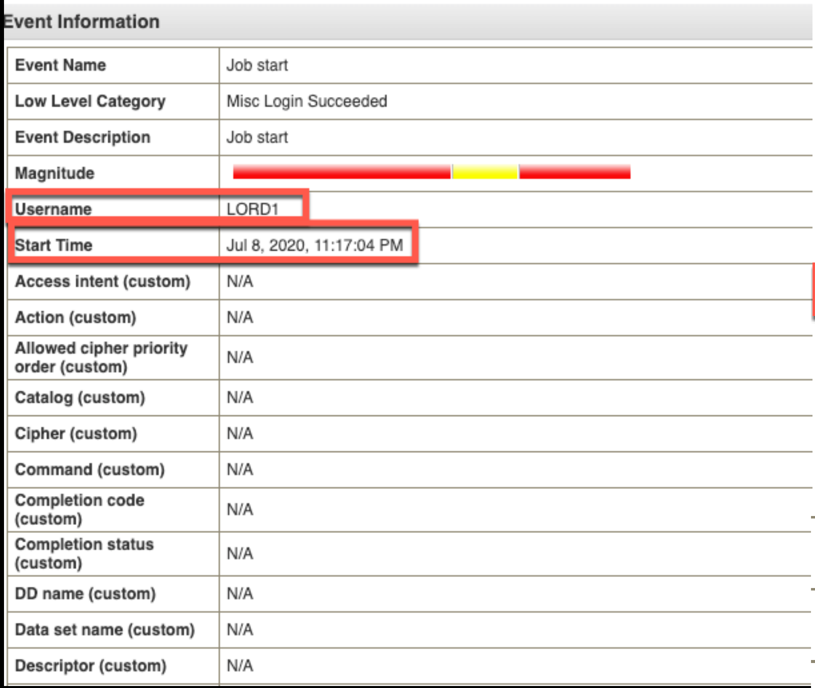
Log Source Group is Mainframe Logsources (Clear Filter) Quick Filter is LORD1 (Clear Filter)

▸ **Current Statistics**

	SMF Record Type (custom)	Event Name	Log Source	Event Count	Start Time ▼	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Userr
	80 2.0	RACHECK Successf…	IBM Resource Access Control Facility @ 192.168.48.122	1	Jul 8, 2020, 11:17:16 …	Access Permitted	192.168.48.122	0	192.168.48.122	0	LORD1
	14	Non-VSAM data set i…	IBM zOS @ 192.168.48.122	2	Jul 8, 2020, 11:17:04 …	Information	192.168.48.122	0	192.168.48.122	0	LORD1
	42-27	VTOC audit log	IBM zOS @ 192.168.48.122	6	Jul 8, 2020, 11:17:04 …	Information	192.168.48.122	0	192.168.48.122	0	LORD1
	42-6	Dataset Activity	IBM zOS @ 192.168.48.122	5	Jul 8, 2020, 11:17:04 …	Information	192.168.48.122	0	192.168.48.122	0	N/A
	42-27	VTOC audit log	IBM zOS @ 192.168.48.122	1	Jul 8, 2020, 11:17:04 …	Information	192.168.48.122	0	192.168.48.122	0	LORD1
	42-27	VTOC audit log	IBM zOS @ 192.168.48.122	1	Jul 8, 2020, 11:17:04 …	Information	192.168.48.122	0	192.168.48.122	0	LORD1
	80 2.0	RACHECK Successf…	IBM Resource Access Control Facility @ 192.168.48.122	1	Jul 8, 2020, 11:17:04 …	Access Permitted	192.168.48.122	0	192.168.48.122	0	LORD1
	30-1	Job start	IBM zOS @ 192.168.48.122	1	Jul 8, 2020, 11:17:04 …	Misc Login Succeeded	192.168.48.122	0	192.168.48.122	0	LORD1
	14	Non-VSAM data set i…	IBM zOS @ 192.168.48.122	1	Jul 8, 2020, 11:17:04 …	Information	192.168.48.122	0	192.168.48.122	0	LORD1
	14	Non-VSAM data set i…	IBM zOS @ 192.168.48.122	1	Jul 8, 2020, 11:17:04 …	Information	192.168.48.122	0	192.168.48.122	0	LORD1
	15	Non-VSAM data set o…	IBM zOS @ 192.168.48.122	1	Jul 8, 2020, 11:17:04 …	Information	192.168.48.122	0	192.168.48.122	0	LORD1
	14	Non-VSAM data set i…	IBM zOS @ 192.168.48.122	1	Jul 8, 2020, 11:17:04 …	Information	192.168.48.122	0	192.168.48.122	0	LORD1
	42-27	VTOC audit log	IBM zOS @ 192.168.48.122	1	Jul 8, 2020, 11:17:04 …	Information	192.168.48.122	0	192.168.48.122	0	LORD1
🗎	N/A	GDP Privileged User …	IBM Guardium @192.168.48.93	1	Jul 8, 2020, 11:14:53 …	Data Loss Possible	192.168.48.99	27	192.168.48.99	18682	LORD1
🗎	N/A	GDP Privileged User …	IBM Guardium @192.168.48.93	1	Jul 8, 2020, 11:13:53 …	Data Loss Possible	192.168.48.99	27	192.168.48.99	18682	LORD1
🗎	N/A	GDP Privileged User …	IBM Guardium @192.168.48.93	1	Jul 8, 2020, 11:13:53 …	Data Loss Possible	192.168.48.99	27	192.168.48.99	18682	LORD1
🗎	N/A	GDP Privileged User …	IBM Guardium @192.168.48.93	1	Jul 8, 2020, 11:12:53 …	Data Loss Possible	192.168.48.99	27	192.168.48.99	18682	LORD1

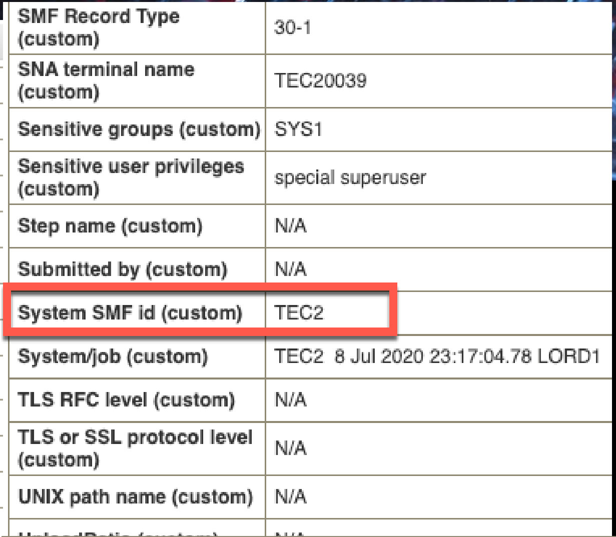
Displaying 121 to 137 of 137 items (Elapsed time: 0:00:00.077)

Chapter 1: SOC Team Detects Possible Data Breach – Jane Drills Down into LORD1 Activity on z/OS

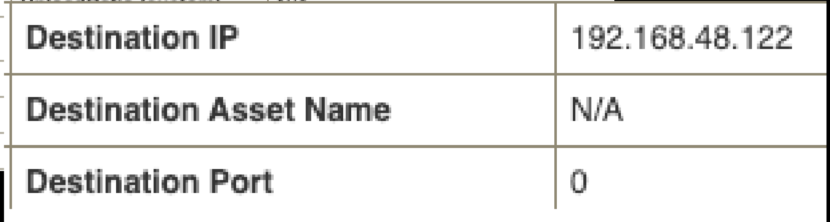


Event Information

Event Name	Job start
Low Level Category	Misc Login Succeeded
Event Description	Job start
Magnitude	🟥🟨🟥
Username	LORD1
Start Time	Jul 8, 2020, 11:17:04 PM
Access intent (custom)	N/A
Action (custom)	N/A
Allowed cipher priority order (custom)	N/A
Catalog (custom)	N/A
Cipher (custom)	N/A
Command (custom)	N/A
Completion code (custom)	N/A
Completion status (custom)	N/A
DD name (custom)	N/A
Data set name (custom)	N/A
Descriptor (custom)	N/A

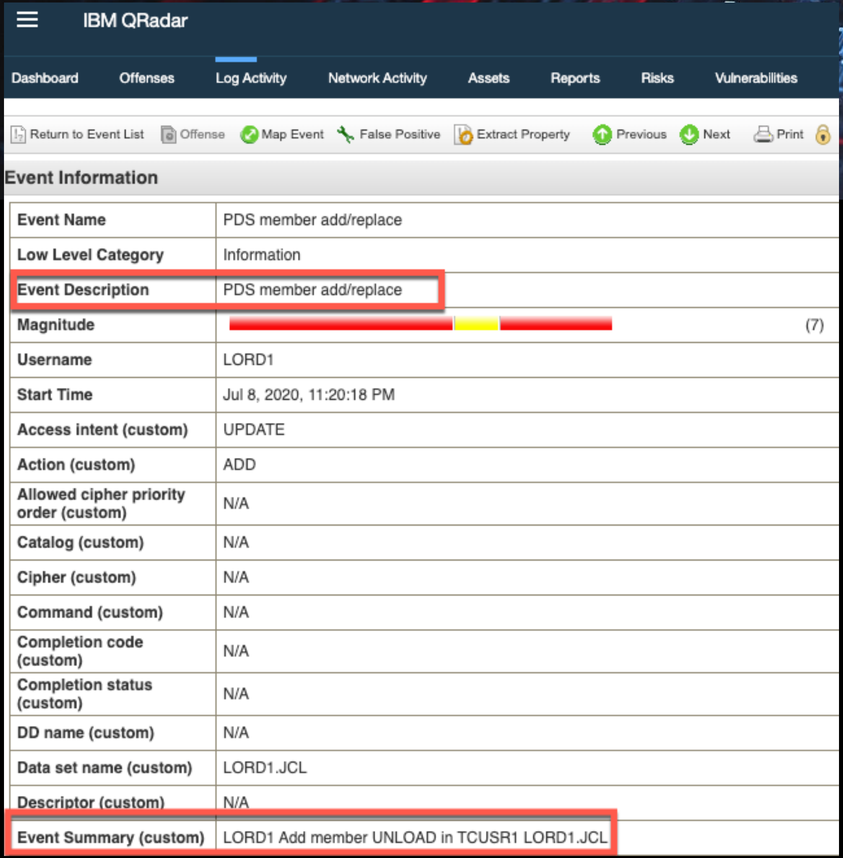


SMF Record Type (custom)	30-1
SNA terminal name (custom)	TEC20039
Sensitive groups (custom)	SYS1
Sensitive user privileges (custom)	special superuser
Step name (custom)	N/A
Submitted by (custom)	N/A
System SMF id (custom)	TEC2
System/job (custom)	TEC2 8 Jul 2020 23:17:04.78 LORD1
TLS RFC level (custom)	N/A
TLS or SSL protocol level (custom)	N/A
UNIX path name (custom)	N/A



Destination IP	192.168.48.122
Destination Asset Name	N/A
Destination Port	0

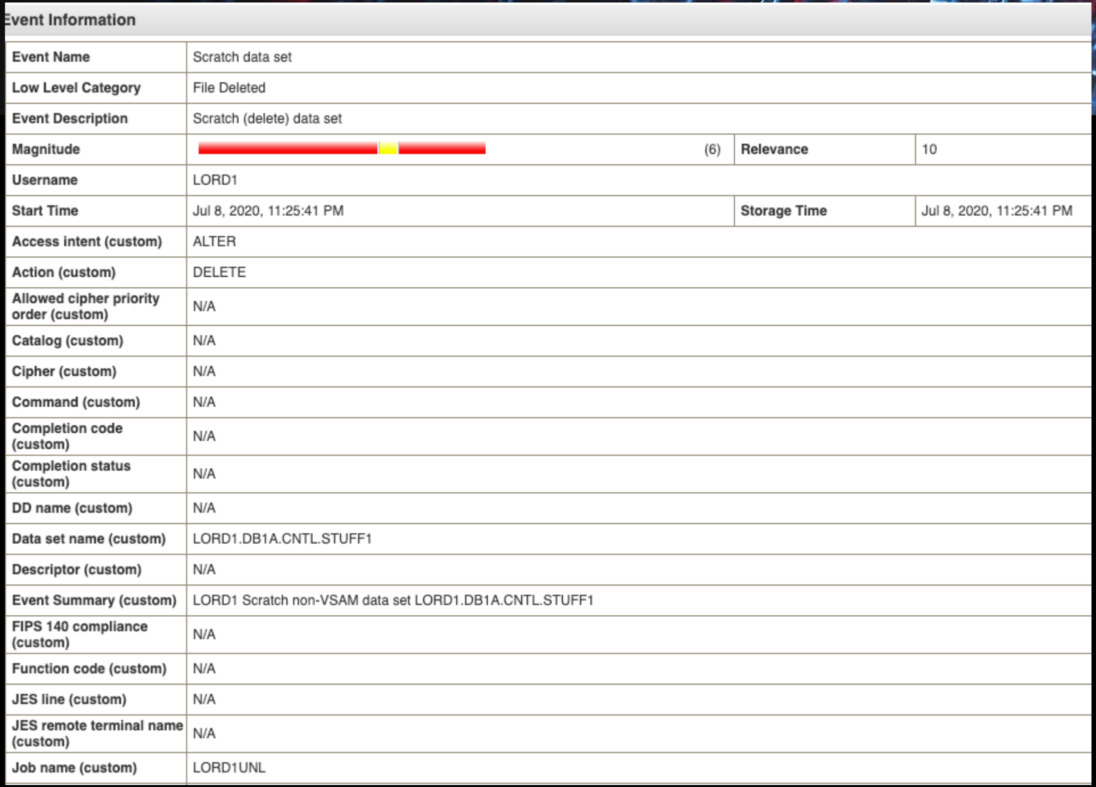
Chapter 1: SOC Team Detects Possible Data Breach – Jane Sees that LORD1 Created Some JCL



Event Information

Event Name	PDS member add/replace
Low Level Category	Information
Event Description	PDS member add/replace
Magnitude	(7)
Username	LORD1
Start Time	Jul 8, 2020, 11:20:18 PM
Access intent (custom)	UPDATE
Action (custom)	ADD
Allowed cipher priority order (custom)	N/A
Catalog (custom)	N/A
Cipher (custom)	N/A
Command (custom)	N/A
Completion code (custom)	N/A
Completion status (custom)	N/A
DD name (custom)	N/A
Data set name (custom)	LORD1.JCL
Descriptor (custom)	N/A
Event Summary (custom)	LORD1 Add member UNLOAD in TCUSR1 LORD1.JCL

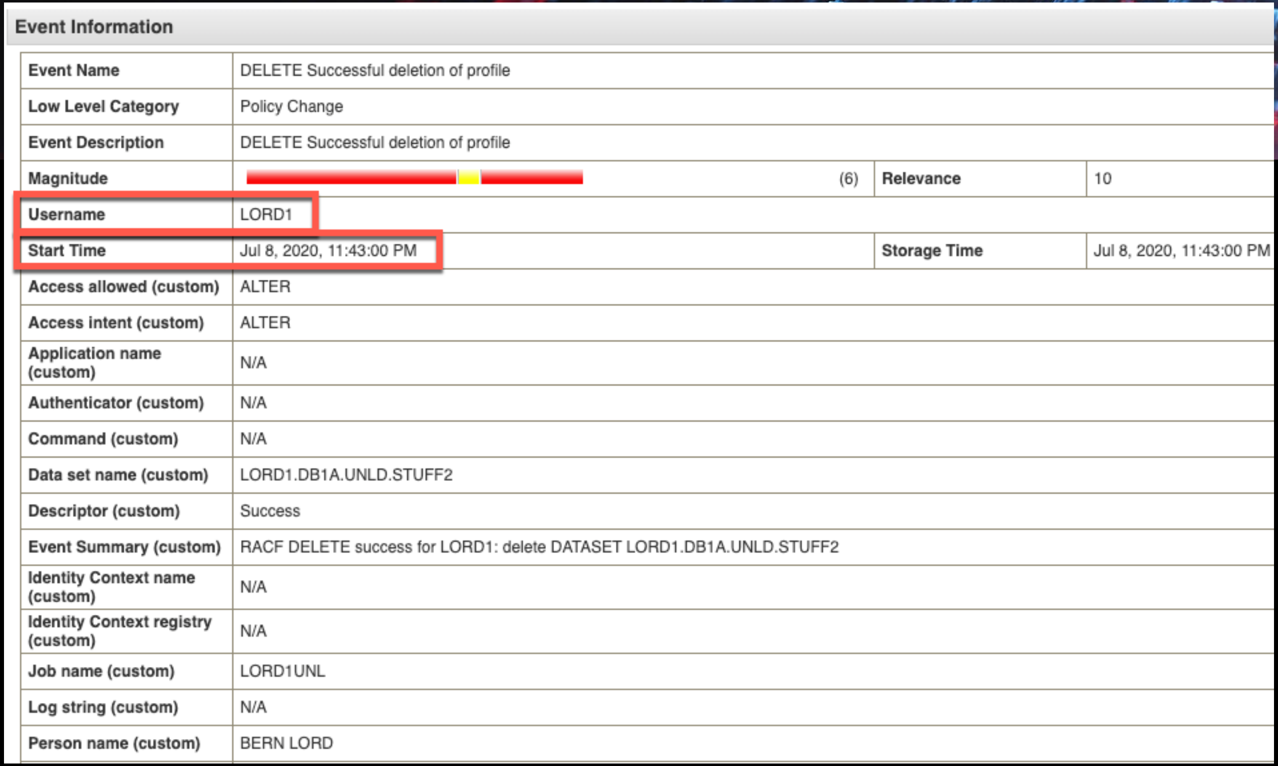
Chapter 1: SOC Team Detects Possible Data Breach – Jane Also Sees that LORD1 Created Some Datasets



Event Information

Event Name	Scratch data set		
Low Level Category	File Deleted		
Event Description	Scratch (delete) data set		
Magnitude	🟥🟥🟥🟨🟥🟥 (6)	Relevance	10
Username	LORD1		
Start Time	Jul 8, 2020, 11:25:41 PM	Storage Time	Jul 8, 2020, 11:25:41 PM
Access intent (custom)	ALTER		
Action (custom)	DELETE		
Allowed cipher priority order (custom)	N/A		
Catalog (custom)	N/A		
Cipher (custom)	N/A		
Command (custom)	N/A		
Completion code (custom)	N/A		
Completion status (custom)	N/A		
DD name (custom)	N/A		
Data set name (custom)	LORD1.DB1A.CNTL.STUFF1		
Descriptor (custom)	N/A		
Event Summary (custom)	LORD1 Scratch non-VSAM data set LORD1.DB1A.CNTL.STUFF1		
FIPS 140 compliance (custom)	N/A		
Function code (custom)	N/A		
JES line (custom)	N/A		
JES remote terminal name (custom)	N/A		
Job name (custom)	LORD1UNL		

Chapter 1: SOC Team Detects Possible Data Breach – Jane Finds When LORD1 Logged Off



Event Information

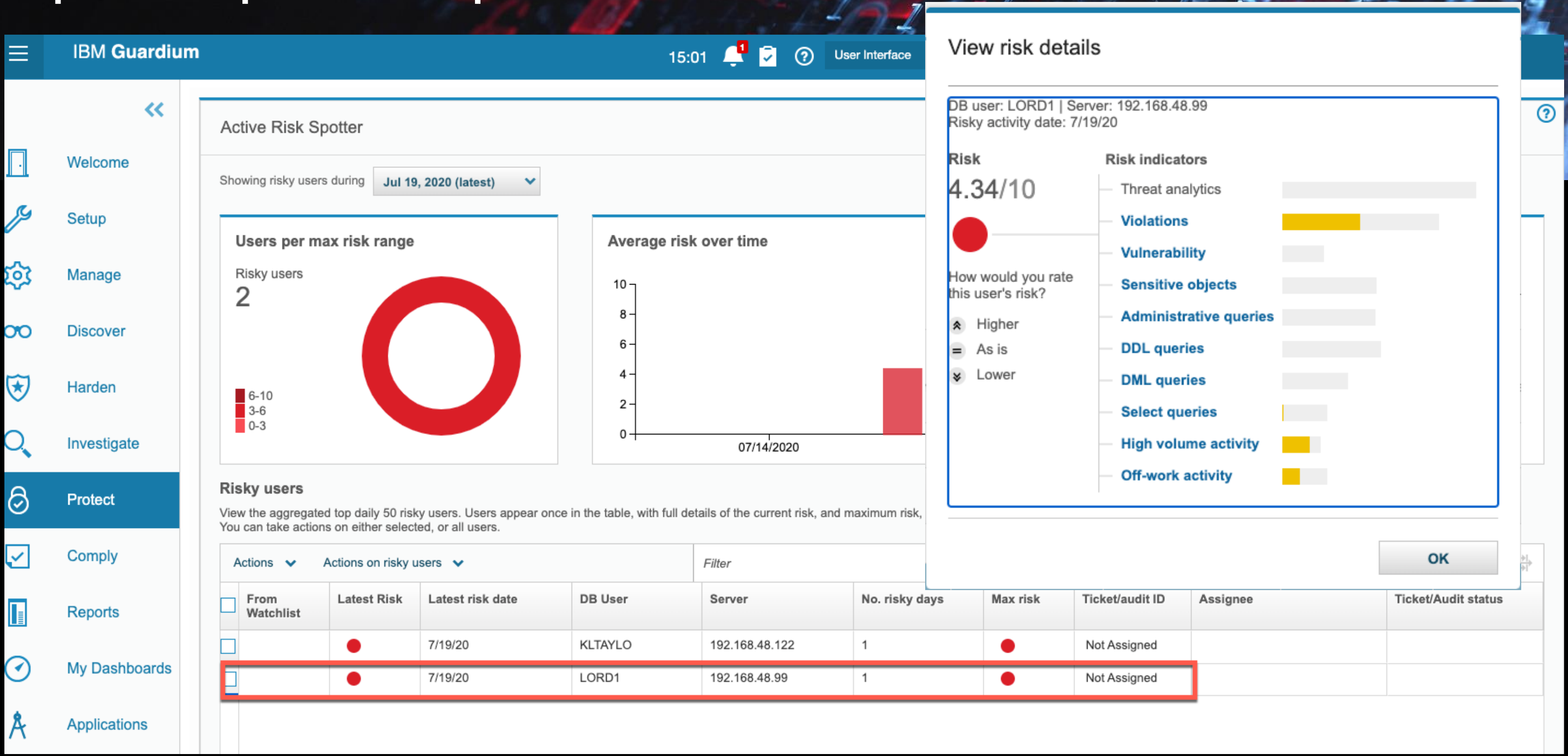
Event Name	DELETE Successful deletion of profile		
Low Level Category	Policy Change		
Event Description	DELETE Successful deletion of profile		
Magnitude	(6)	Relevance	10
Username	LORD1		
Start Time	Jul 8, 2020, 11:43:00 PM	Storage Time	Jul 8, 2020, 11:43:00 PM
Access allowed (custom)	ALTER		
Access intent (custom)	ALTER		
Application name (custom)	N/A		
Authenticator (custom)	N/A		
Command (custom)	N/A		
Data set name (custom)	LORD1.DB1A.UNLD.STUFF2		
Descriptor (custom)	Success		
Event Summary (custom)	RACF DELETE success for LORD1: delete DATASET LORD1.DB1A.UNLD.STUFF2		
Identity Context name (custom)	N/A		
Identity Context registry (custom)	N/A		
Job name (custom)	LORD1UNL		
Log string (custom)	N/A		
Person name (custom)	BERN LORD		

Chapter 2: Jane Contacts Sam on the Guardium Team

Sam investigates but knows they only have part of the picture

Guardium has no visibility into Db2 z/OS

Chapter 2: Guardium Team Investigates - Sam Opens up Risk Spotter and Finds LORD1



Active Risk Spotter

Showing risky users during Jul 19, 2020 (latest)

Users per max risk range

Risky users
2

Average risk over time

Risky users

View the aggregated top daily 50 risky users. Users appear once in the table, with full details of the current risk, and maximum risk, You can take actions on either selected, or all users.

□	From Watchlist	Latest Risk	Latest risk date	DB User	Server	No. risky days	Max risk	Ticket/audit ID	Assignee	Ticket/Audit status
□		●	7/19/20	KLTAYLO	192.168.48.122	1	●	Not Assigned		
□		●	7/19/20	LORD1	192.168.48.99	1	●	Not Assigned		

View risk details

DB user: LORD1 | Server: 192.168.48.99
Risky activity date: 7/19/20

Risk

4.34/10

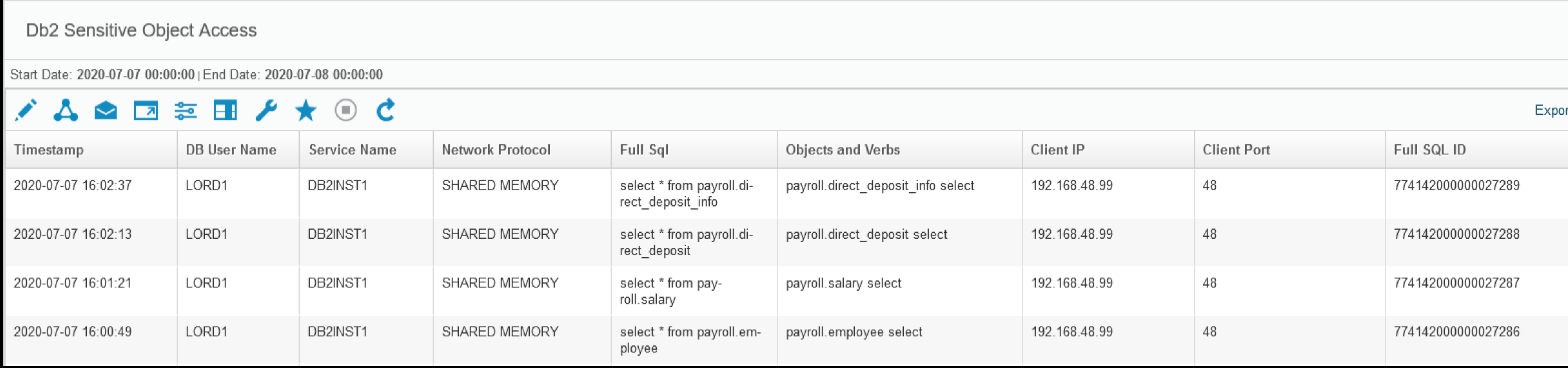
How would you rate this user's risk?

- Higher
- As is
- Lower

Risk indicators

- Threat analytics
- Violations
- Vulnerability
- Sensitive objects
- Administrative queries
- DDL queries
- DML queries
- Select queries
- High volume activity
- Off-work activity

Chapter 2: Guardium Team Investigates - Sam Determines which Sensitive Objects were accessed

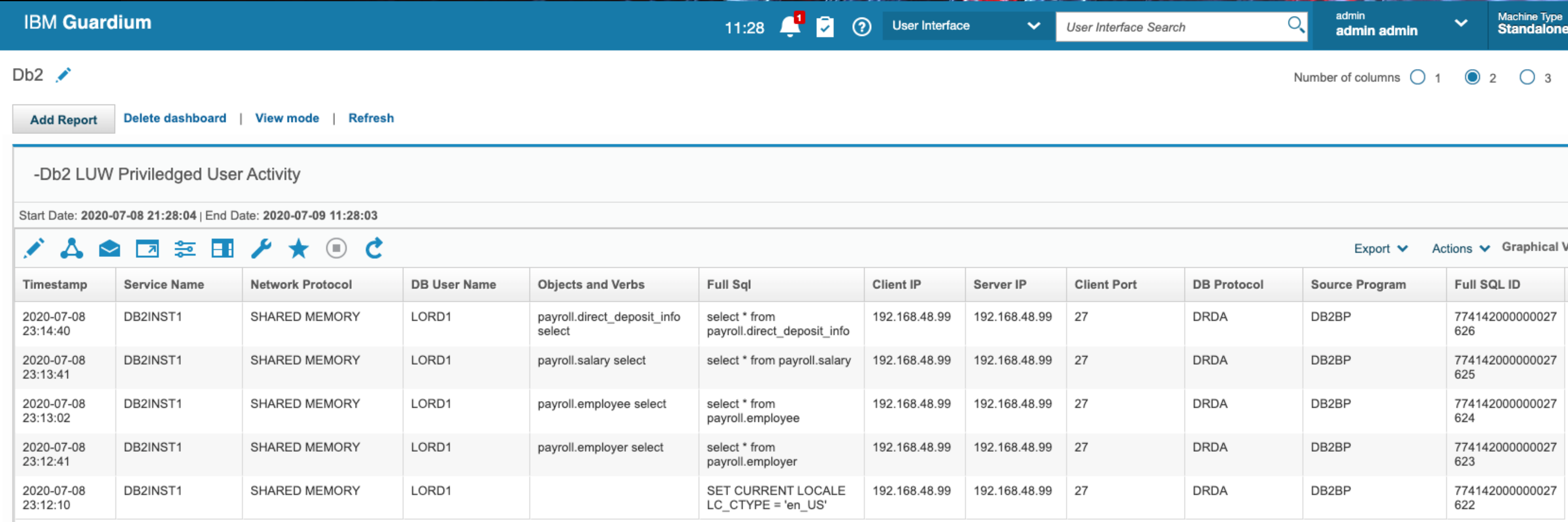


Db2 Sensitive Object Access

Start Date: **2020-07-07 00:00:00** | End Date: **2020-07-08 00:00:00**

Timestamp	DB User Name	Service Name	Network Protocol	Full Sql	Objects and Verbs	Client IP	Client Port	Full SQL ID
2020-07-07 16:02:37	LORD1	DB2INST1	SHARED MEMORY	select * from payroll.direct_deposit_info	payroll.direct_deposit_info select	192.168.48.99	48	774142000000027289
2020-07-07 16:02:13	LORD1	DB2INST1	SHARED MEMORY	select * from payroll.direct_deposit	payroll.direct_deposit select	192.168.48.99	48	774142000000027288
2020-07-07 16:01:21	LORD1	DB2INST1	SHARED MEMORY	select * from payroll.salary	payroll.salary select	192.168.48.99	48	774142000000027287
2020-07-07 16:00:49	LORD1	DB2INST1	SHARED MEMORY	select * from payroll.employee	payroll.employee select	192.168.48.99	48	774142000000027286

Chapter 2: Guardium Team Investigates - Sam Runs a Detailed Activity Report for LORD1



Db2

Number of columns ○ 1 ● 2 ○ 3

-Db2 LUW Priviledged User Activity

Start Date: **2020-07-08 21:28:04** | End Date: **2020-07-09 11:28:03**

Timestamp	Service Name	Network Protocol	DB User Name	Objects and Verbs	Full Sql	Client IP	Server IP	Client Port	DB Protocol	Source Program	Full SQL ID
2020-07-08 23:14:40	DB2INST1	SHARED MEMORY	LORD1	payroll.direct_deposit_info select	select * from payroll.direct_deposit_info	192.168.48.99	192.168.48.99	27	DRDA	DB2BP	774142000000027626
2020-07-08 23:13:41	DB2INST1	SHARED MEMORY	LORD1	payroll.salary select	select * from payroll.salary	192.168.48.99	192.168.48.99	27	DRDA	DB2BP	774142000000027625
2020-07-08 23:13:02	DB2INST1	SHARED MEMORY	LORD1	payroll.employee select	select * from payroll.employee	192.168.48.99	192.168.48.99	27	DRDA	DB2BP	774142000000027624
2020-07-08 23:12:41	DB2INST1	SHARED MEMORY	LORD1	payroll.employer select	select * from payroll.employer	192.168.48.99	192.168.48.99	27	DRDA	DB2BP	774142000000027623
2020-07-08 23:12:10	DB2INST1	SHARED MEMORY	LORD1		SET CURRENT LOCALE LC_CTYPE = 'en_US'	192.168.48.99	192.168.48.99	27	DRDA	DB2BP	774142000000027622

Chapter 3: Wake Up Call
- Bill (lord1) Tells Sam He Did Not Access Either System Last Night

Where are we now?

CISO discovers that their State of the Art Security was incomplete

Scope of the Breach is Unknown

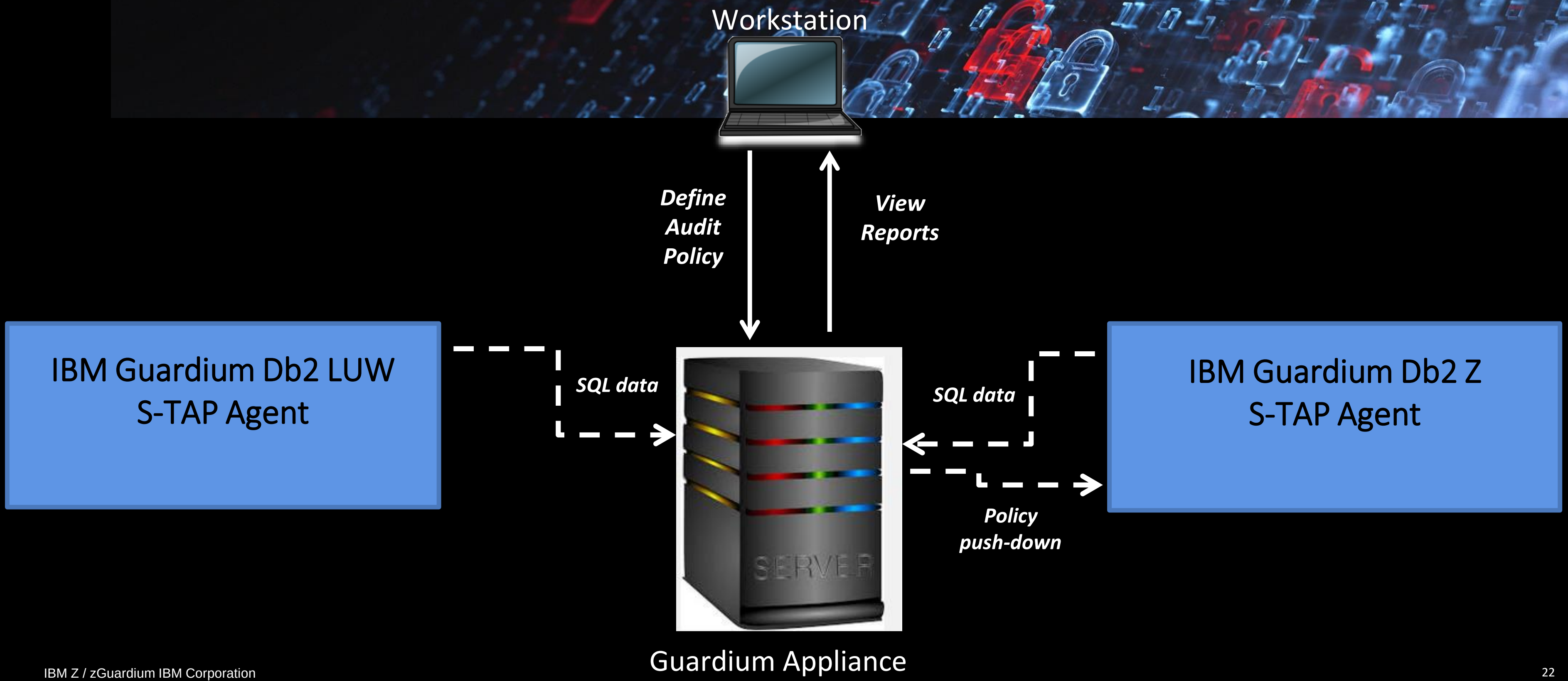
Lack of mainframe monitoring was a mistake

Looking back – if we had been monitoring Db2 z/OS

We would know the scope of the Breach

We may have detected z/OS activity earlier and averted breach all together

Chapter 4: CISO Adds Guardium on Db2 for z/OS – Architecture Overview



Workstation

Define Audit Policy

View Reports

IBM Guardium Db2 LUW S-TAP Agent

SQL data

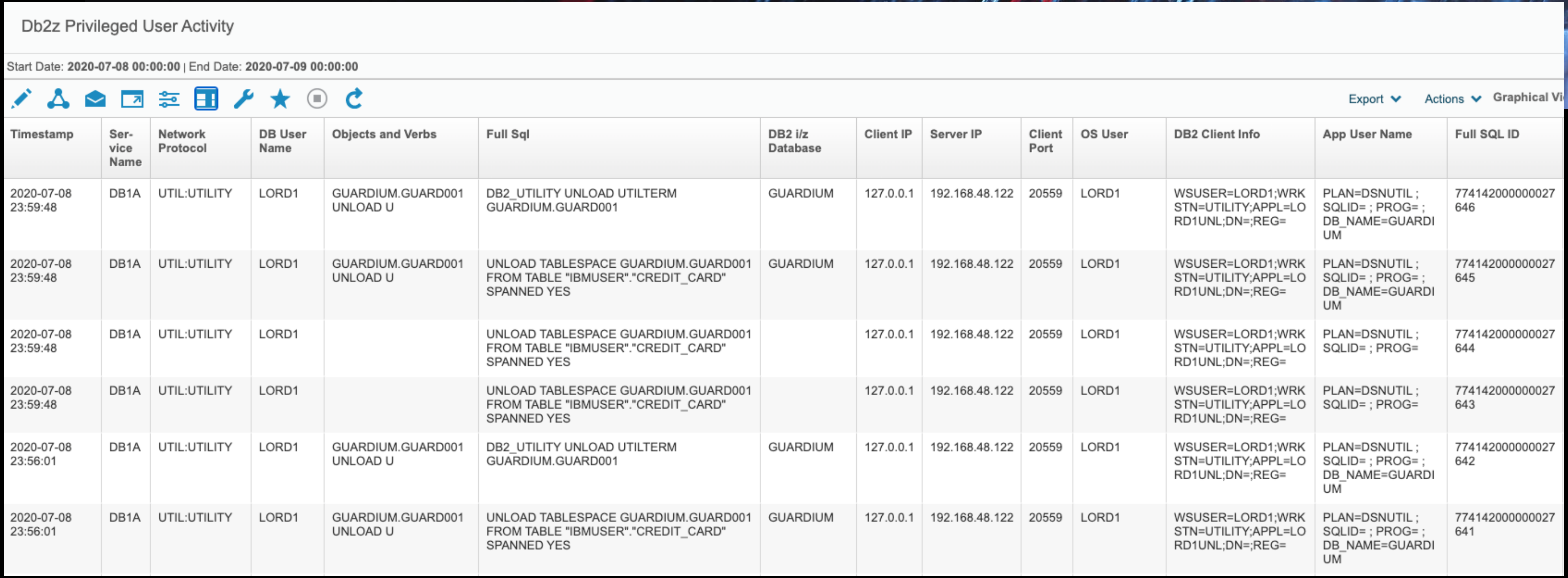
SQL data

IBM Guardium Db2 Z S-TAP Agent

Policy push-down

Guardium Appliance

Chapter 4: CISO Adds Guardium on Db2 for z/OS

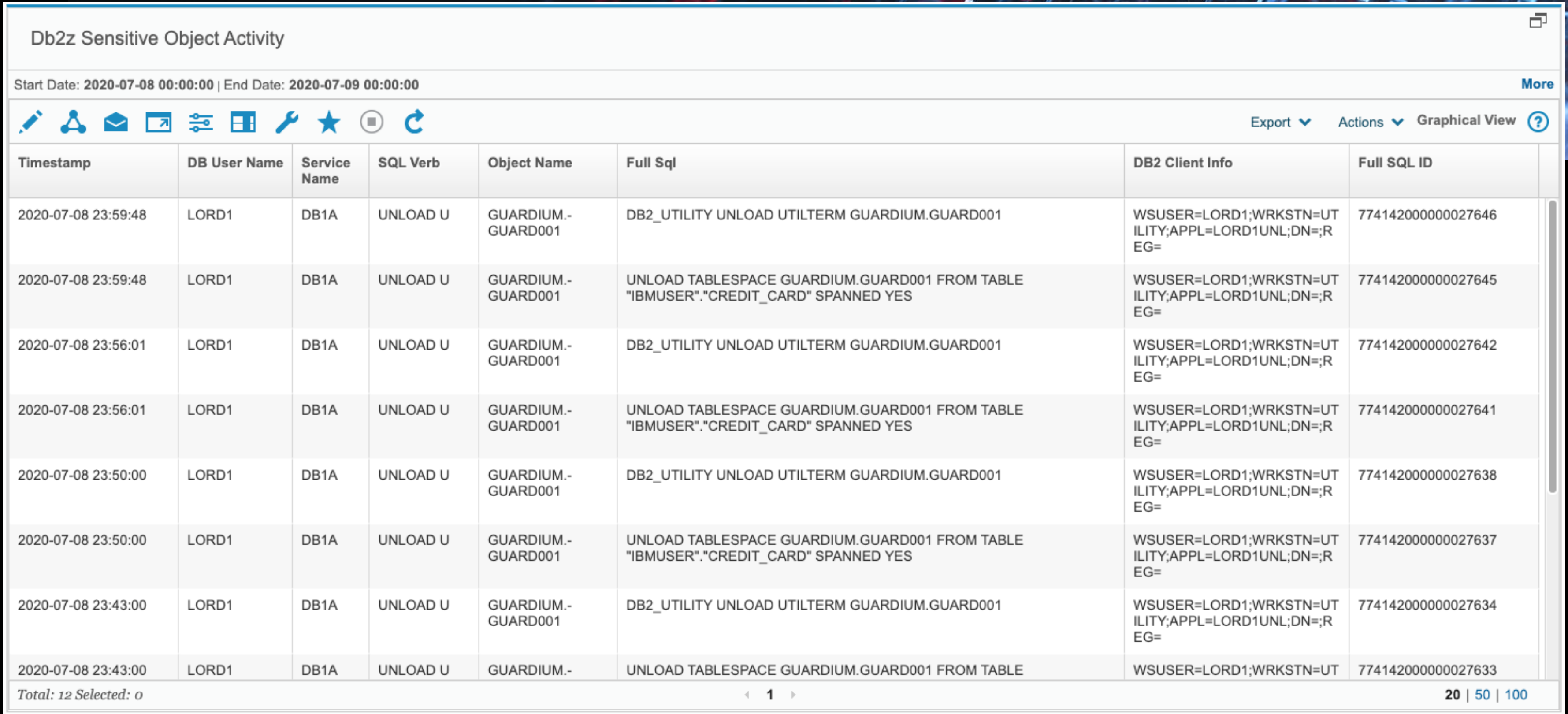


Db2z Privileged User Activity

Start Date: **2020-07-08 00:00:00** | End Date: **2020-07-09 00:00:00**

Timestamp	Ser-vice Name	Network Protocol	DB User Name	Objects and Verbs	Full Sql	DB2 i/z Database	Client IP	Server IP	Client Port	OS User	DB2 Client Info	App User Name	Full SQL ID
2020-07-08 23:59:48	DB1A	UTIL:UTILITY	LORD1	GUARDIUM.GUARD001 UNLOAD U	DB2_UTILITY UNLOAD UTILTERM GUARDIUM.GUARD001	GUARDIUM	127.0.0.1	192.168.48.122	20559	LORD1	WSUSER=LORD1;WRKSTN=UTILITY;APPL=LORD1UNL;DN=;REG=	PLAN=DSNUTIL ; SQLID= ; PROG= ; DB_NAME=GUARDIUM	774142000000027646
2020-07-08 23:59:48	DB1A	UTIL:UTILITY	LORD1	GUARDIUM.GUARD001 UNLOAD U	UNLOAD TABLESPACE GUARDIUM.GUARD001 FROM TABLE "IBMUSER"."CREDIT_CARD" SPANNED YES	GUARDIUM	127.0.0.1	192.168.48.122	20559	LORD1	WSUSER=LORD1;WRKSTN=UTILITY;APPL=LORD1UNL;DN=;REG=	PLAN=DSNUTIL ; SQLID= ; PROG= ; DB_NAME=GUARDIUM	774142000000027645
2020-07-08 23:59:48	DB1A	UTIL:UTILITY	LORD1		UNLOAD TABLESPACE GUARDIUM.GUARD001 FROM TABLE "IBMUSER"."CREDIT_CARD" SPANNED YES		127.0.0.1	192.168.48.122	20559	LORD1	WSUSER=LORD1;WRKSTN=UTILITY;APPL=LORD1UNL;DN=;REG=	PLAN=DSNUTIL ; SQLID= ; PROG=	774142000000027644
2020-07-08 23:59:48	DB1A	UTIL:UTILITY	LORD1		UNLOAD TABLESPACE GUARDIUM.GUARD001 FROM TABLE "IBMUSER"."CREDIT_CARD" SPANNED YES		127.0.0.1	192.168.48.122	20559	LORD1	WSUSER=LORD1;WRKSTN=UTILITY;APPL=LORD1UNL;DN=;REG=	PLAN=DSNUTIL ; SQLID= ; PROG=	774142000000027643
2020-07-08 23:56:01	DB1A	UTIL:UTILITY	LORD1	GUARDIUM.GUARD001 UNLOAD U	DB2_UTILITY UNLOAD UTILTERM GUARDIUM.GUARD001	GUARDIUM	127.0.0.1	192.168.48.122	20559	LORD1	WSUSER=LORD1;WRKSTN=UTILITY;APPL=LORD1UNL;DN=;REG=	PLAN=DSNUTIL ; SQLID= ; PROG= ; DB_NAME=GUARDIUM	774142000000027642
2020-07-08 23:56:01	DB1A	UTIL:UTILITY	LORD1	GUARDIUM.GUARD001 UNLOAD U	UNLOAD TABLESPACE GUARDIUM.GUARD001 FROM TABLE "IBMUSER"."CREDIT_CARD" SPANNED YES	GUARDIUM	127.0.0.1	192.168.48.122	20559	LORD1	WSUSER=LORD1;WRKSTN=UTILITY;APPL=LORD1UNL;DN=;REG=	PLAN=DSNUTIL ; SQLID= ; PROG= ; DB_NAME=GUARDIUM	774142000000027641

Chapter 4: CISO Deploys Guardium on Db2 for z/OS



Db2z Sensitive Object Activity

Start Date: **2020-07-08 00:00:00** | End Date: **2020-07-09 00:00:00**

Timestamp	DB User Name	Service Name	SQL Verb	Object Name	Full Sql	DB2 Client Info	Full SQL ID
2020-07-08 23:59:48	LORD1	DB1A	UNLOAD U	GUARDIUM.-GUARD001	DB2_UTILITY UNLOAD UTILTERM GUARDIUM.GUARD001	WSUSER=LORD1;WRKSTN=UTILITY;APPL=LORD1UNL;DN=;REG=	774142000000027646
2020-07-08 23:59:48	LORD1	DB1A	UNLOAD U	GUARDIUM.-GUARD001	UNLOAD TABLESPACE GUARDIUM.GUARD001 FROM TABLE "IBMUSER"."CREDIT_CARD" SPANNED YES	WSUSER=LORD1;WRKSTN=UTILITY;APPL=LORD1UNL;DN=;REG=	774142000000027645
2020-07-08 23:56:01	LORD1	DB1A	UNLOAD U	GUARDIUM.-GUARD001	DB2_UTILITY UNLOAD UTILTERM GUARDIUM.GUARD001	WSUSER=LORD1;WRKSTN=UTILITY;APPL=LORD1UNL;DN=;REG=	774142000000027642
2020-07-08 23:56:01	LORD1	DB1A	UNLOAD U	GUARDIUM.-GUARD001	UNLOAD TABLESPACE GUARDIUM.GUARD001 FROM TABLE "IBMUSER"."CREDIT_CARD" SPANNED YES	WSUSER=LORD1;WRKSTN=UTILITY;APPL=LORD1UNL;DN=;REG=	774142000000027641
2020-07-08 23:50:00	LORD1	DB1A	UNLOAD U	GUARDIUM.-GUARD001	DB2_UTILITY UNLOAD UTILTERM GUARDIUM.GUARD001	WSUSER=LORD1;WRKSTN=UTILITY;APPL=LORD1UNL;DN=;REG=	774142000000027638
2020-07-08 23:50:00	LORD1	DB1A	UNLOAD U	GUARDIUM.-GUARD001	UNLOAD TABLESPACE GUARDIUM.GUARD001 FROM TABLE "IBMUSER"."CREDIT_CARD" SPANNED YES	WSUSER=LORD1;WRKSTN=UTILITY;APPL=LORD1UNL;DN=;REG=	774142000000027637
2020-07-08 23:43:00	LORD1	DB1A	UNLOAD U	GUARDIUM.-GUARD001	DB2_UTILITY UNLOAD UTILTERM GUARDIUM.GUARD001	WSUSER=LORD1;WRKSTN=UTILITY;APPL=LORD1UNL;DN=;REG=	774142000000027634
2020-07-08 23:43:00	LORD1	DB1A	UNLOAD U	GUARDIUM.-	UNLOAD TABLESPACE GUARDIUM.GUARD001 FROM TABLE	WSUSER=LORD1;WRKSTN=UT	774142000000027633

Total: 12 Selected: 0

1

20 | 50 | 100

Other Gaps in z/OS Security

Passwords are a weak link

If you can not access the system you can not steal data

Multi Factor Authentication can replace the weak password only link

Chapter 5: Eliminate Password Only Access

What is multi-factor authentication?

SOMETHING THAT YOU KNOW

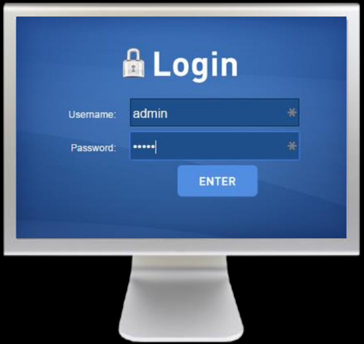
- Passwords
- PIN Code

SOMETHING THAT YOU HAVE

- ID Badge
- One time passwords
  - Time-based

SOMETHING THAT YOU ARE

- Biometrics



Username: admin

Password: •••••

United States Government

JAN2009

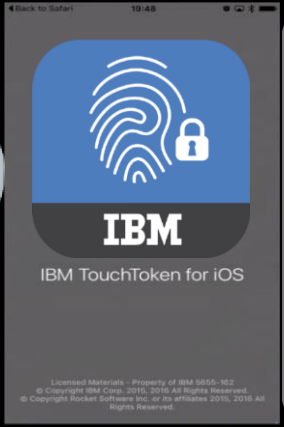
Affiliation Civilian

Agency/Department DoD

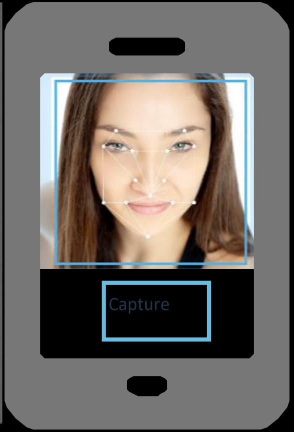
Expires 2009JAN18

Doe, John, G.

Identification Card



Licensed Materials - Property of IBM 5655-162
© Copyright IBM Corp. 2015, 2016 All Rights Reserved.
© Copyright Rocket Software Inc. or its affiliates 2015, 2016 All Rights Reserved.



Chapter 5: How could this have been prevented?

Black Hat 2017 Hacker Survey Report[1]

QUESTION: **What type of security is the hardest to get past?**

68% say multi-factor authentication and encryption are biggest hacker obstacles

32% OF HACKERS SAY

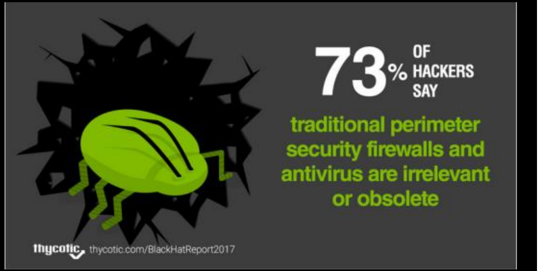
accessing privileged accounts was the number one choice for the easiest and fastest way to get at sensitive data

thycotic thycotic.com/BlackHatReport2017

80% OF HACKERS SAY

humans are the most responsible for security breaches

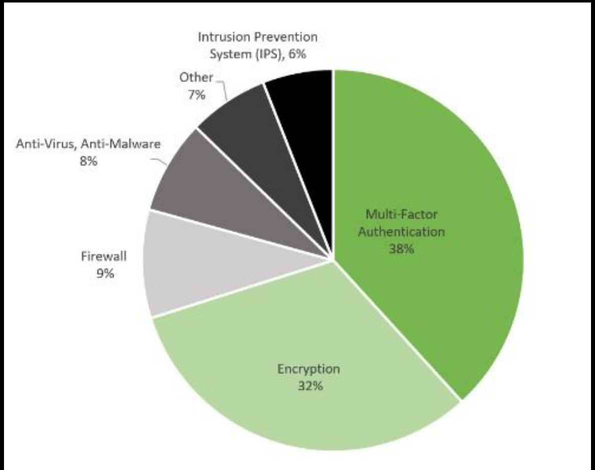
thycotic thycotic.com/BlackHatReport2017



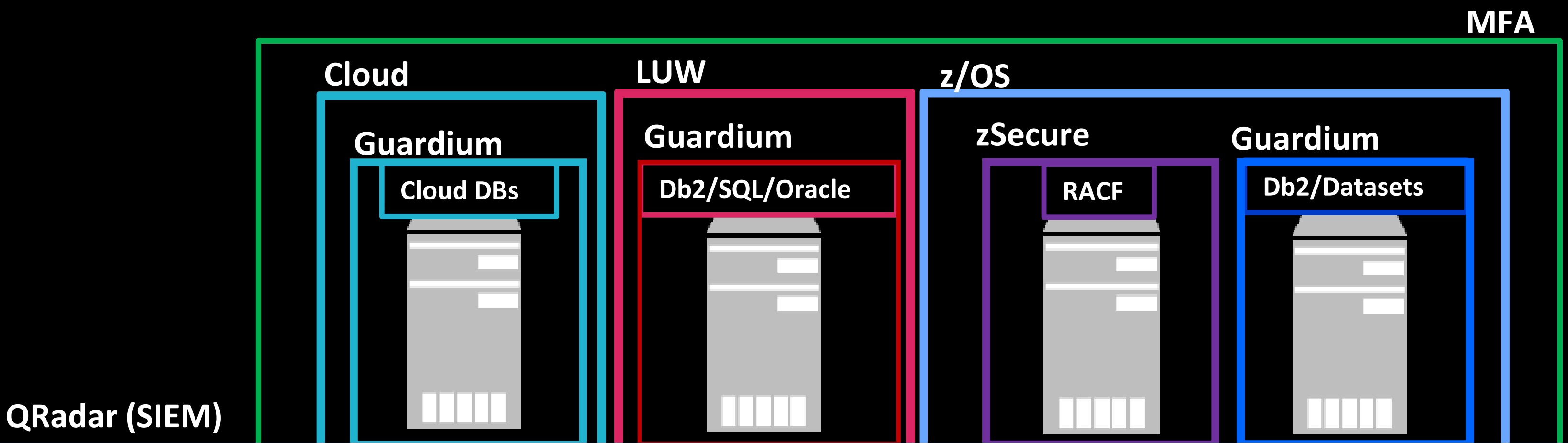
73% OF HACKERS SAY

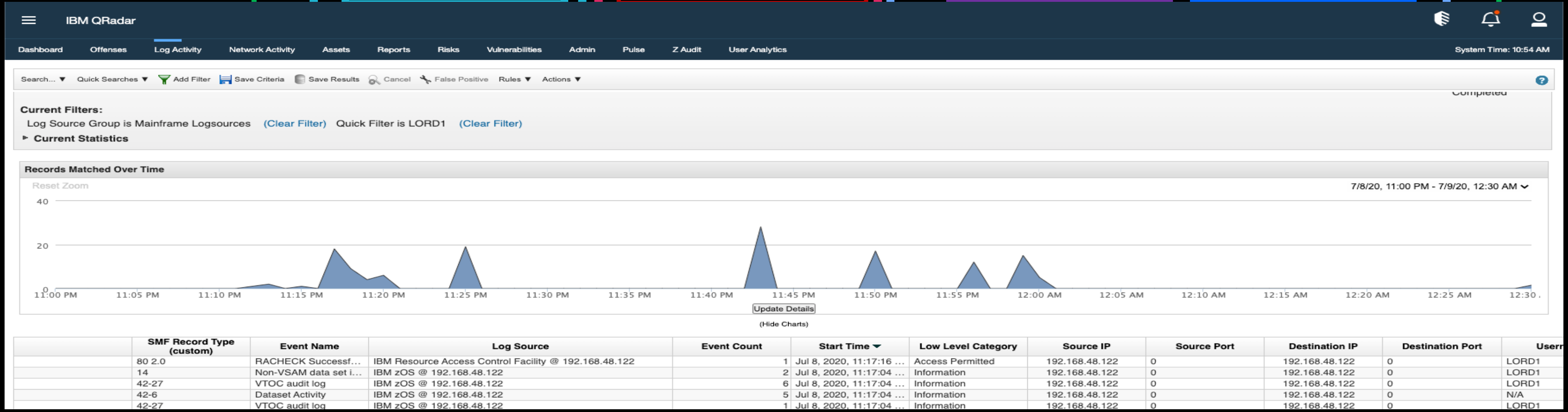
traditional perimeter security firewalls and antivirus are irrelevant or obsolete

thycotic thycotic.com/BlackHatReport2017



Chapter 6: Holistic Security Picture





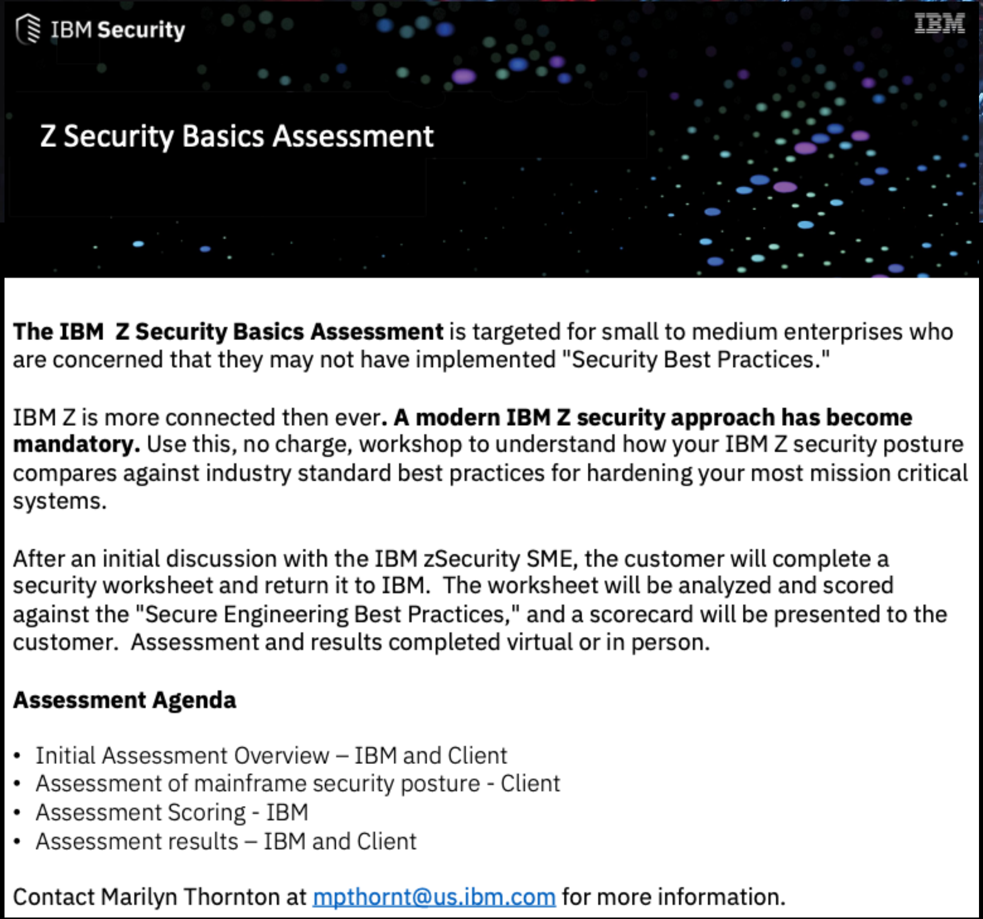
Current Filters:

Log Source Group is Mainframe Logsources (Clear Filter) Quick Filter is LORD1 (Clear Filter)

▸ **Current Statistics**

	SMF Record Type (custom)	Event Name	Log Source	Event Count	Start Time ▼	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Userr
	80 2.0	RACHECK Successf...	IBM Resource Access Control Facility @ 192.168.48.122	1	Jul 8, 2020, 11:17:16 ...	Access Permitted	192.168.48.122	0	192.168.48.122	0	LORD1
	14	Non-VSAM data set i...	IBM zOS @ 192.168.48.122	2	Jul 8, 2020, 11:17:04 ...	Information	192.168.48.122	0	192.168.48.122	0	LORD1
	42-27	VTOC audit log	IBM zOS @ 192.168.48.122	6	Jul 8, 2020, 11:17:04 ...	Information	192.168.48.122	0	192.168.48.122	0	LORD1
	42-6	Dataset Activity	IBM zOS @ 192.168.48.122	5	Jul 8, 2020, 11:17:04 ...	Information	192.168.48.122	0	192.168.48.122	0	N/A
	42-27	VTOC audit log	IBM zOS @ 192.168.48.122	1	Jul 8, 2020, 11:17:04 ...	Information	192.168.48.122	0	192.168.48.122	0	LORD1

Chapter 7: How does your Security Stack Up?



IBM Security

IBM

Z Security Basics Assessment

The IBM Z Security Basics Assessment is targeted for small to medium enterprises who are concerned that they may not have implemented "Security Best Practices."

IBM Z is more connected then ever**. A modern IBM Z security approach has become mandatory.** Use this, no charge, workshop to understand how your IBM Z security posture compares against industry standard best practices for hardening your most mission critical systems.

After an initial discussion with the IBM zSecurity SME, the customer will complete a security worksheet and return it to IBM. The worksheet will be analyzed and scored against the "Secure Engineering Best Practices," and a scorecard will be presented to the customer. Assessment and results completed virtual or in person.

Assessment Agenda

- Initial Assessment Overview – IBM and Client
- Assessment of mainframe security posture - Client
- Assessment Scoring - IBM
- Assessment results – IBM and Client

Contact Marilyn Thornton at mpthornt@us.ibm.com for more information.

Chapter 8: Closing Statements

Q and A

IBM **Security**

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- ibm.com/security/community
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2019. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM®

IBM