FRESCHE SOLUTIONS

Data Encryption

The Last Line of Defense for Your IBM i?

Carol Woodbury
CTO, DXR Security

Pauline Brazil Ayala
VP, Compliance & Security Solutions

Why Encryption?

- Compliance requirements:
  - PCI DSS
- Eliminate breach notification requirements

DXR SECURITY

2

Privacy Around the World

More US States Enforce Privacy Laws in 2023:

- California (effective 1/1/23)
- Colorado (effective 7/1/23)
- Connecticut (effective 7/1/23)
- Utah (effective 12/31/23)
- Virginia (effective 1/1/23)

Canada

Singapore

EU

UK

3

Data is an Asset

- More organizations understand that their data has value
  - Data unique to the organization
    - Pricing
    - Inventory levels
    - Sales information
    - Accounts payable (vendor list)
    - Accounts receivable (customer list)

4

Data Goes EVERYWHERE !!!

5

The Play ransomware gang has released data allegedly stolen from Dutch maritime logistics services company Royal Dirkzwager.

Ferrari Says Ransomware Attack Exposed Customer Data

Ferrari said that a ransomware attack was responsible for a data breach that exposed customer details, but did not impact company operations.

Hitachi Energy Blames Data Breach on Zero-Day as Ransomware Gang Threatens Firm

Hitachi Energy has blamed a data breach affecting employees on the recent exploitation of a zero-day vulnerability in Fortra's GoAnywhere solution.

Florida-based health services company Independent Living Systems (ILS) has started sending out notification letters to more than 4 million individuals to inform them of a data breach impacting their personal and medical information.

Latitude Financial Services Data Breach Impacts 300,000 Customers

Latitude Financial Services says the personal information of 300,000 customers was stolen in a cyberattack.

Headlines from SecurityWeek.com one week in March 2023

6

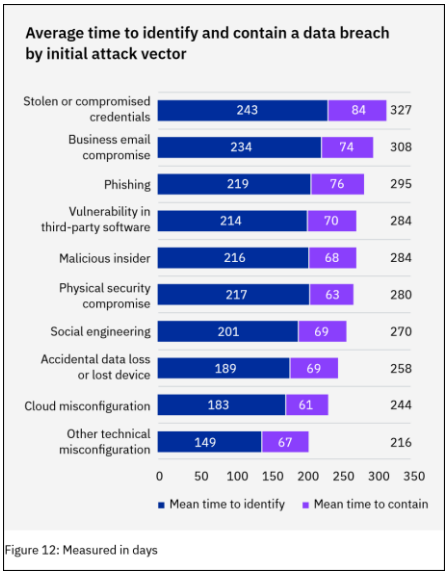
Protect Data with Encryption

Encryption for Data:

- In motion
- At rest

7

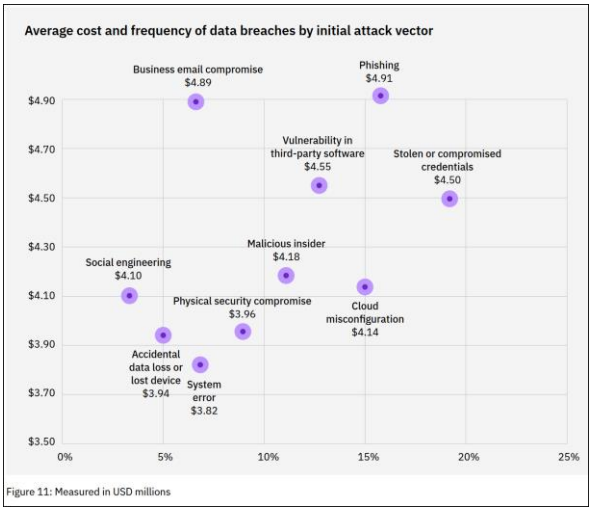
Average Time to Detect and Contain a Breach via Compromised Credentials



- Source: Ponemon Institute's Cost of a Data Breach Report 2022 (sponsored by IBM)

8

Most Frequent Initial Attack Vector: Compromised Credentials



Source: Ponemon Institute's Cost of a Data Breach Report 2021 (sponsored by IBM)

9

Use Encrypted Transmissions

- Not just for external communications but internal as well.

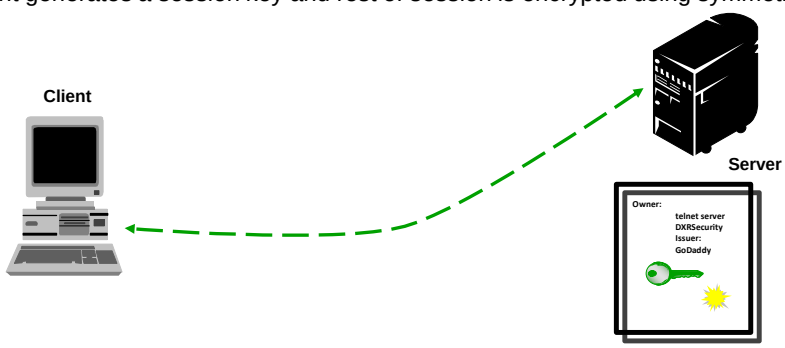
10

Encrypting Data in Motion on IBM i

11

End-to-End Encrypted Communication Sessions

1. Client is configured to request the server for an encrypted session
2. Client contacts the server and provides it with the list of ciphers available to use to encrypt the session
3. Server responds with info on its digital certificate and which cipher it will use
4. Client verifies the server's digital certificate
5. Client generates a session key and rest of session is encrypted using symmetric key



12

Digital Certificate

- Allows:
  - the client to trust the server
  - enables encrypted session
- Issued by a CA (Certificate Authority)
  - Well-known
  - Internal
  - IBM i
- For more information:
  - https://www.ibm.com/docs/en/i/7.5?topic=security-digital-certificate-manager

13

13

QSSL* System Values

- QSSLPCL – list of SSL protocols on the system
  - *OPSYS – list is determined by the system and can varies by release. This is the default. Or to control, specify one or more of the following:
    - *TLSV13
    - *TLSV12
    - *TLSV11
    - *TLSV1
    - *SSLV3
    - *SSLV2
- QSSLCSLCTL – who controls the list specified in QSSLCSL – the system (*OPSYS - default) or user (*USRDFN)
- QSSLCSL – contains list of ordered cipher suites to be used on an SSL connection. Can only be modified if QSSLCSLCTL is *USRDFN.

14

Protocols by Release

OS Release	SSLv2	SSLv3	TLS1.0	TLS1.1	TLS1.2	TLS1.3
V5R4	A	X	X			
V6R1	A	X	X			
V7R1	A	X	X			
V7R1 w/TR6	A	X	X	A	A	
V7R2	A	A	X	X	X	
V7R3	A	A	X	X	X	
V7R3 w/TR18	A	A	X	X	X	A
V7R4		A	A	A	X	X
V7R5		A	A	A	X	X

X = Enabled by default
A = Available but not by default
Blank = Not available

15

Ciphers by Release

V7R3

- ECDHE_ECDSA_AES_128_GCM_SHA256
- ECDHE_ECDSA_AES_256_GCM_SHA384
- ECDHE_RSA_AES_128_GCM_SHA256
- ECDHE_RSA_AES_256_GCM_SHA384
- RSA_AES_128_GCM_SHA256
- RSA_AES_256_GCM_SHA384
- ECDHE_ECDSA_AES_128_CBC_SHA256
- ECDHE_ECDSA_AES_256_CBC_SHA384
- ECDHE_RSA_AES_128_CBC_SHA256
- ECDHE_RSA_AES_256_CBC_SHA384
- RSA_AES_128_CBC_SHA256
- RSA_AES_128_CBC_SHA
- RSA_AES_256_CBC_SHA256
- RSA_AES_256_CBC_SHA
- ECDHE_ECDSA_3DES_EDE_CBC_SHA
- ECDHE_RSA_3DES_EDE_CBC_SHA
- RSA_3DES_EDE_CBC_SHA

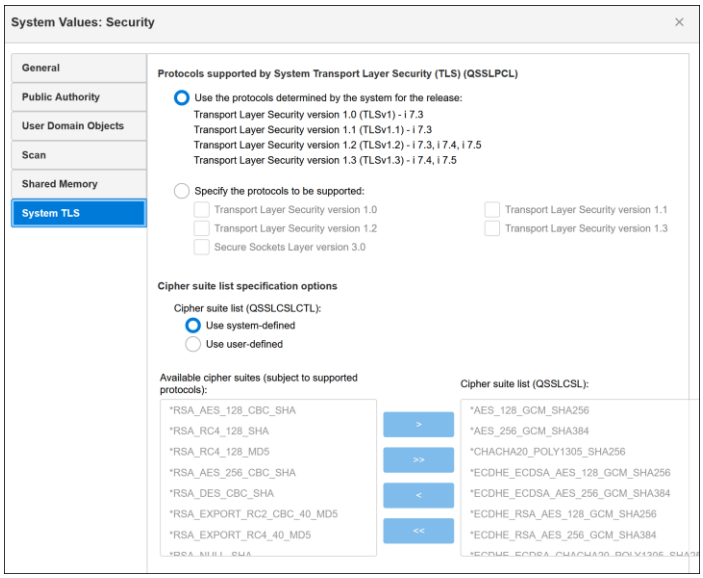
V7R4 / V7R5

- *AES_128_GCM_SHA256
- *AES_256_GCM_SHA384
- *CHACHA20_POLY1305_SHA256
- *ECDHE_ECDSA_AES_128_GCM_SHA256
- *ECDHE_ECDSA_AES_256_GCM_SHA384
- *ECDHE_RSA_AES_128_GCM_SHA256
- *ECDHE_RSA_AES_256_GCM_SHA384
- *ECDHE_ECDSA_CHACHA20_POLY1305_SHA256
- *ECDHE_RSA_CHACHA20_POLY1305_SHA256

16

16

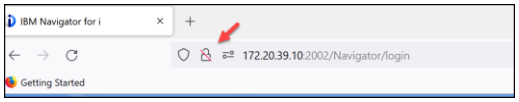
TLS (SSL) System Values



17

Secure the New Nav Connection

- IBM stopped shipping a self-signed cert
- Need to assign one
- https://www.ibm.com/support/pages/enabling-tls-ibm-navigator-i



18

Encrypting Data at Rest

19

Malware on IBM i

Two types of malware affect IBM i:

- Resident (Stored) in the IFS
- Coming in via a file share

Malware has evolved:

- Data is now often exfiltrated (downloaded) prior to encryption

20

Remember - Data Goes EVERYWHERE !!!

21

Encrypting Data at Rest on IBM i

22

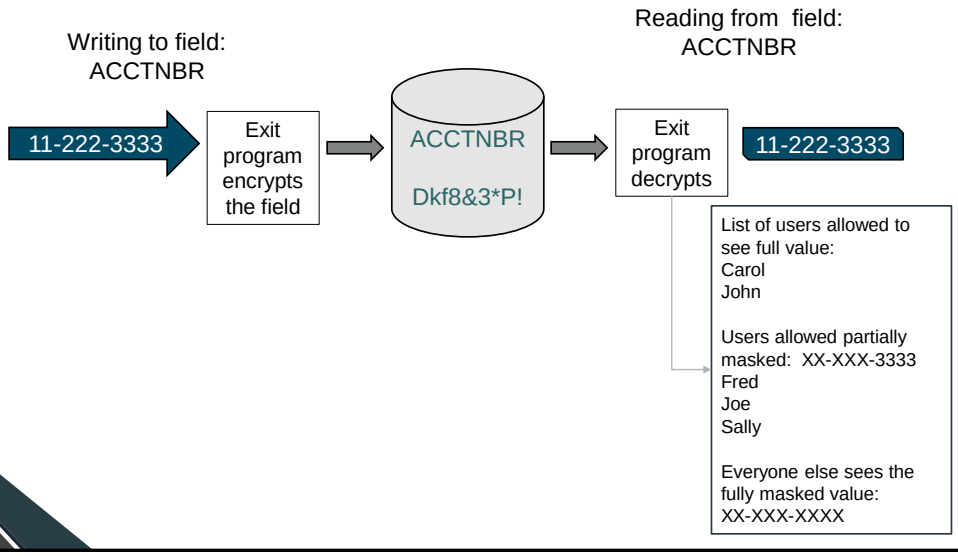
Field Procedures (FIELDPROC)

SQL programming enhancement:

- a FIELDPROC allows a user-written exit routine to be defined that will encrypt a field
  - No need to re-write an application to hold the encrypted field
    - Encrypted field is held 'internally'
  - Encryption is not provided by OS
- Values can be displayed as
  - Clear text
  - Partial mask support (for example - xxxx-xxxxxx-1003)
  - "Not authorized/Fully masked" (for example – zzzz-zzzzzzz-zzzzz)

23

Field Procedure Encryption / Decryption



24

24

Why are More Organizations Choosing to Encrypt?

- More types of data are being categorized as PII (Personally Identifiable Information)
- PCI DSS 4.0 clarifies that masking (e.g., RCAC masking) plus full disk encryption <> field encryption
- More organizations are choosing to encrypt at the field level because they see the value of protecting their data

25

Implementing Defense in Depth

- Multiple layers of defense:
  - Best practices for system values
    - Security level (QSECURITY)
    - Password level and composition rules (QPWDLVL and QPWDRULES)
  - Least privilege access assigned to User profiles
  - Deny by default object level authorities for both objects in libraries as well as directories
- Exit programs for more granular access controls
- Encryption additional control of who sees data (including the omission of *ALLOBJ users) and potential separation of duties

26

More Information

Ponemon Institute:

- The Cost of a Data Breach – 2022

Newsletters:

- Sans Newsbites
- SecurityWeek
- Dark Reading
- Bank Info Security

IBM i Security Administration and Compliance, 3nd edition, by Carol Woodbury, 2020, available from Amazon.com

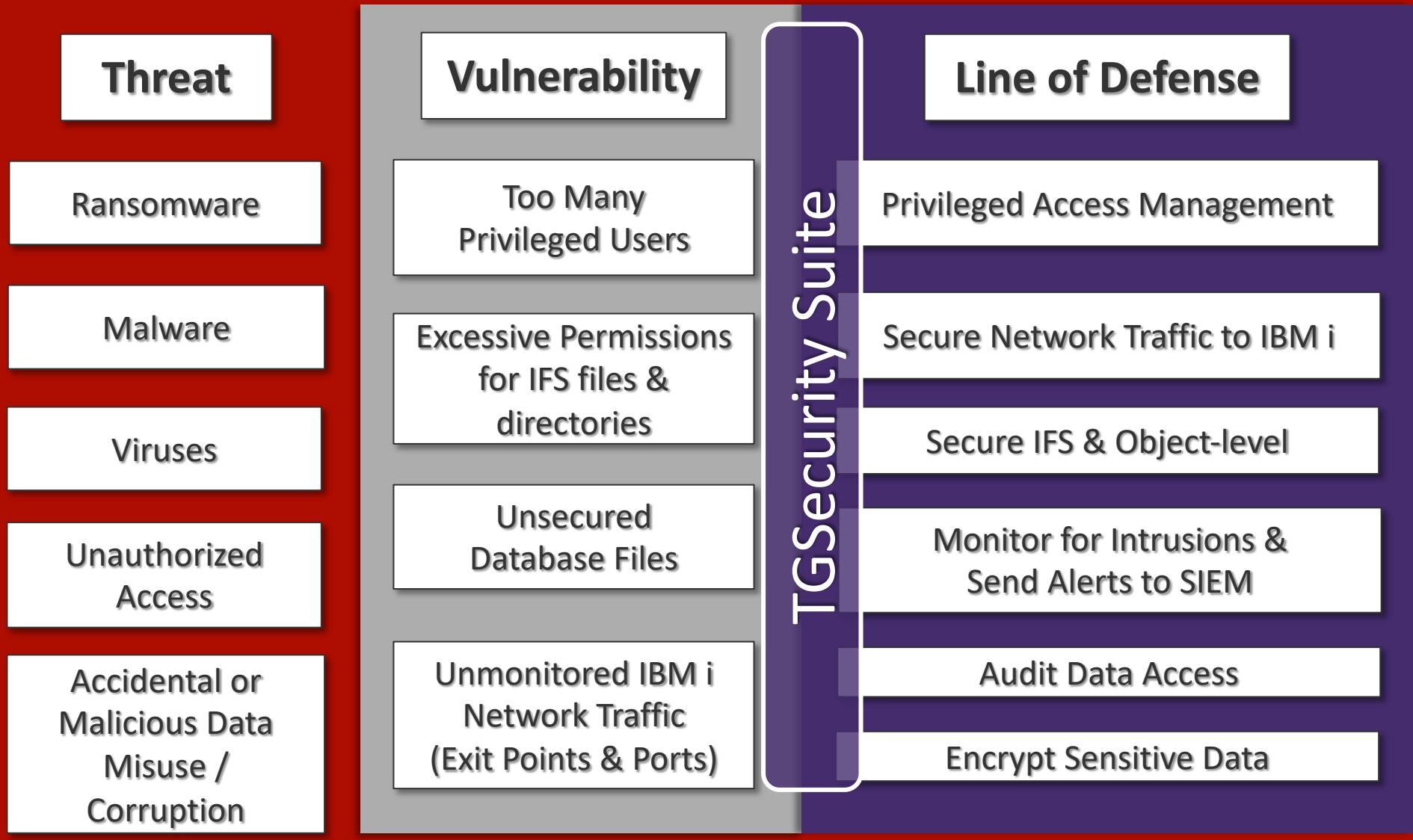
Mastering IBM i Security: A Step by Step Approach by Carol Woodbury, 2022, available from Amazon.com

27

Questions?

Contact: carol@DXRSecurity.com

28



TGEncrypt - Features

- Database Field-level Encryption
  - AES 256-Bit Encryption – standard recommended by NIST
  - Use TG internal keys or use existing keystore data to encrypt data
- Masking Field Data
  - Create your own mask for how end-users see sensitive data
- Scrambling Field Data
  - Scramble data based on internal TG scramble algorithm or customize your own algorithm

Contents of QGPL.CUSTOMER - Tgbld1(Seawolf)

	CUS_NO	CUS_NAME	CUS_SSN
1	111111111	James Bond	777-77-7777
2	222222222	Maggie Smith	666-66-6666
3	333333333	John Smith	555-55-5555

Contents of QGPL.CUSTOMER - Tgbld1(Seawolf)

	CUS_NO	CUS_NAME
1	111111111	òò¶□Õï‹ÆÔäç-f¹B□¶#rí)Ø/F!æSVAÿµ8ß§s¢BbÈGØ¾¼Q□□iå□-ëóx2"³P±{Íí□@}©JI8ØÃPÉ□#LO□ÏHéþN¹¾Ø□□²Åd³M
2	222222222	HòvN²²+¿ f¹B□¶#rí)Ø/F!æSVAÿµ8ß§s¢BbÈGØ¾¼Q□□iå□-ëóx2"³P±{Íí□@}©JI8ØÃPÉ□#LO□ÏHéþN¹¾Ø□□²Åd³M
3	333333333	ò¹¡□Z(□aù\ç-f¹B□¶#rí)Ø/F!æSVAÿµ8ß§s¢BbÈGØ¾¼Q□□iå□-ëóx2"³P±{Íí□@}©JI8ØÃPÉ□#LO□ÏHéþN¹¾Ø□□²Åd³M

Contents of QGPL.CUSTOMER - Tgbld1(Seawolf)

	CUS_NO	CUS_NAME	CUS_SSN
1	111111111	James Bond	XXX-XX-7777
2	222222222	Maggie Smith	XXX-XX-6666
3	333333333	John Smith	XXX-XX-5555

FRESCHE SOLUTIONS

TGEncrypt - Configuration

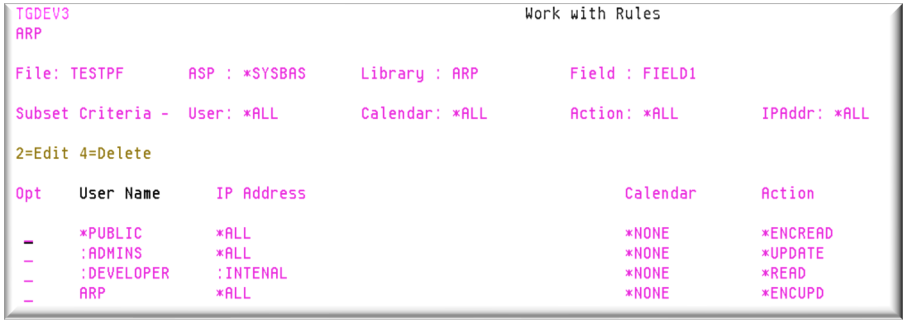
- Scan for sensitive data
  - Scan for data patterns
  - Scan for field types
  - Scan for field length

Sensitive Database Content

TGDEV3	ARP	2020-11-01	18:35:55

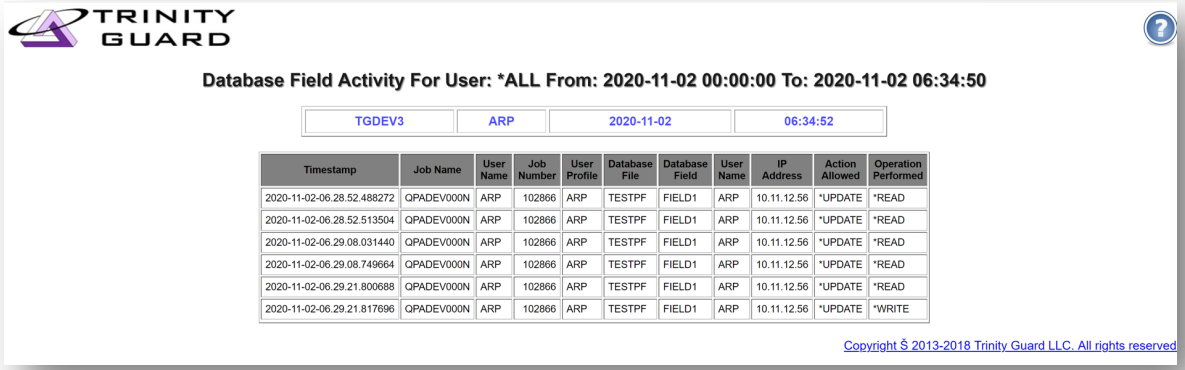
File Library	File Name	Field Name	Field Type	Field Length	Field Description	Type of Data Found
PSAUDIT	DDLF55B	WHSEQ	CHAR	13	Format level identifier	Credit Card
TGDATA	CMP00021F	UPMXSU	DECIMAL	15	Storage used	Credit Card
PSAUDIT	AALF2003	GHGSZ	DECIMAL	15	GROUP SIZE	Credit Card
PSAUDIT	AALF2003	GHGNO	DECIMAL	15	GROUP OBJ COUNT	Credit Card
TGDATA	CMP00610F	UPMXSU	DECIMAL	15	Storage used	Credit Card
PSAUDIT	AALF30A	MBDSZ2	DECIMAL	15	Data space size in bytes	Credit Card
PSAUDIT	AAPF75	CNT175	DECIMAL	15	COUNT 1	Credit Card
KAPILA	USRPRF	UPMXSU	DECIMAL	15	Storage used	Credit Card

- Field-level Role Based Access Control
  - Define who can view and edit data
  - Define how data is displayed
  - Use TGUser and TGNetwork Groups



TGEncrypt – Auditing and Alerting

- Audit Trail includes:
  - User Details
  - IP Address
  - Operation Performed
  - Operation Allowed
- Alert Integration
  - Track Critical Access
  - Real-time Alerts
  - Send Events to SIEM

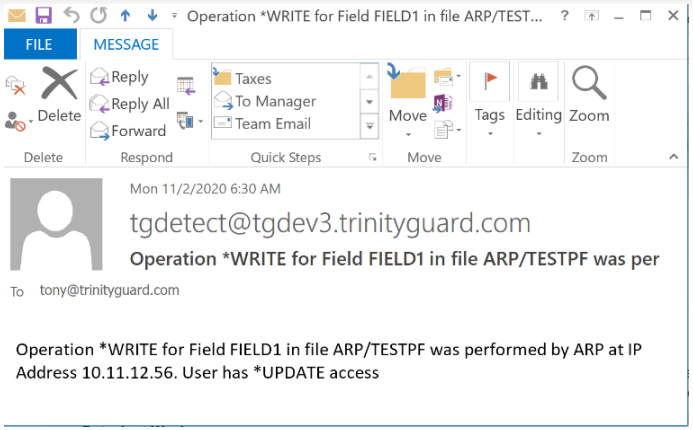


TRINITY GUARD

Database Field Activity For User: *ALL From: 2020-11-02 00:00:00 To: 2020-11-02 06:34:50

TGDEV3	ARP	2020-11-02	06:34:52

Timestamp	Job Name	User Name	Job Number	User Profile	Database File	Database Field	User Name	IP Address	Action Allowed	Operation Performed
2020-11-02-06.28.52.488272	QPADEV000N	ARP	102866	ARP	TESTPF	FIELD1	ARP	10.11.12.56	*UPDATE	*READ
2020-11-02-06.28.52.513504	QPADEV000N	ARP	102866	ARP	TESTPF	FIELD1	ARP	10.11.12.56	*UPDATE	*READ
2020-11-02-06.29.08.031440	QPADEV000N	ARP	102866	ARP	TESTPF	FIELD1	ARP	10.11.12.56	*UPDATE	*READ
2020-11-02-06.29.08.749664	QPADEV000N	ARP	102866	ARP	TESTPF	FIELD1	ARP	10.11.12.56	*UPDATE	*READ
2020-11-02-06.29.21.800688	QPADEV000N	ARP	102866	ARP	TESTPF	FIELD1	ARP	10.11.12.56	*UPDATE	*READ
2020-11-02-06.29.21.817696	QPADEV000N	ARP	102866	ARP	TESTPF	FIELD1	ARP	10.11.12.56	*UPDATE	*WRITE



Operation *WRITE for Field FIELD1 in file ARP/TEST...

FILE MESSAGE

Reply, Reply All, Forward, Delete, Taxes, To Manager, Team Email, Move, Tags, Editing, Zoom

Delete Respond Quick Steps Move Zoom

Mon 11/2/2020 6:30 AM

tgdetect@tgdev3.trinityguard.com

Operation *WRITE for Field FIELD1 in file ARP/TESTPF was per

To tony@trinityguard.com

Operation *WRITE for Field FIELD1 in file ARP/TESTPF was performed by ARP at IP Address 10.11.12.56. User has *UPDATE access

FRESCHE SOLUTIONS

Next Steps

- Explore options, discuss a project or validate your plans
- Strategy session with an IBM i security expert

Have a project in mind? Questions?

Let us know in the exit survey, or get in touch:

pauline.ayala@freschesolutions.com