

Mainframe SMF event integration with SIEM Tool

David Z. Rossi

Cybersecurity Architect

IBM Z

dzrossi@us.ibm.com

IBM Z

© 2017 IBM Corporation

you ^{IBM}

Equifax Announces Cybersecurity Incident Involving Consumer

No Evidence of Unauthorized Access to Core Consumer or Commercial Credit Reporting Databases

Company to Offer Free Identity Theft Protection and Credit File Monitoring to All U.S. Consumers

September 7, 2017 — Equifax Inc. (NYSE: EFX) today announced a cybersecurity incident potentially impacting approximately 143 million U.S. consumers. Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017. The company has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases.

The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed. As part of its investigation of this application vulnerability, Equifax also identified unauthorized access to limited personal information for certain UK and Canadian residents. Equifax will work with UK and Canadian regulators to determine appropriate next steps. The company has found no evidence that personal information of consumers in any other country has been impacted.





2017 Cost of Data Breach Study

Global Overview

Benchmark research sponsored by IBM Security

Independently conducted by Ponemon Institute LLC

June 2017

*** David Rossi's back of napkin calculations

Controls that reduce cost of data breach

13 % Incident Response

11% Extensive use of Encryption

Incident response teams and the extensive use of encryption reduce costs. In this year's research, an incident response (IR) team reduced the cost by as much as \$19 per compromised record. Hence, companies with a strong IR capability would anticipate an adjusted cost of \$122 (\$141-\$19 per record). Similarly, the extensive use of encryption reduced cost by \$16 per capita, with an adjusted average cost of \$125 (\$141-\$16) per record.

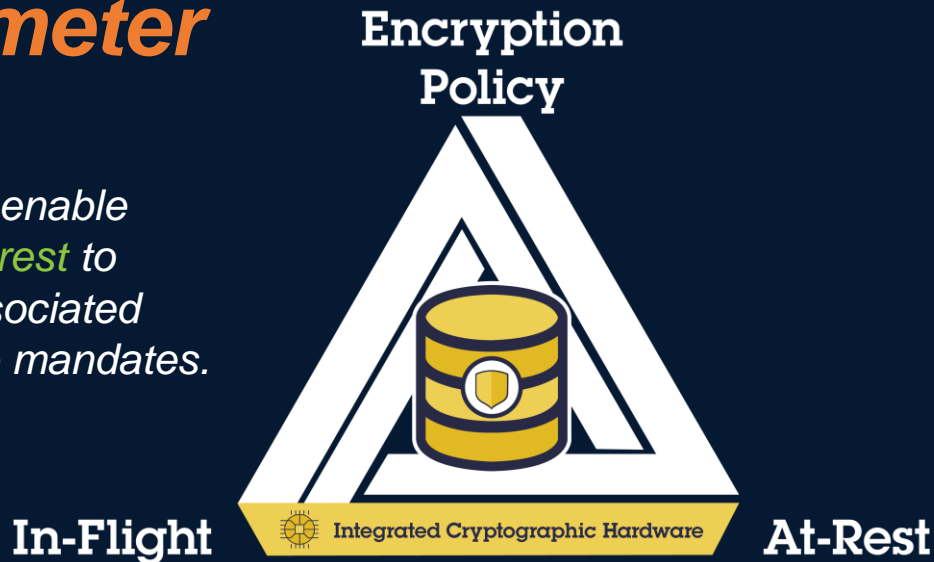


IBM Z Pervasive Encryption

A Data Centric Approach to Information Security

Data is the new perimeter

A *transparent* and consumable approach to enable extensive encryption of data *in-flight* and *at-rest* to substantially simplify & reduce the costs associated with protecting data & achieving compliance mandates.





Pervasive Encryption with IBM Z

Enabled through tight platform integration

Full Disk
Encryption



Full disk encryption utilizes encrypting disk drives that protect data at rest when disk drives are retired, sent for repair or repurposed

Integrated Crypto
Hardware



Hardware accelerated encryption on every core – CPACF

PCIe Hardware Security Module (HSM) & Cryptographic Coprocessor – Crypto Express5S

Network
Encryption



Protect network traffic using standards based encryption from end to end, including encryption readiness technology² to ensure that z/OS systems meet approved encryption criteria

Data Set & File
Encryption



Protect Linux file systems and z/OS data sets¹ using policy controlled encryption that is transparent to applications and databases

Coupling
Facility



Protect z/OS Coupling Facility² data end-to-end, using encryption that's transparent to applications

Secure Service
Container



Secure deployment of software appliances including tamper protection during installation and runtime, restricted administrator access, and encryption of data and code in-flight and at-rest








1 Statement of Direction* in the z/OS Announcement Letter (10/4/2016) - <http://ibm.co/2ldwKoC>

2 IBM z/OS Version 2 Release 3 Preview Announcement Letter (2/21/2017) - <http://ibm.co/2l43ctN>




* All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

IBM Security Strategy

SUPPORT
the CISO agenda

- Advanced Threats 
- Cloud 
- Mobile and Internet of Things 
- Compliance Mandates 
- Skills Shortage 

ACCELERATE
with key innovation

- Cognitive 
- Cloud 
- Collaboration 

LEAD
in strategic domains

Security Transformation Services

Management Consulting | Systems Integration | Managed Security

Security Operations and Response			Information Risk and Protection		
Incident Response			Cloud Security		Mobile Security
Security Intelligence and Analytics			Identity Governance and Access Management		
Vulnerability and Patch Management	Endpoint and Network Protection	User Behavior Analytics	Data Protection	Application Security	Advanced Fraud Prevention

Security Research and Threat Intelligence

Common Drivers

Security analytics

Privileged user management

Access management

User behavior analytics

Data access control

Incident response

Data protection

Endpoint patching and management

Fraud protection

Identity governance and administration

Network visibility and segmentation

Mainframe security

Network forensics and threat management

Vulnerability management

IDaaS

Malware protection

Firewalls

Device management

Application scanning

Application security management

Sandboxing

Virtual patching

Transaction protection

Criminal detection

Content security

Endpoint detection and response

Indicators of compromise

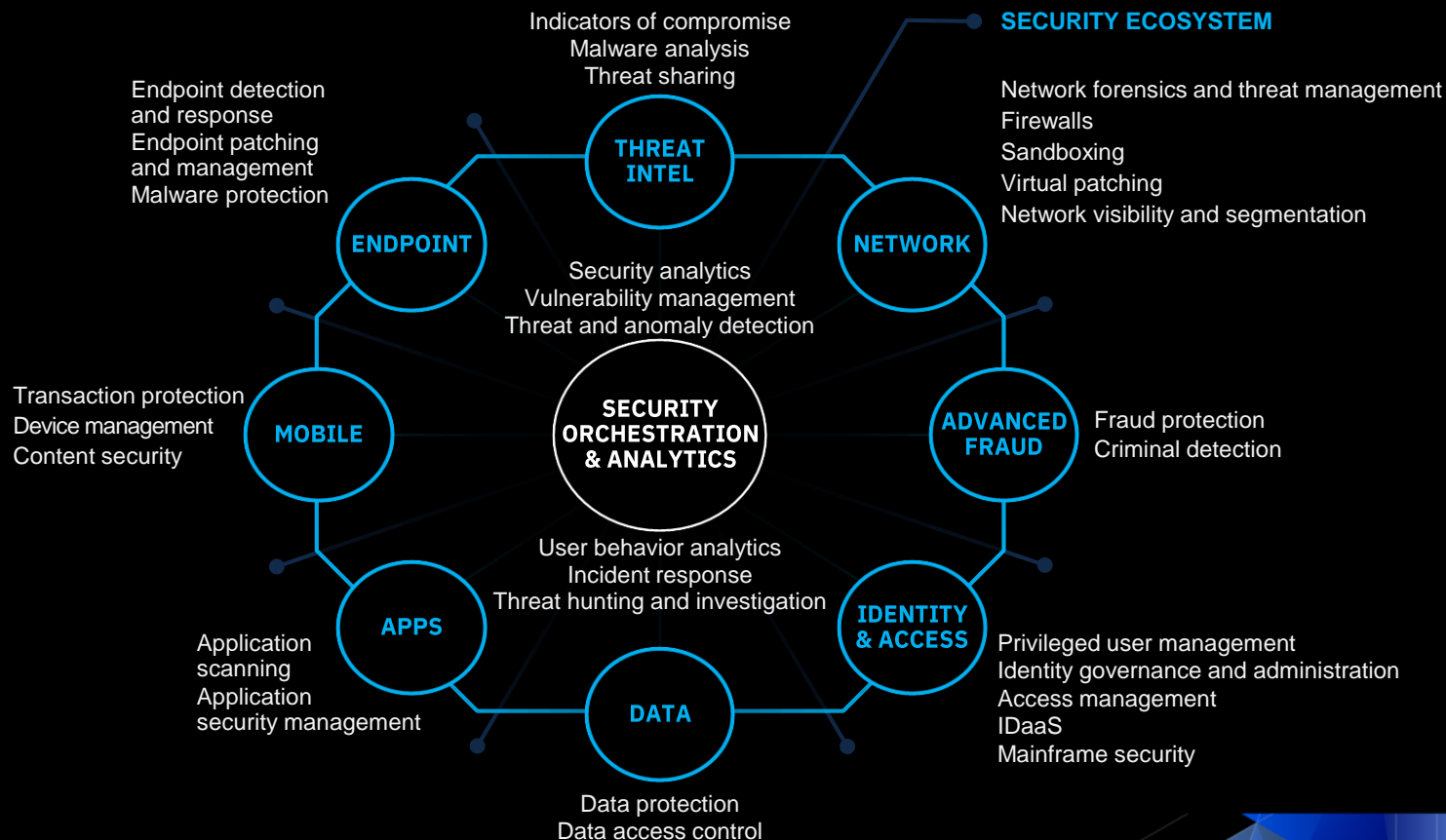
Threat and anomaly detection

Threat sharing

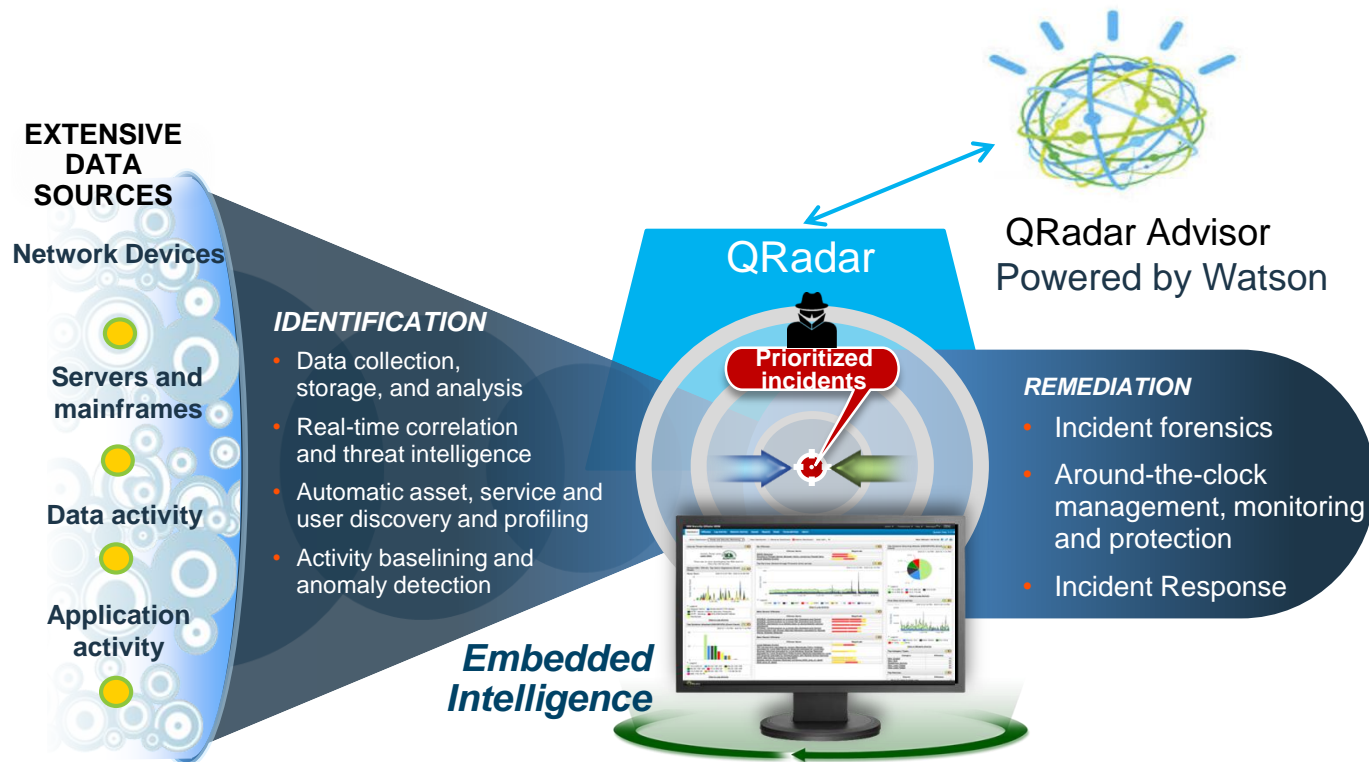
Malware analysis

Threat hunting and investigation

An integrated and intelligent security immune system



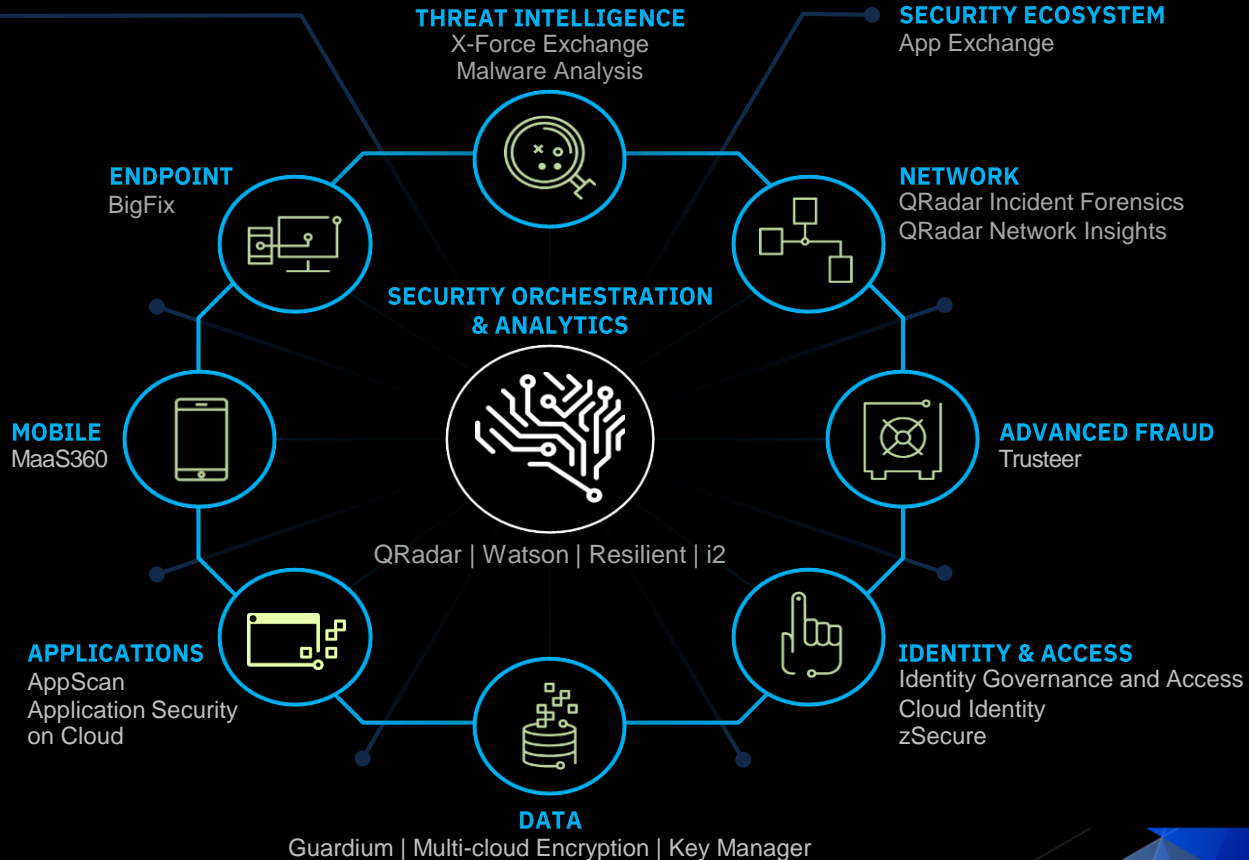
Enterprise Security Intelligence and Analytics Strategy



IBM Security Immune System

SECURITY TRANSFORMATION SERVICES

- Consulting & Systems Integration
- Managed Security
- Cloud Security



Base Insider Threat Monitoring Use Cases

CISO's Security Analytics QRadar is focused on Insider Threat monitoring following ITSS standard. CISO's main goal is to detect and respond to insider threats.

1. Multiple users access sensitive data
2. Privileged user access sensitive data
3. Successful login from multiple locations
4. Audit logs are not being generated
5. Audit logs are not being stored
6. User access to sensitive data is not being monitored
7. User access to sensitive data is not being logged
8. Direct access to sensitive data is not being monitored
9. Global access to sensitive data is not being monitored
10. Local Privileged account was created or modified
11. Crown Jewel system does not send logs for one hour

Although Important event based monitoring is compliance driven. It does not help CISO organization understand RISK or Provide enough details for forensics and incident response

Security Intelligence

Requirements

- Collector of Flows
- Collector of Events
- Search
- Rules
- Analytics
- Cognitive
- Reporting
- Real Time



Market shift from compliance to risk based focused. Real time meaningful feeds mandatory

Sample SMF Records to collect.

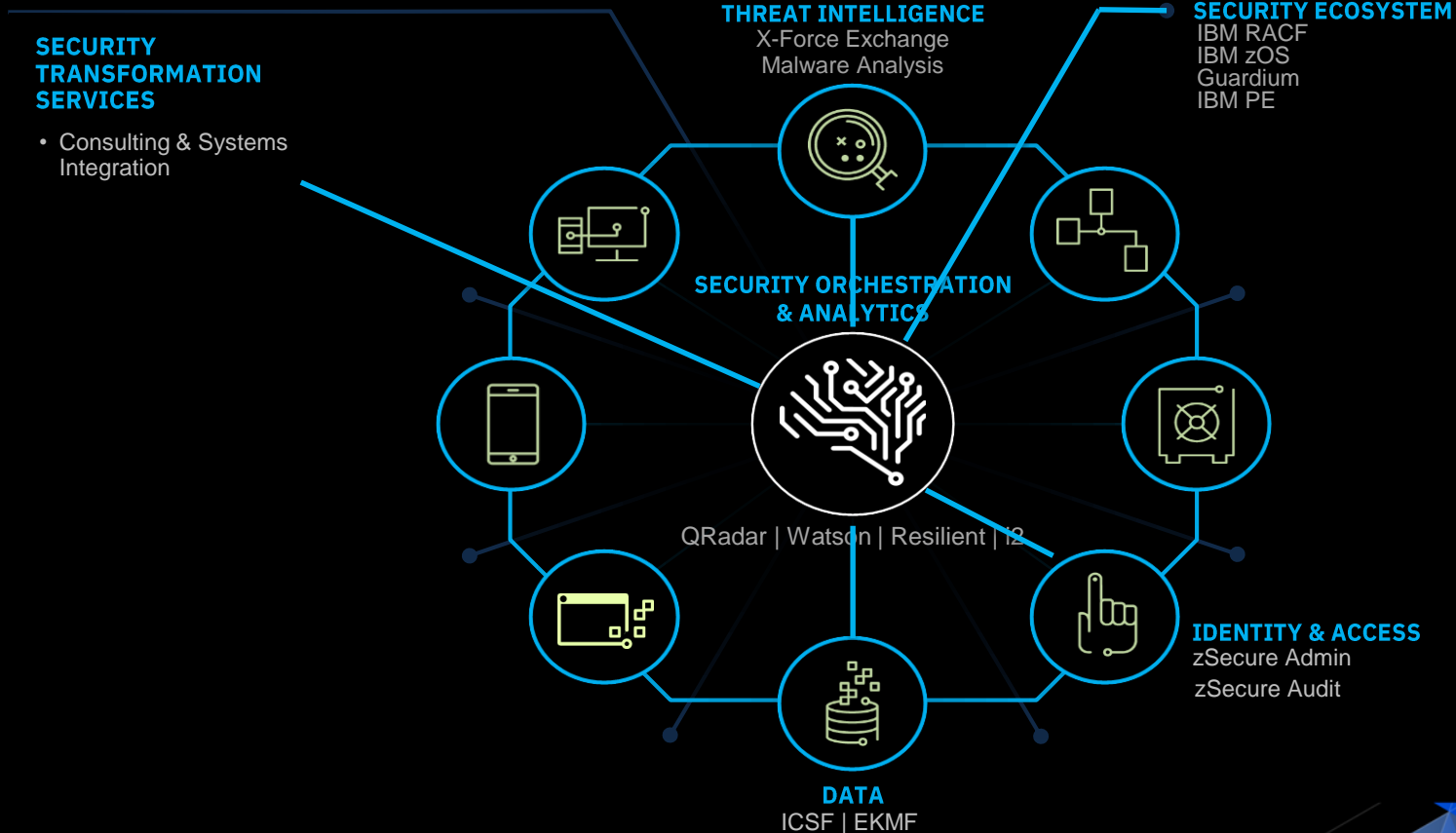
SMF Type	Sub-type	Required	Recommended
Record Type 14	--- INPUT or RDBACK Data Set Activity	yes	
Record Type 15	--- OUTPUT, UPDAT, INOUT, or OUTIN Data Set Activity	yes	
Record Type 30	--- Common address space work		
	1 Job start or start of other work unit	yes	
	2 Activity since previous interval ended		yes
	3 Activity for the last interval before step termination		yes
	4 Step total		yes
	5 Job termination or termination of other work unit	yes	
	6 System address space, which did not go through full function start.		yes
Record Type 42	-- DFSMS statistics and configuration		
	6 records DASD data set level I/O statistics		yes
Record Type 60	--- VSAM Volume Data Set Updated	yes	
Record Type 61	--- ICF Define Activity	yes	
Record Type 62	--- VSAM Component or Cluster Opened	yes	
Record Type 64	--- VSAM Component or Cluster Status		yes
Record Type 65	--- ICF Delete Activity	yes	
Record Type 66	--- ICF Alter Activity	yes	
Record Type 80	--- Security Product Processing	yes	
Record Type 81	--- RACF Initialization	yes for RACF	
Record type 92	--- File system activity		
	1 file system is mounted.	yes	
	2 file system is quiesced (or suspended).		yes
	4 file system is unquiesced (or resumed).		yes
	5 file system is unmounted.	yes	
	6 file system is remounted.		yes
	7 file system is moved.		yes
	10 file is opened.	yes	
	11 file is closed.	yes	
	12 MMAP subtype information.		yes
	13 MUNMAP subtype information.		yes
	14 file or file directory is deleted or renamed.	yes	
	15 file's security attributes for APF authorized, program control, or shared library are changed.	yes	
	16 socket, character special file, pipe, or fifo is closed.	yes	
	17 how many times a file is accessed throughout the life of an open and is written on the SMF global recording interval.		yes

Record Type 119

---	TCP/IP Statistics		
1	TCP connection initiation record (subtype 1)		yes
2	TCP connection termination record (subtype 2)		yes
3	FTP client transfer completion record (subtype 3)		yes
4	TCP/IP profile event record (subtype 4)		yes
5	TCP/IP statistics record (subtype 5)		yes
6	Interface statistics record (subtype 6)		yes
7	Server port statistics record (subtype 7)		yes
8	TCP/IP stack start/stop record (subtype 8)		yes
10	UDP socket close record (subtype 10)		yes
11	zERT connection detail record		yes
20	TN3270E Telnet server SNA session initiation record (subtype 20)		yes
21	TN3270E Telnet server SNA session termination record (subtype 21)		yes
22	TSO Telnet client connection initiation record (subtype 22)		yes
23	TSO Telnet client connection termination record (subtype 23)		yes
24	Telnet profile configuration		yes
32	DVIPA status change record (subtype 32)		yes
33	DVIPA removed record (subtype 33)		yes
34	DVIPA target added record (subtype 34)		yes
35	DVIPA target removed record (subtype 35)		yes
36	DVIPA target server started record (subtype 36)		yes
37	DVIPA target server ended record (subtype 37)		yes
41	SMC-R link group statistics record (subtype 41)		yes
42	SMC-R link state start record (subtype 42)		yes
43	SMC-R link state end record (subtype 43)		yes
44	RDMA network interface card (RNIC) interface statistics record (subtype 44)		yes
48	CSSMTP configuration record (CONFIG subtype 48)		yes
49	CSSMTP connection record (CONNECT subtype 49)		yes
50	CSSMTP mail record (MAIL subtype 50)		yes
51	CSSMTP spool file record (SPOOL subtype 51)		yes
52	CSSMTP statistical record (STATS subtype 52)		yes
70	FTP server transfer completion record (subtype 70)		yes
71	FTP daemon configuration record (subtype 71)		yes
72	FTP server logon failure record (subtype 72)		yes
73	IPSec IKE tunnel activation and refresh record (subtype 73)		yes
74	IPSec IKE tunnel deactivation and expire record (subtype 74)		yes
75	IPSec dynamic tunnel activation and refresh record (subtype 75)		yes
76	IPSec dynamic tunnel deactivation record (subtype 76)		yes
77	IPSec dynamic tunnel added record (subtype 77)		yes
78	IPSec dynamic tunnel removed record (subtype 78)		yes
79	IPSec manual tunnel activation record (subtype 79)		yes
80	IPSec manual tunnel deactivation record (subtype 80)		yes
94	OpenSSH Client Connection Started		yes
95	OpenSSH Server Connection Started		yes
96	OpenSSH Server Transfer Completion		yes

DEMO

IBM Security Immune System Applied to Pervasive Encryption



SOC view of Near Real Time Feeds

Event Information

Event Name	RACHECK Successful access				
Low Level Category	Access Permitted				
Event Description	RACHECK Successful access				
Magnitude	1	Relevance	1	Severity	0
Username	U010010				
Start Time	Nov 8, 2017, 12:46:48 PM	Storage Time	Nov 8, 2017, 12:46:48 PM	Log Source Time	Nov 8, 2017, 11:51:54 AM
Access allowed (custom)	READ				
Access intent (custom)	READ				
Application name (custom)	N/A				
Authenticator (custom)	N/A				
Command (custom)	N/A				
Data set name (custom)	N/A				
Descriptor (custom)	Success				
Event Summary (custom)	RACF ACCESS success for U010010: (READ,READ) on FACILITY FPZ.ACCELERATOR.COMPRESSION				
Identity Context name (custom)	N/A				
Identity Context registry (custom)	N/A				
Job name (custom)	U010010				
Log string (custom)	N/A				
Person name (custom)	TESTER				
Physical DASD box serial (custom)	N/A				
Port of entry (custom)	N/A				
Private/owned data set (custom)	N/A				
RACF authority used (custom)	Normal				
RACF profile (custom)	FPZ.ACCELERATOR.COMPRESSION				
Resource sensitivity (custom)	N/A				
SAF Class (custom)	FACILITY				
SAF resource name (custom)	FPZ.ACCELERATOR.COMPRESSION				
SERVAUTH IP (custom)	N/A				
SMF Record Type (custom)	80 2.0				

Connection Details

Status: At Risk



ConnectionID	00104BEE
Event Time	10:29:59 AM
Sysplex	UTCPLXJ8
System	JB0
User	DBWGSYS
Source IP	192.168.25.33
Source Port	8892
Remote IP	9.12.17.92
Remote Port	447
Protocol Version	None
Negotiated Cipher Suite	
Encryption Algorithm	
Key Exchange Algorithm	*
Message Authentication Algorithm	
Server Cert Signature Method	*
Client Cert Signature Method	

IBM QRadar Security Intelligence

Dashboard Offenses Log Activity Network Activity Assets

IBM QRadar Z Security Suite

- Network
- Storage
- Reports
- Analytics

System Time: 10:30 AM

Last Updated: Wed Nov 8 15:34:46 2017

90.7%

10:33:30 AM

Search:

Protocol Version

- TLSv1.0
- TLSv1.0
- TLSv1.0
- TLSv1.0
- TLSv1.0

Close

Network

Storage

Reports

Analytics

Dataset Security Dashboard

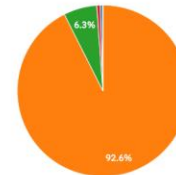
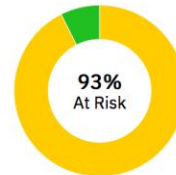
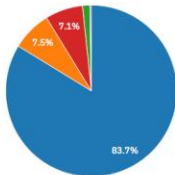
Overview

Last Updated: Wed Nov 8 16:58:33 2017

Dataset Events - System

Dataset Encryption Status

Dataset Security - Key Label



Dataset Events

Total Results: 10000 - Filters: | Time Range: Last 8 Hours |

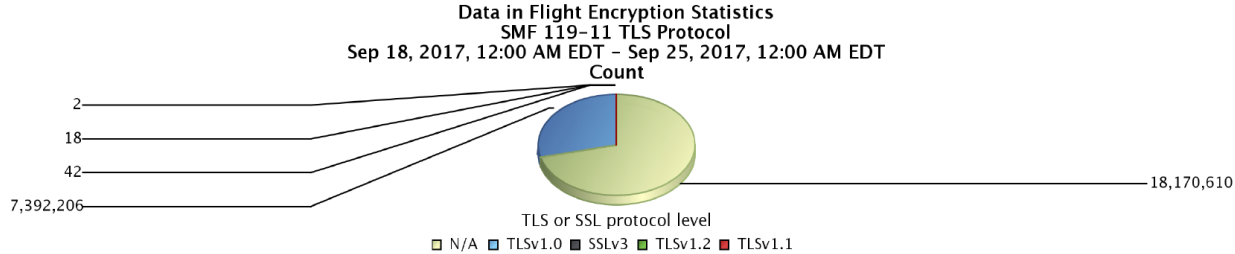
Secure		Total		At Risk	
Dataset Name	Event Time	System	User	SAF Profile	Key Label
DSNDBWG.DBWD.ARCLG1.D17312.T1200215.80022012	11:55:23 AM	J00	DBWGSYS	DSNDBWG*.ARCLG**	None
DSNDBWG.DBWD.ARCLG1.D17312.T1200215.A0022012	11:55:38 AM	J00	DBWGSYS	DSNDBWG*.ARCLG**	None
DSNDBWG.DBW6.ARCLG1.D17312.T1004453.80037586	09:59:47 AM	J00	DBWGSYS	DSNDBWG*.ARCLG**	None
DSNDBWG.DBW4.BSDS01	11:42:31 AM	J00	DBWGSYS	DSNDBWG*.BSDS*	None
DSNDBWG.DBW4.BSDS01	11:42:32 AM	J00	DBWGSYS	DSNDBWG*.BSDS*	None
DB2.V12.PLX1.SETA.SDXRRESL	04:58:52 AM	J00	DBWGSYS	DB2**	None
CANDLE.PLEX1.OMPES4.JDS4RTE.DBWD.RKD2VS01	09:59:32 AM	J00	OMEGADM	CANDLE**	None
CANDLE.PLEX1.OMPES4.JAS4RTE.DBW3.RKD2VS02	11:56:15 AM	J00	OMEGADM	CANDLE**	None

Showing 1 to 8 of 8 entries (filtered from 10,000 total entries)

Previous 1 Next

zERT Summary Report

Generated: Sep 28, 2017, 3:37:28 PM



Encryptions Protocols in Use

SMF 119-11 TLS Protocol

Sep 18, 2017, 12:00:00 AM - Sep 25, 2017, 12:00:00 AM

TLS or SSL protocol level (custom)	TLS Algorithm (custom) (Unique Count)	TLS Channel (custom) (Unique Count)	TLS key length (custom) (Unique Count)	TLS message digest (custom) (Unique Count)	Count
N/A	Multiple (3)	Multiple (3)	Multiple (4)	None	18,170,610
TLSv1.0	AES	CBC	Multiple (2)	HMAC-SHA1	7,392,206
SSLv3	Multiple (2)	None	Multiple (2)	Multiple (2)	42
TLSv1.2	AES	CBC	128	Multiple (2)	18
TLSv1.1	AES	CBC	256	HMAC-SHA1	2

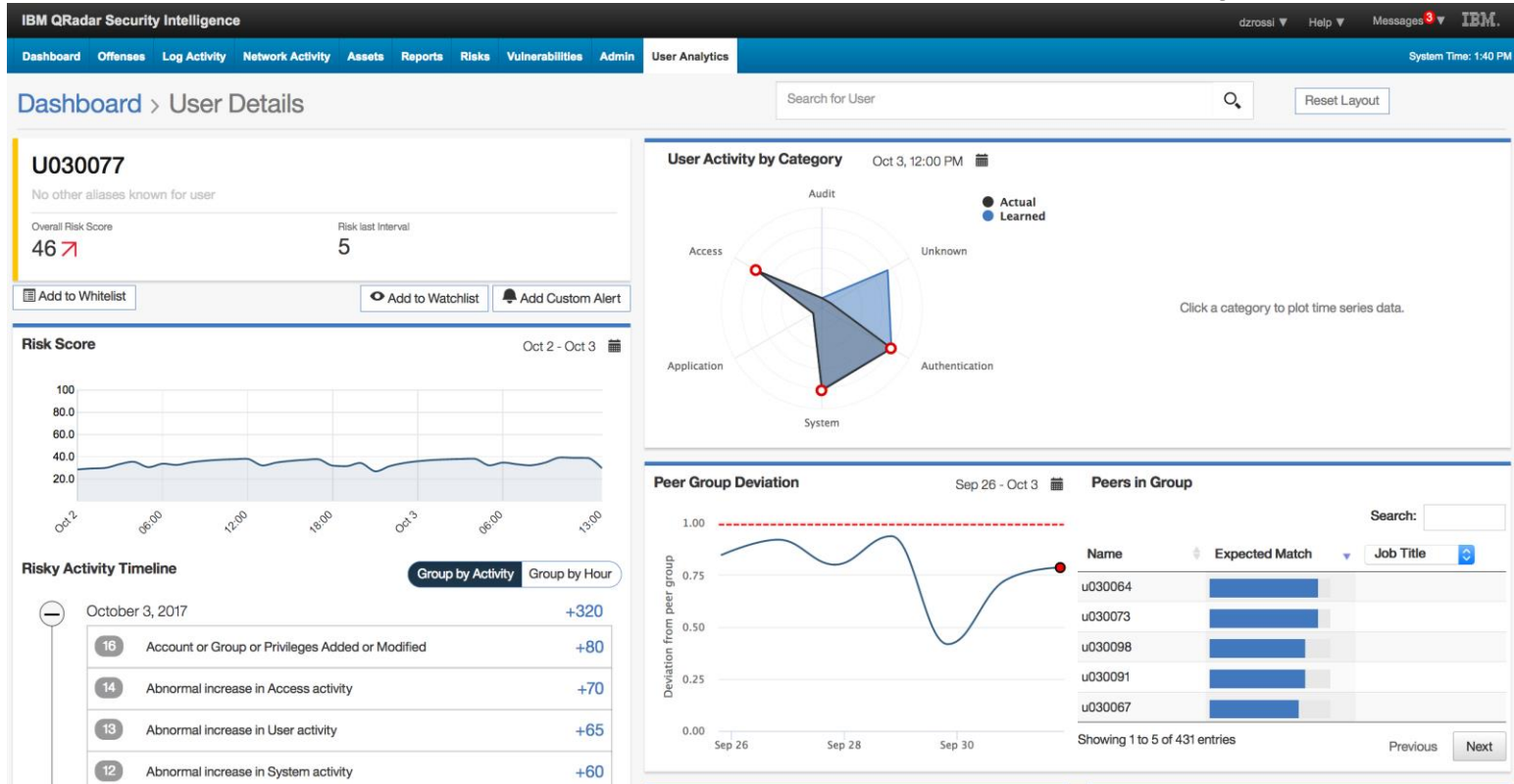
Log Sources sending zERT statistics

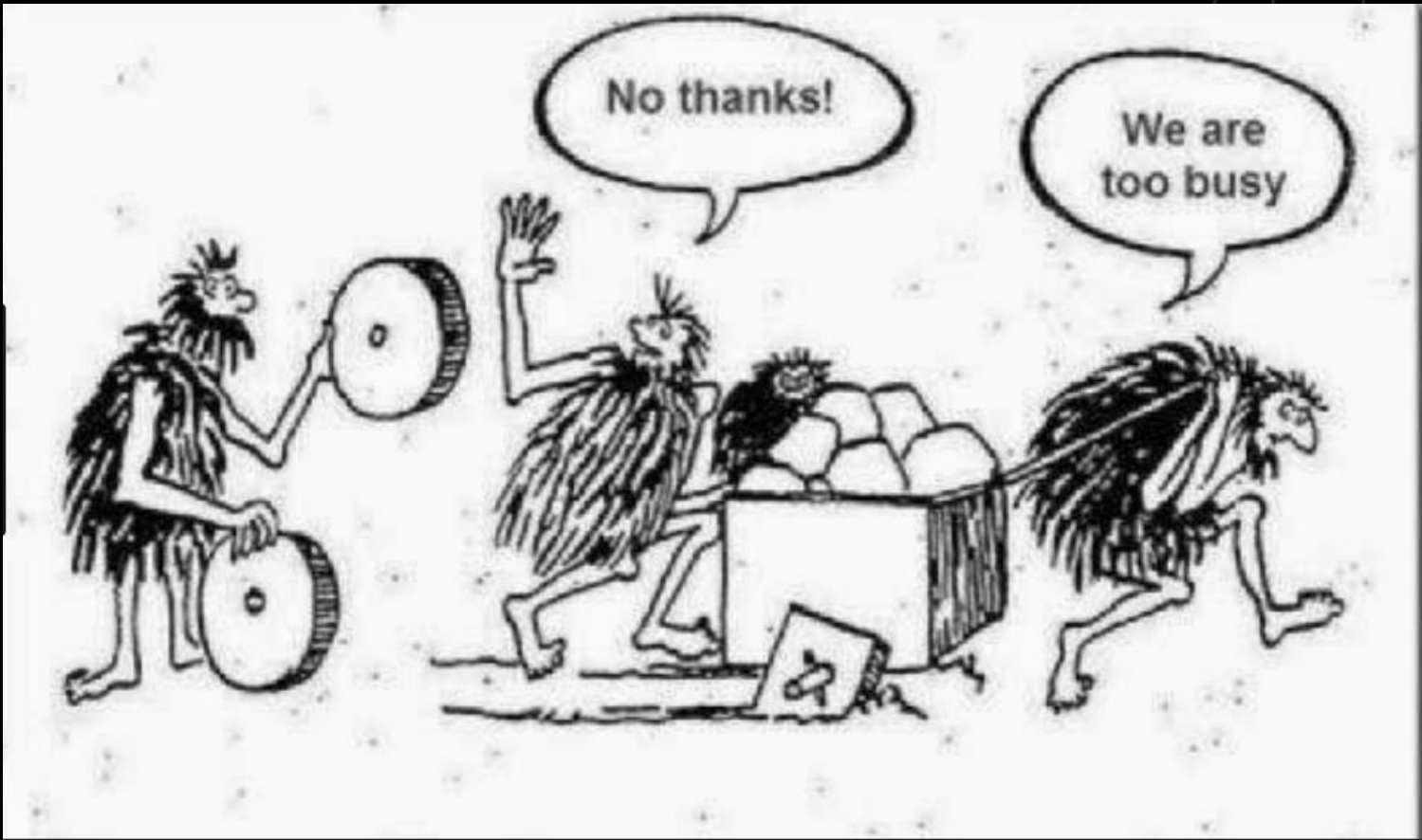
SMF 119-11 Logsource

Sep 18, 2017, 12:00:00 AM - Sep 25, 2017, 12:00:00 AM

Log Source	Subsystem name (custom) (Unique Count)	Sysplex Name (custom) (Unique Count)	Start Time (Maximum)	Magnitude (Minimum)	Event Count (Sum)	Count
IBM z/OS	Multiple (2)	Multiple (2)	Sep 24, 2017, 11:59:59 PM	3	25,562,878	25,562,878

QRadar User Behavior Analytics





Thank You

David Z. Rossi
Cyber Security Architect
IBM Z
dzrossi@us.ibm.com

IBM Z

© 2017 IBM Corporation

you^{IBM}