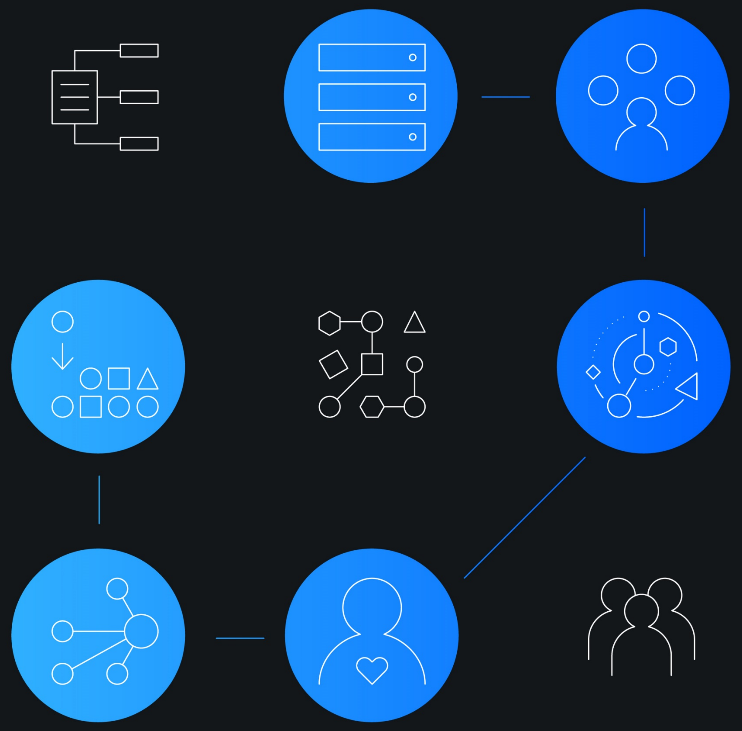
Welcome to A Day in the Life with a Z Security Incident

IBM Security Virtual User Group Day

Chris Ganim - CIPM
Cybersecurity Technical Specialist
IBM Z
cganim@us.ibm.com



IBM Security Community

8,000 Members Strong and Growing Every Day!

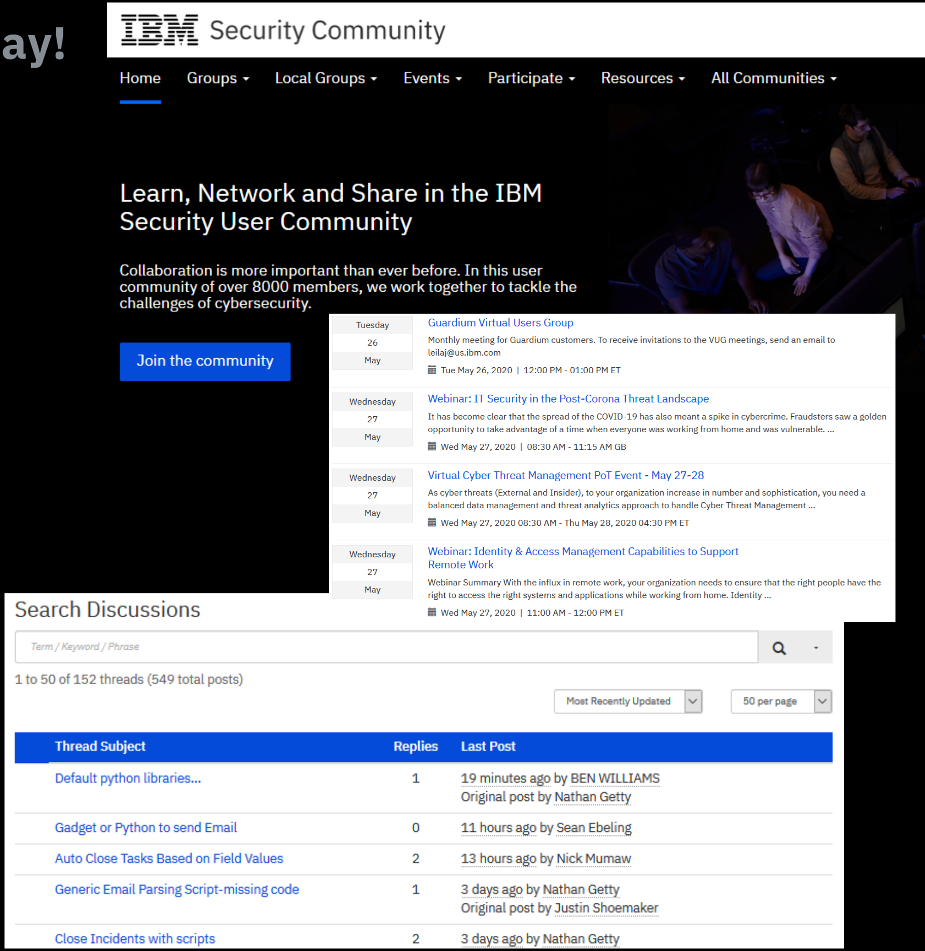
Sign up: https://community.ibm.com/security

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.



IBM Security Community

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

3J Mechanical Supplies, Inc.

- Industrial parts supplier
- 5,000 employees
- 10 warehouses in 6 states

Mission Critical applications running on Z

- Parts transaction including orders, inventory, refunds, etc
- Human Resources including payroll
- Freight management

Security Tools

- SIEM – QRadar
- RACF Administration, audit, and compliance – zSecure Suite

Jane Thomas

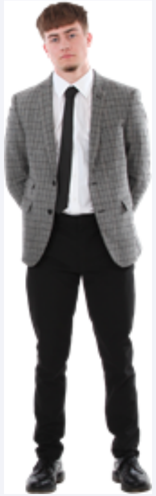
ID = JANET

- SOC Team Security Analyst
- Minimal mainframe experience

Bob Ryan

ID = BOBR

- RACF administrator
- 20+ mainframe and RACF experience
- No SOC experience



John Francis

ID = JOEF

- Bad actor
- Looking to cause harm and steal PII data

Lilly Thompson

ID = LILLYT

- Disgruntled Systems Programmer
- Passed up for promotion to manager

QRadar terminology pertaining to Mainframe data

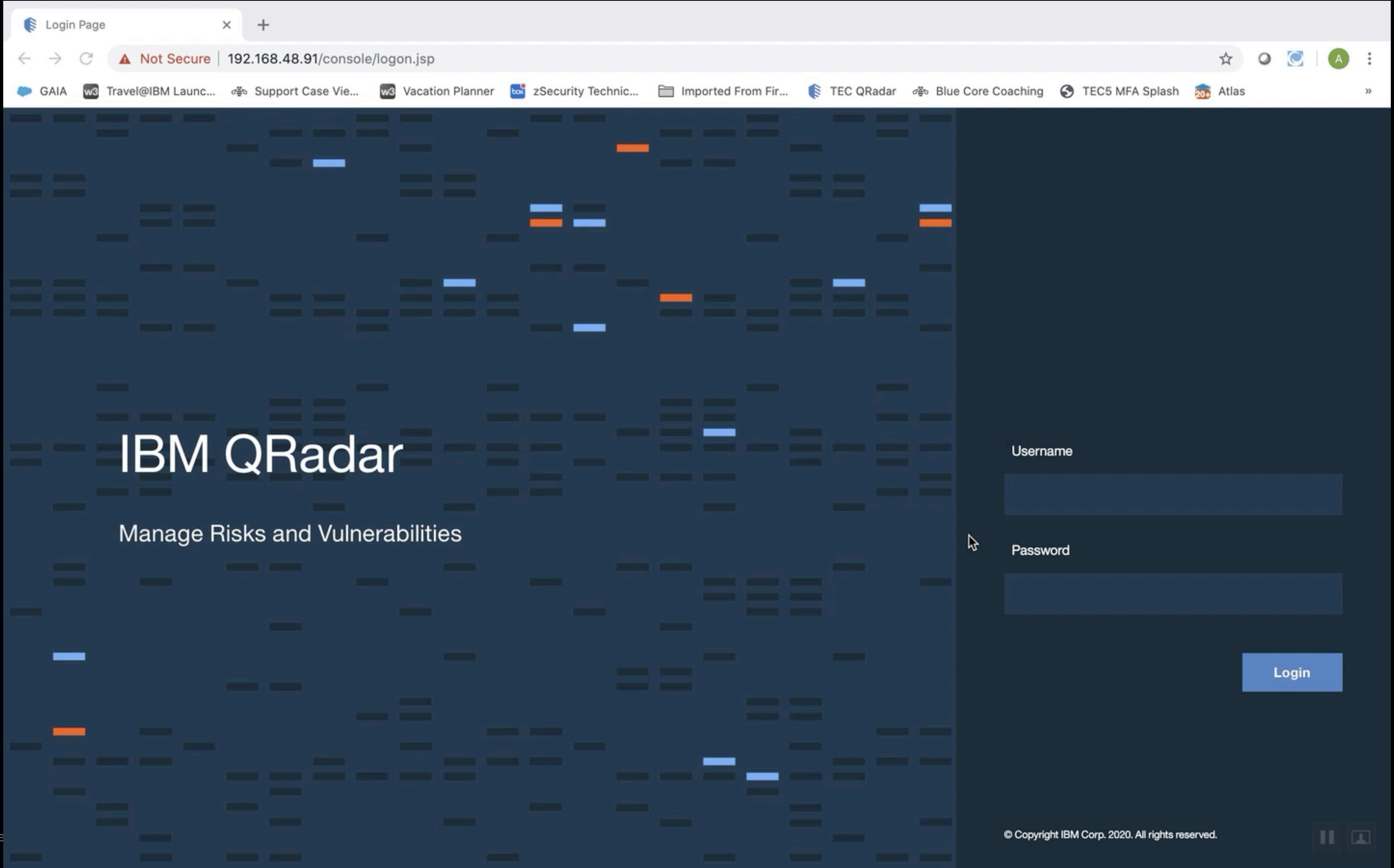
Alerts – zSecure Alert

Events – QRadar streaming events from log sources (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

Security Incident Detected



IBM QRadar

Manage Risks and Vulnerabilities

Username

Password

© Copyright IBM Corp. 2020. All rights reserved.

Jane Thomas

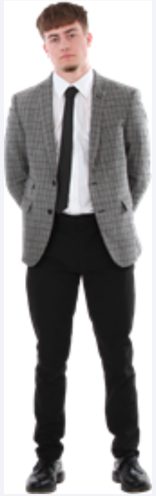
ID = JANET

- SOC Team Security Analyst
- Minimal mainframe experience

Bob Ryan

ID = BOBR

- RACF administrator
- 20+ mainframe and RACF experience
- No SOC experience



John Francis

ID = JOEF

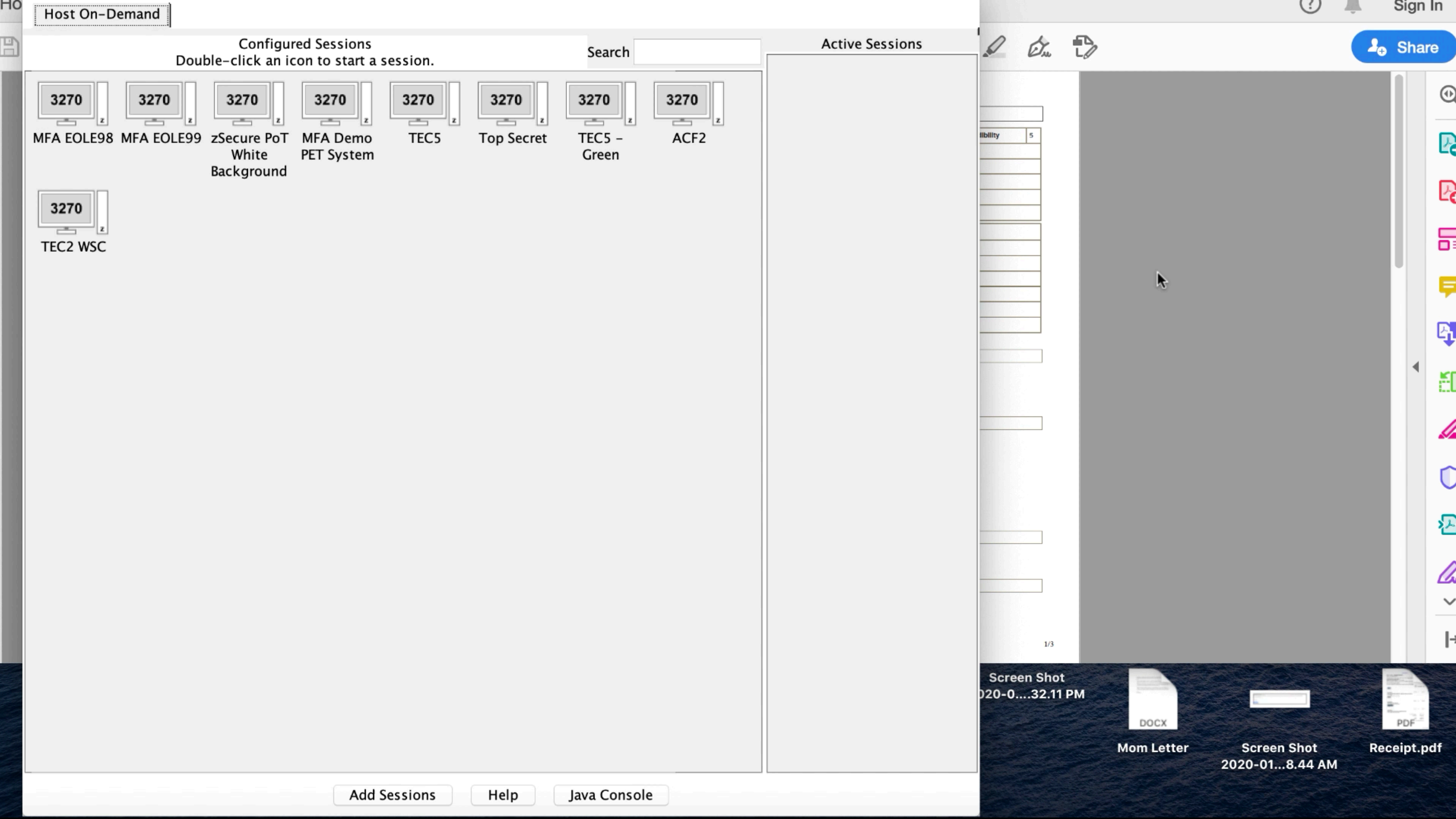
- Bad actor
- Looking to cause harm and steal PII data

Lilly Thompson

ID = LILLYT

- Disgruntled Systems Programmer
- Passed up for promotion to manager

Investigation and Remediation



Configured Sessions
Double-click an icon to start a session.

Jane Thomas

ID = JANET

- SOC Team Security Analyst
- Minimal mainframe experience

Bob Ryan

ID = BOBR

- RACF administrator
- 20+ mainframe and RACF experience
- No SOC experience

John Francis

ID = JOEF

- Bad actor
- Employee looking for financial gain by whatever means possible

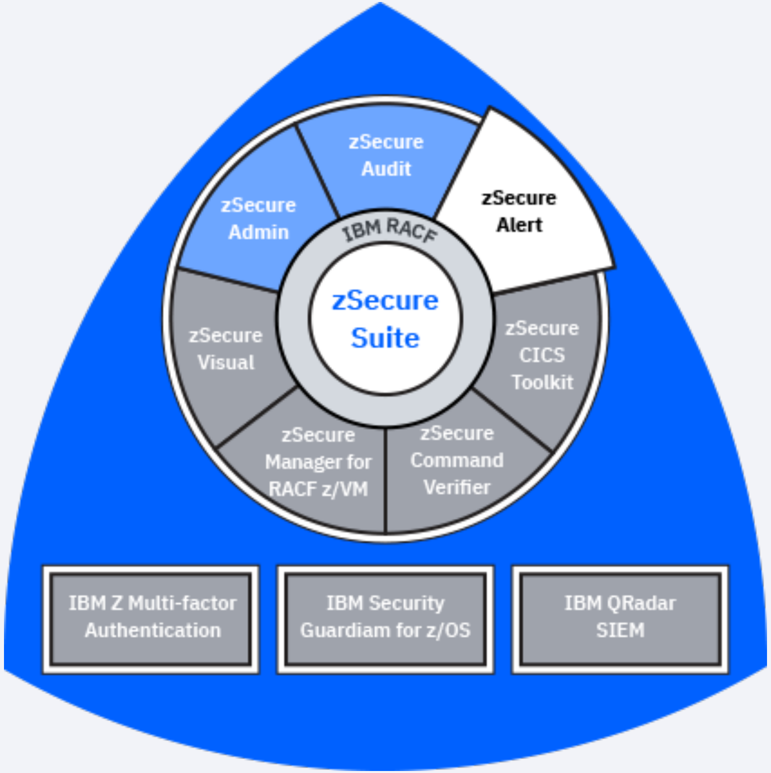
Lilly Thompson

ID = LILLYT

- Disgruntled Systems Programmer
- Passed up for promotion to manager

How did Jane and Bob find and eliminate the threat actors?

IBM Security zSecure Alert

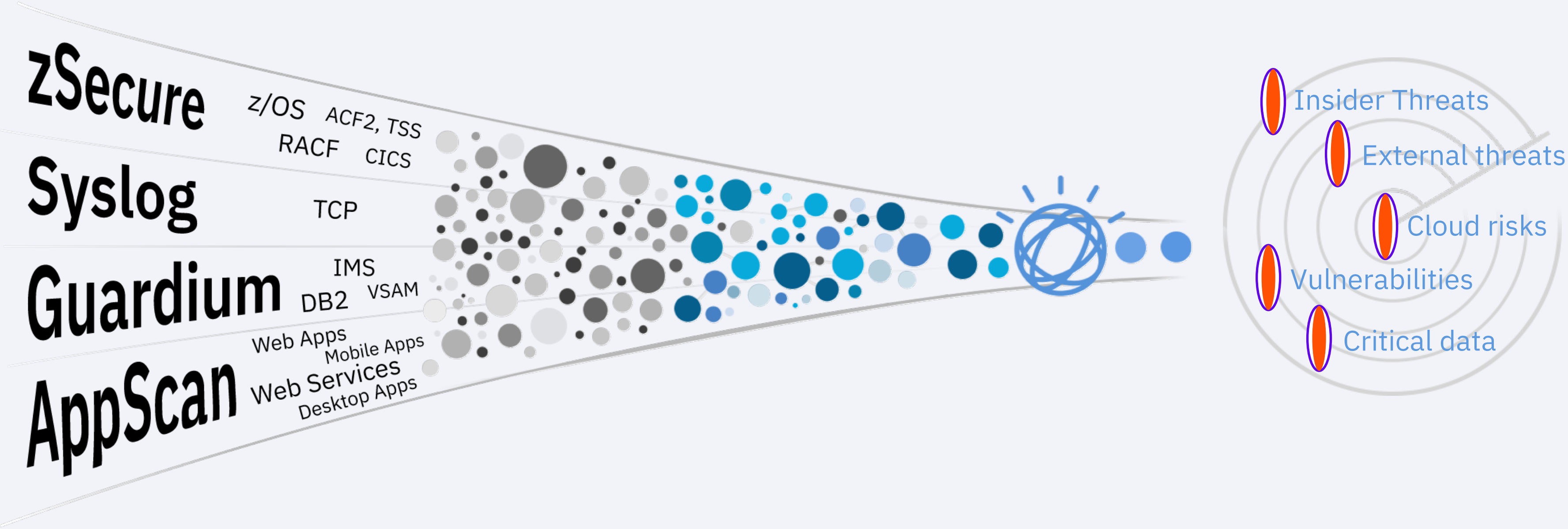


Improves SOC effectiveness, threat detection and remediation with near real-time monitoring and triggers that automate alerts and corrective actions.

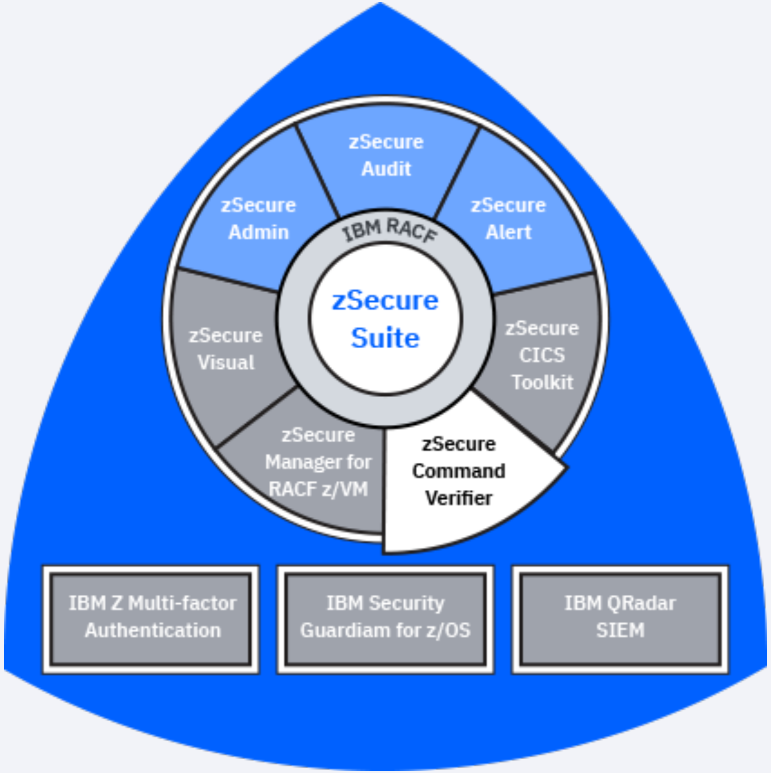
- Monitors for configuration changes in z/OS, RACF, and ACF2
- Provides over 65 out of the box alerts for common security concerns
  – Includes emergency user logins
- Provides the ability to build customized, predefined alerts to match your operational model
- Sends alerts to SOC with SIEM integration (QRadar and others)
- Send alerts as email or SMS

Included with zSecure Audit…Real time security logs to SIEM (QRadar, Splunk, Arcsight, etc)

Mainframe data sources and integration



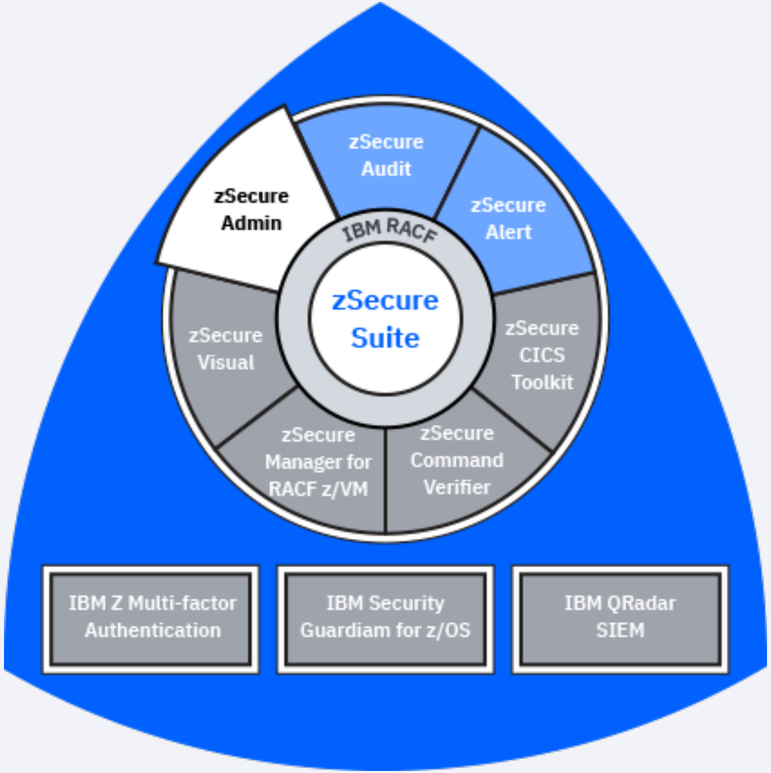
IBM Security zSecure Command Verifier



Reduce the risk of security breaches and failed audits caused by internal errors and noncompliant commands

- Prevents RACF commands that are erroneous or do not adhere to corporate security policy
- Reduces database pollution by preventing noncompliant commands
- Enforces naming conventions
- Provides audit trail to determine who, what, and when changes were made to RACF

IBM Security zSecure Admin



Maximizes IT resources, reduces administrative overhead and errors, and minimizes security risks.

- Automate routine tasks to save time and ensure accuracy
- Prevents overentitled users by monitoring user access
  - Provides the ability to remove unused access
- Test RACF database changes in an offline database before running in production

IBM Z MFA

SOMETHING THAT YOU KNOW

-Usernames and passwords

-PIN Code

SOMETHING THAT YOU HAVE

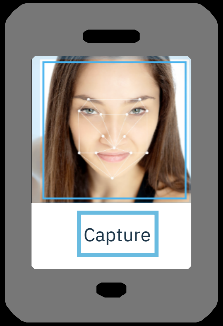
-ID Badge

-One time passwords

-Time-based

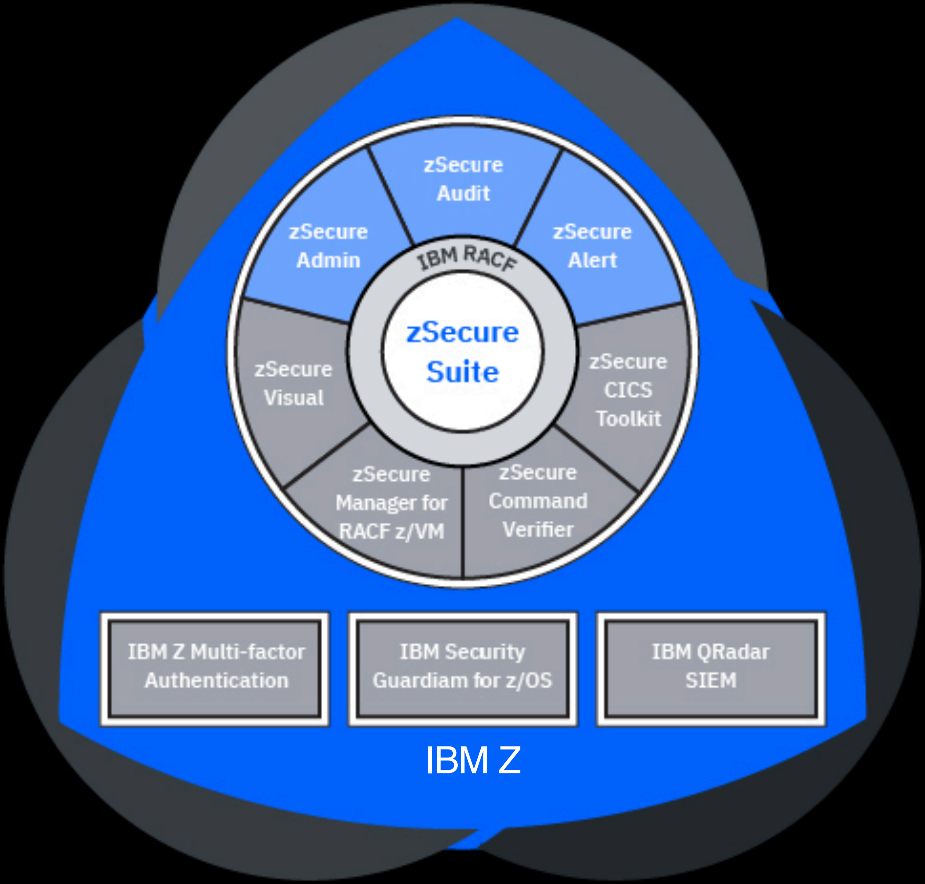
SOMETHING THAT YOU ARE

- Biometrics



IBM Z Security

A rich portfolio for modern, comprehensive mainframe security



zSecurity Events/Engagements

zSecure Value Assessment

- Guided assessment of customers zSecure configuration/utilization

zSecure Demo and Technical Discussion

– “Day in The Life” of zSecure User as it relates to customer environment

zSecure Health Check

– 3 day zSecure Audit review of your environment for potential vulnerabilities

Mainframe Security Control Review

– Guided security assessment of the highest priority security controls

zSecurity Technical Workshop

- Hands on experience with zSecure and Guardium solutions

Proof of Concept

– Install and use zSecure in your environment for a predetermined amount of time

2 Question Survey

https://www.surveymonkey.com/r/HK89MPR

IBM Security Community

8,000 Members Strong and Growing Every Day!

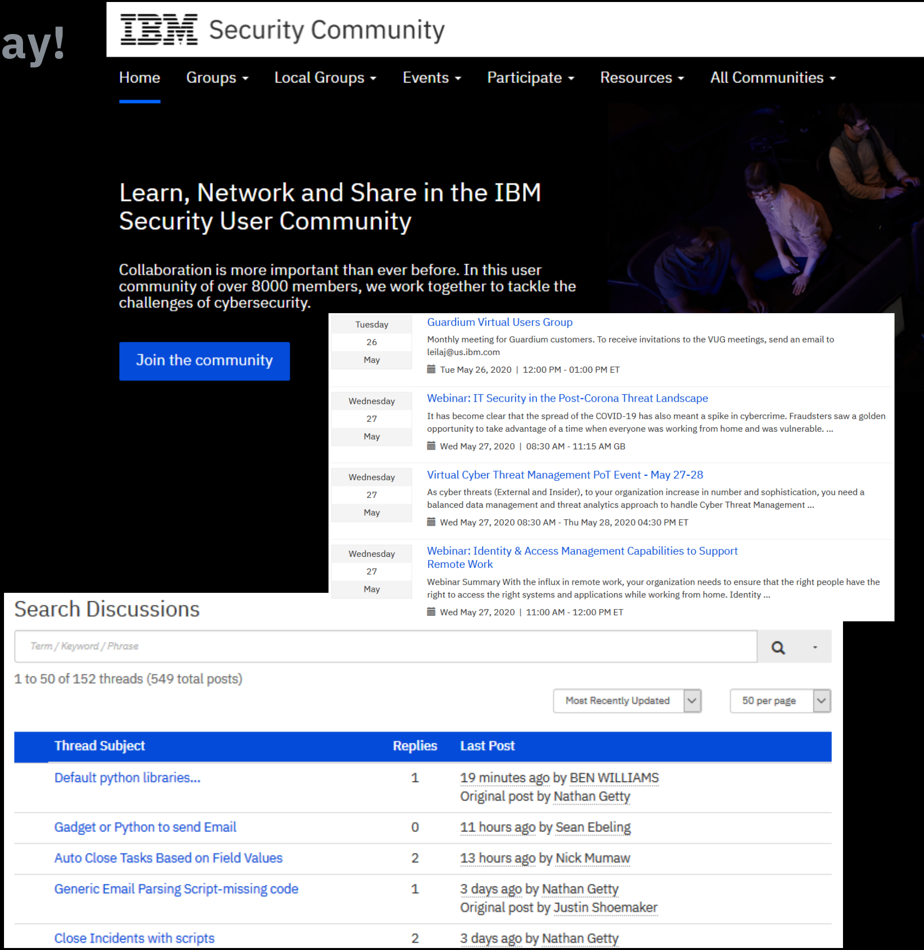
Sign up: https://community.ibm.com/security

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 — Guardian 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

Questions?

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube/user/ibmsecuritysolutions

https://www.ibm.com/security/mainframe-security/zsecure

https://www.ibm.com/us-en/marketplace/ibm-multifactor-authentication-for-zos

https://community.ibm.com/community/user/security/communities/zsecurity

https://www.ibm.com/security/mainframe-security/zsecure

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.