Join the Guardiums of the Z Galaxy: Protecting Your Data on the Mainframe

Bern Lord
IBM, Cybersecurity Specialist

ECC 2023

Agenda

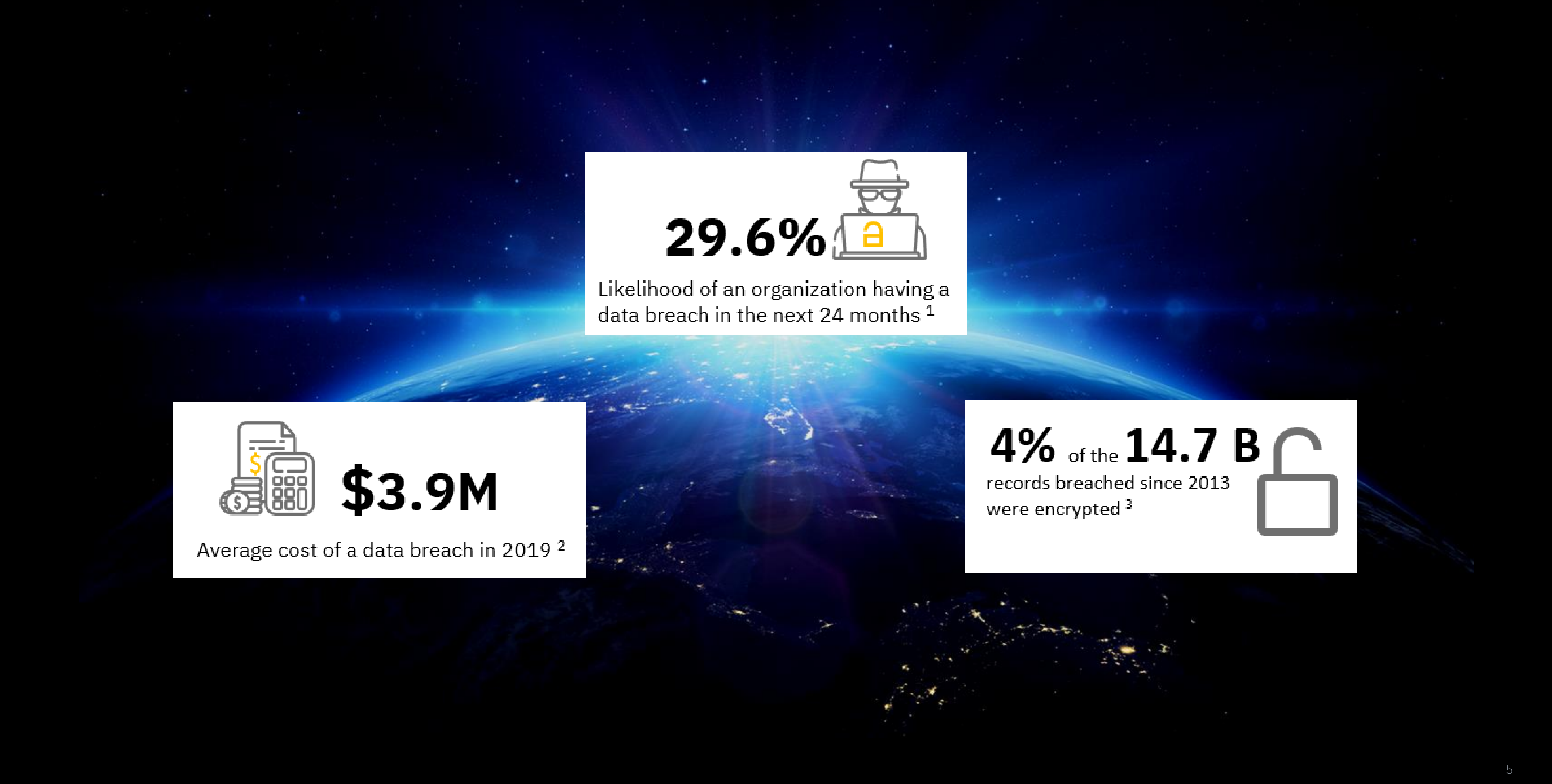
- The Threat Landscape
- Protecting critical assets
- Integrating with SIEM or SOC
- Call to Action

Threat Landscape

Is it Safe?

You need visibility more than ever!

“It’s no longer a matter of if, but when…”



29.6%

Likelihood of an organization having a data breach in the next 24 months [1]

$3.9M

Average cost of a data breach in 2019 [2]

4% of the **14.7 B** records breached since 2013 were encrypted [3]

Cyber Resiliency

***Cyber resiliency** refers to an organization's ability to continuously deliver the intended outcome, despite adverse cyber events*

The objective of cyber resilience is to maintain the organization's ability to deliver the intended outcome continuously

Cyber security is designed to protect systems, networks and data from cyber crimes

Effective cyber security reduces the risk of a cyberattack and protects organizations from the deliberate exploitation of its assets

+

Business continuity provides the capability to resume operations when an event causes a service disruption

Plans for Business continuity address natural catastrophes, accidents and deliberate physical attacks; but now, they must also support resumption of operations following cyberattack disruptions

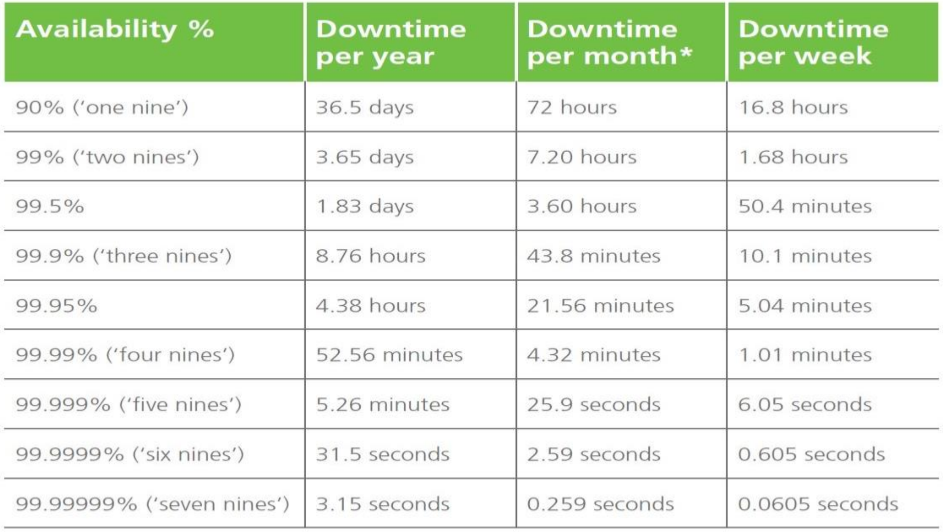
99.99% uptime is the new standard

38%

of clients surveyed in 2013 required 99.99% uptime

In 2019, that number rose to

85%



Availability %	Downtime per year	Downtime per month*	Downtime per week
90% ('one nine')	36.5 days	72 hours	16.8 hours
99% ('two nines')	3.65 days	7.20 hours	1.68 hours
99.5%	1.83 days	3.60 hours	50.4 minutes
99.9% ('three nines')	8.76 hours	43.8 minutes	10.1 minutes
99.95%	4.38 hours	21.56 minutes	5.04 minutes
99.99% ('four nines')	52.56 minutes	4.32 minutes	1.01 minutes
99.999% ('five nines')	5.26 minutes	25.9 seconds	6.05 seconds
99.9999% ('six nines')	31.5 seconds	2.59 seconds	0.605 seconds
99.99999% ('seven nines')	3.15 seconds	0.259 seconds	0.0605 seconds

Exacerbated Data Security Challenges for Organizations

Stop threats before they disrupt business

$5.52 M

Average total cost of a breach at enterprises of more than 25,000 employees

Achieve regulatory compliance

$255,626

Average cost increase of a breach due to compliance failure

Keep up with the sprawl of data

$267,469

Average cost increase of a breach due to extensive cloud migration

280 days Average time to detect (207) and contain (73) a data breach

Not protecting data is costly - Yet

56%

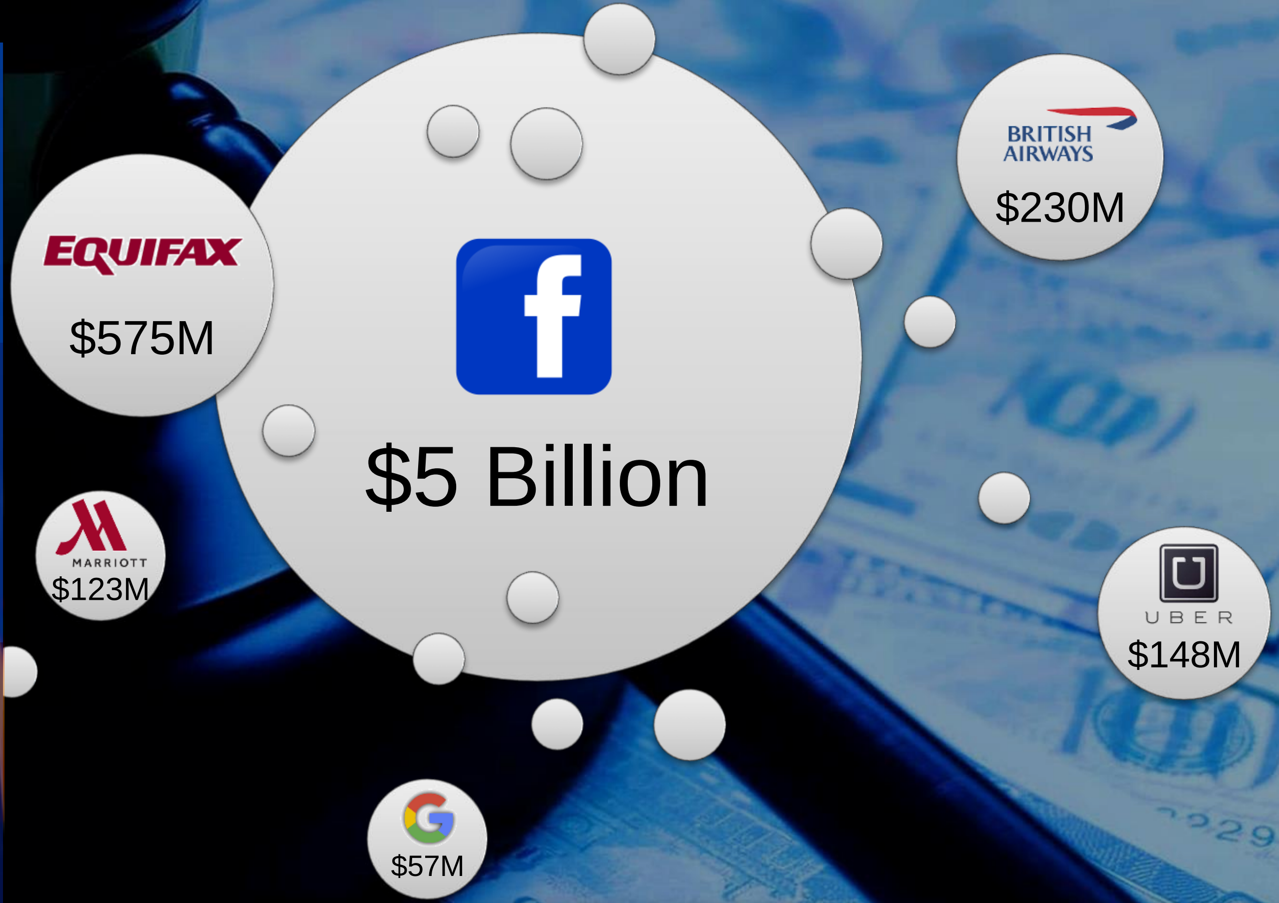
of organizations have experienced a significant security event in the past year

94%

know they have further to go to implement an effective data privacy solution

43%

sometimes have to take shortcuts when dealing with security issues



EQUIFAX $575M

$5 Billion

BRITISH AIRWAYS $230M

MARRIOTT $123M

UBER $148M

$57M

Protect Critical Assets

Defense in Depth – DB2, IMS, and VSAM Data

1. **First Layer – Encrypt Data at Rest**
   - Prevents access to dataset containers

   IBM Pervasive Encryption Dataset Feature

2. **Second Layer - Database Activity Monitoring**
   - This ensures each SQL statement is inspected, audited, and subject to security policy control

   IBM Security Guardium Database Activity Monitoring

3. **Third Layer - Audit Access to VSAM Datasets and System Datasets**

   IBM Security Guardium Datasets Activity Monitoring and zSecure Audit

4. **Fourth Layer - Implement Business Need-to-Know Control for Critical Data**
   - Limits access to only the data needed for a role

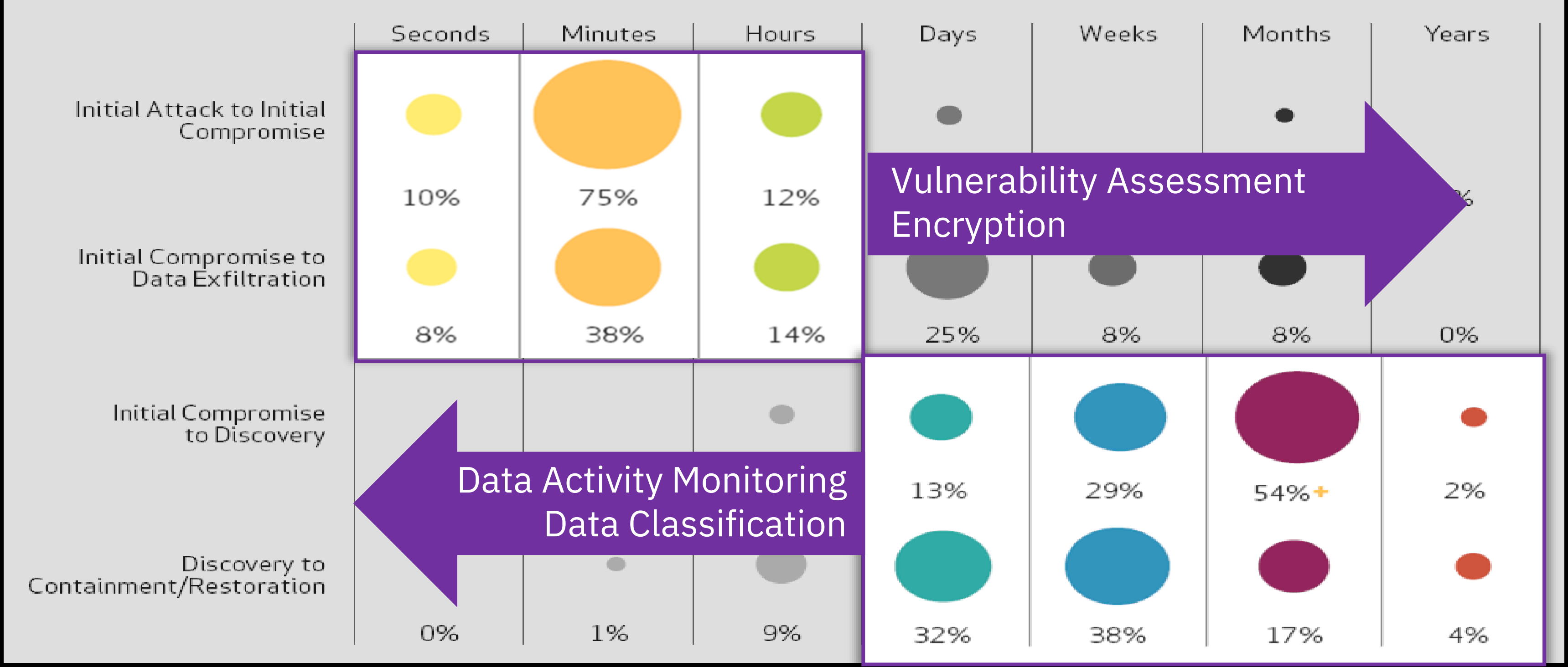
   DB2 10 Row masking

5. **Fifth Layer - Test Data Management and Generation**

   Optim TDM/ Data Privacy

Data Compromises Occur…QUICKLY!

*It takes days **or more** to discover compromises - and weeks **or more** to contain them.*

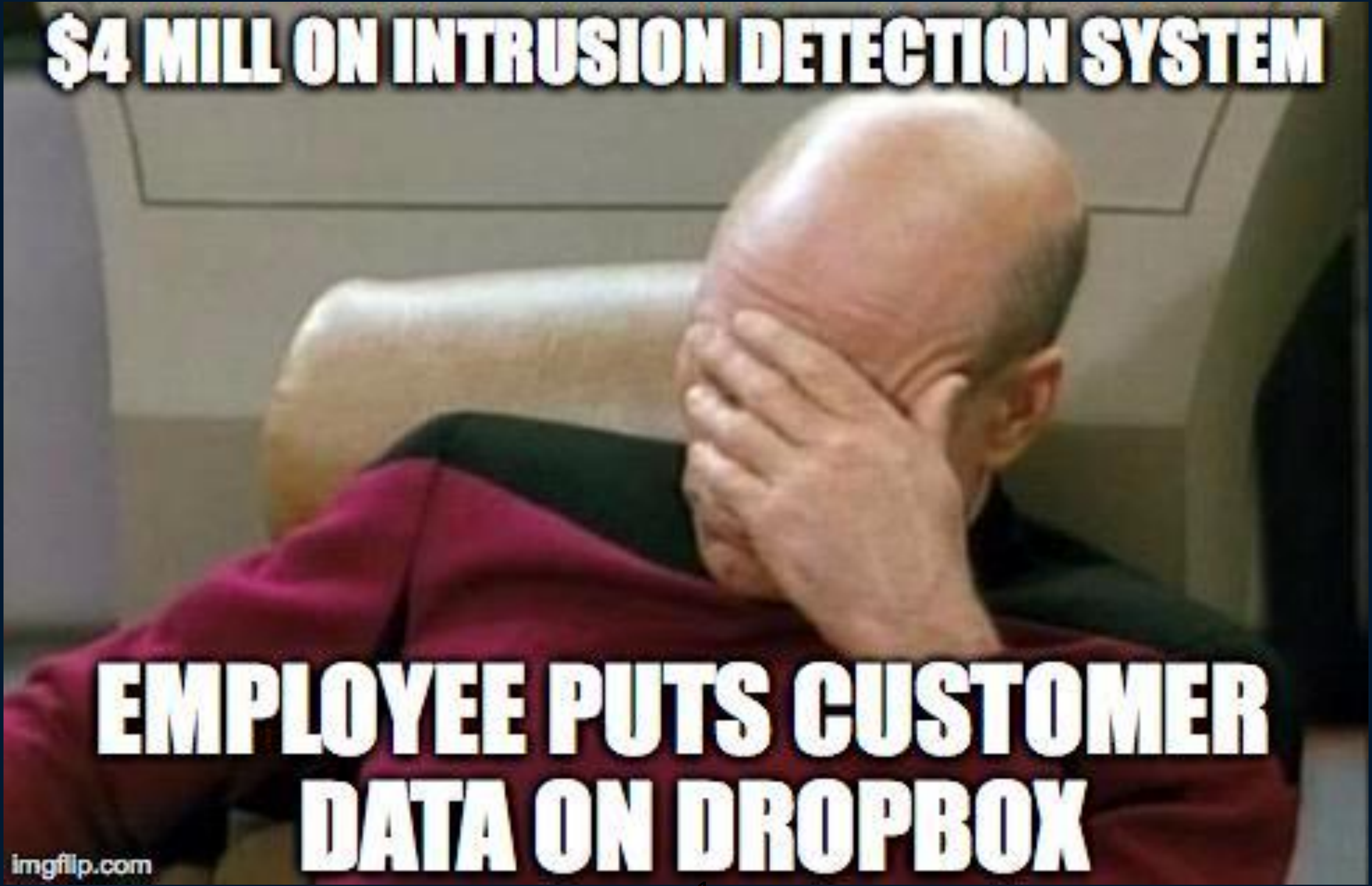


	Seconds	Minutes	Hours	Days	Weeks	Months	Years
Initial Attack to Initial Compromise	10%	75%	12%				%
Initial Compromise to Data Exfiltration	8%	38%	14%	25%	8%	8%	0%
Initial Compromise to Discovery				13%	29%	54%+	2%
Discovery to Containment/Restoration	0%	1%	9%	32%	38%	17%	4%

Vulnerability Assessment
Encryption

Data Activity Monitoring
Data Classification

Source: Verizon Data Breach Investigations Report

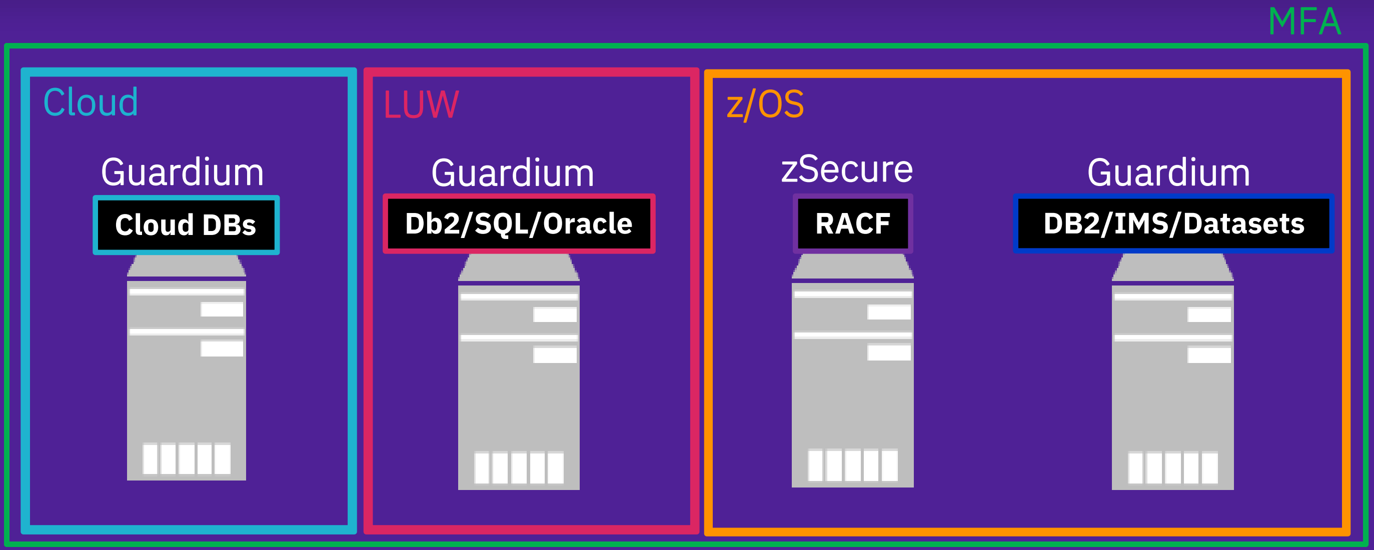

$4 MILL ON INTRUSION DETECTION SYSTEM
EMPLOYEE PUTS CUSTOMER DATA ON DROPBOX
imgflip.com

Integrate with SIEM or SOC

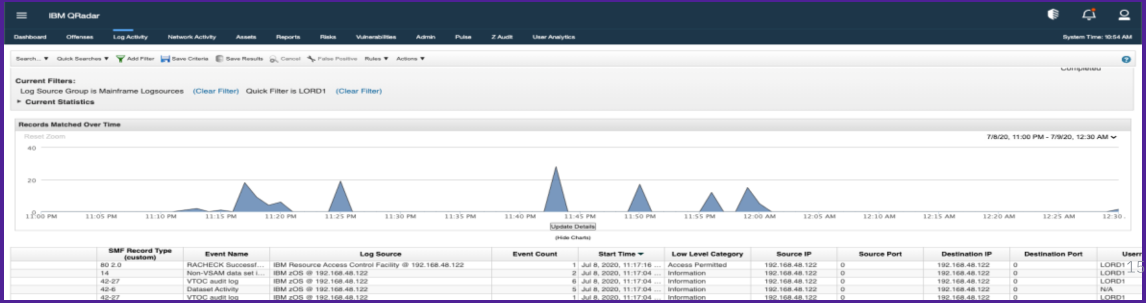
Holistic Security Picture

Environments & Data Sources

- Databases/Structured data ★
- Cloud
- Containers
- Big data/Semi-structured data
- Files/Unstructured data
- Mainframes ★
- Applications
- IoT



QRadar (SIEM)



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	User
	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

Call to Action

Start with the most securable platform

80% of the world’s corporate data is stored or originates on IBM z Systems

2/3 of business transactions for U.S. retail banks run directly on mainframes

Businesses that run on z Systems

- **92 of the top 100** worldwide banks
- **10 of the top 10** global life / health insurance providers
- **23 out of the 25** largest airlines

EAL5+ encryption and cryptographic hardware to secure data in motion and at rest

Run over a thousand virtual Linux images

- Virtualization of services for cloud implementations

5 minutes per year downtime of an application running on z Systems

Pervasive Encryption

Comply and Protect

Phase 1

Communicate, make security everyone’s business

Encrypt your most sensitive data

Monitor all Privileged User Activity

Implement Multi-Factor Authentication

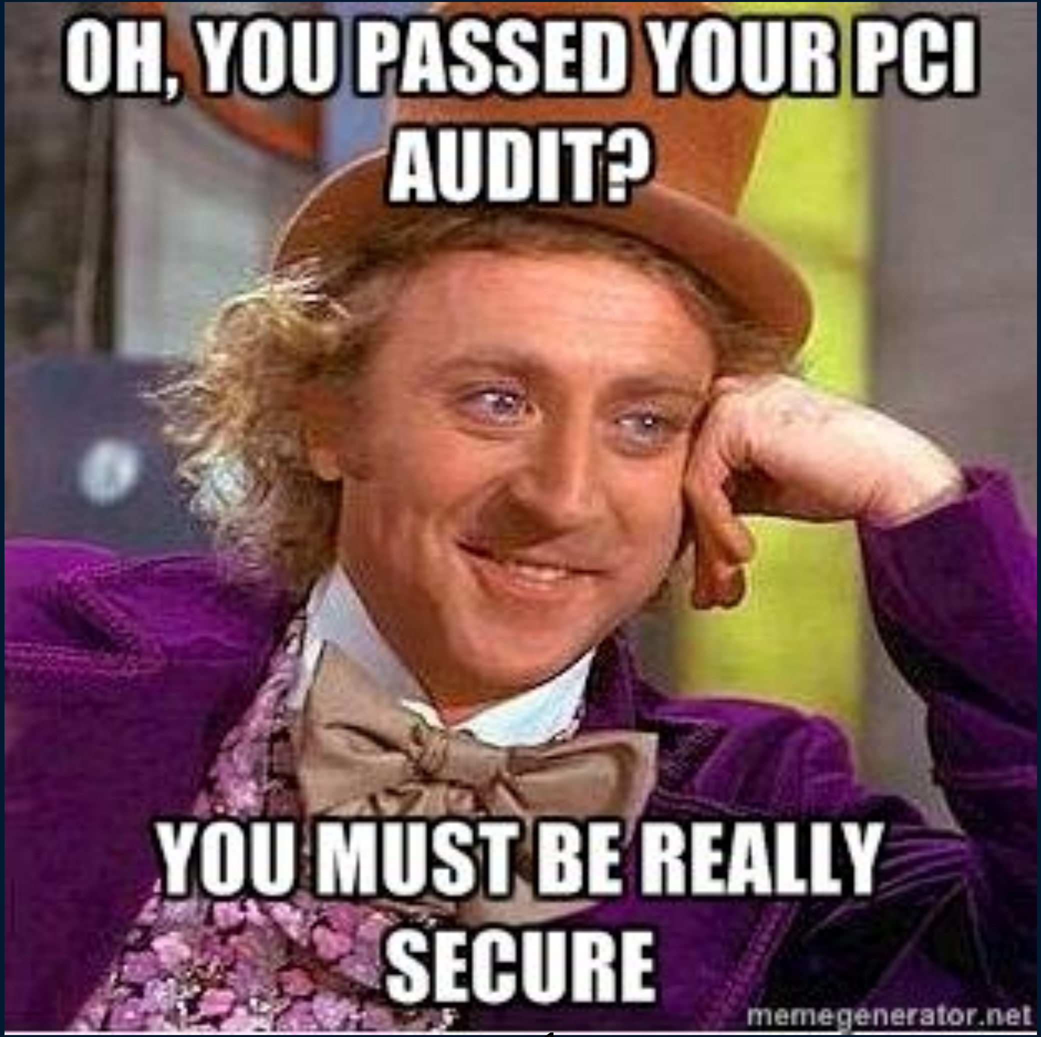
Ensure test data is sanitized

Test for Vulnerabilities

Phase 2

Monitor Sensitive Objects

Expand Encryption


OH, YOU PASSED YOUR PCI AUDIT?
YOU MUST BE REALLY SECURE
memegenerator.net

Monitoring Best Practices

Scalable, manageable processes for:

1. Aggregation
2. Remediation
3. Regular reviewal of data activity
4. Regular reviewal of STAP health

Documented processes for:

1. Installing upgrades
2. Installing patches
3. Backup of data
4. Backup of configuration

Architectural Concerns:

1. Maintain diagrams of infrastructure
2. Stress test
3. Functioning HA/DR

Leverage Guardium Capabilities:

1. SIEM Integration
2. Ticketing Service Integration
3. Roles and security profiles
4. External Authentication

IBM Security Community

8,000 Members Strong and Growing Every Day!

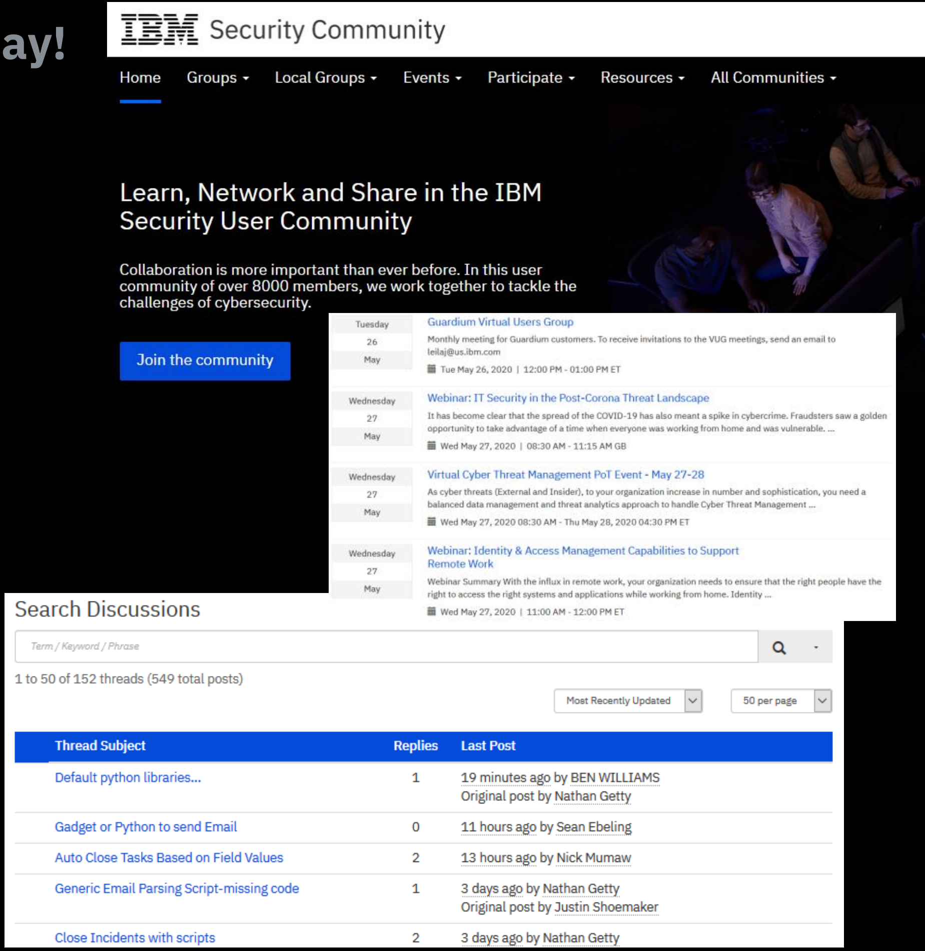
Sign up: https://community.ibm.com/security

User Group Day discussion: https://ibm.biz/zsecure-usergroupday (share feedback, ask questions and continue the conversation after this session!)

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

1 to 50 of 152 threads (549 total posts)

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

Notices and disclaimers

U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed "as is" without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those

customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

Notices and disclaimers

- Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**

- The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

- IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml