

Modernizing Mainframe Security

Christopher Perry, Lead Product Manager BMC AMI For Security

Christopher Perry

Lead Product Manager, BMC AMI For Security

• Military Experience

- Technical Advisor to the Commanding General of Army Cyber Command – FT Belvoir, VA (2011)
- Infantry Officer – Germany/Afghanistan (2012-2015)
- Cyber Training Officer – FT Gordon, GA (2016)
- Expeditionary Cyber Company Commander – FT Meade, MD (2017-2018)

• Civilian Education

- Georgia Institute of Technology, Masters Degree in Computer Science – Machine Learning (ongoing)
- United States Military Academy, Bachelors of Science Degree in Computer Science
- Offensive Security Certified Professional + Expert (OSCP / OSCE)
- Certified Information Systems Security Professional (CISSP)
- Certified Ethical Hacker (CEH)
- GIAC Penetration Tester (GPEN)
- GIAC Certified Intrusion Analyst (GCIA)
- GIAC Certified Forensic Analyst (GCFA)



The BMC 2019 Survey Says....

52%

See security as a key
mainframe strength

58%

Do not use privileged
user monitoring

↑ #2

Security/Compliance
second highest
priority on the
mainframe survey

38%

Of executives are
concerned about
mainframe security
skills

Myth 1

“We don’t really need extra security because our mainframe is behind the firewall”

- Head of Mainframe Operations

Myth 2

“I’m not worried, we use RACF to secure our users and datasets from malicious threats”

- Senior System Programmer

Myth 3

“Only two of my most loyal sysprogs have access to system datasets, I trust them.”

- Head of Mainframe Operations

Myth 4

“It’s just a development machine...we only focus on our production mainframes that can impact our business”

- Head of Mainframe Security

“If hacking a mainframe is so possible then why has it never happened before?”

- VP of Mainframe

Real-Life Mainframe Attacks

NEWS
Pirate Bay co-founder charged with hacking IBM mainframes, stealing money



By **Loek Essers**
Amsterdam Correspondent, IDG News Service | APR 16, 2013 9:05 AM PT

Gottfrid Svartholm Warg and three associates were charged with hacking the mainframes of the Swedish IT Firm Logica and the Nordea Bank and stealing over 800K.

Only caught because greed in transferring too large a sum of money triggered a flag, not because of IT security solutions

Unnamed Bank victim of first known case of mainframe ransomware

A bank fell victim to a ransomware in a 4 part attack:

- 1 – Spear Phishing attack against system programmers of the mainframe**
- 2 – Keylogged their windows computer to pilfer mainframe credentials**
- 3 – Submit a JCL job through FTP to scan for sensitive datasets**
- 4 – Submit a second JCL job through FTP to encrypt datasets with custom ransomware**

“Alright, you have my attention. So how do I defend against these threats?”

- Most of you, probably

National Institute of Standards and Technology (NIST) Cyber Security Framework

In order to effectively defend your mainframe you need to be able to effectively accomplish ALL 5 steps of the NIST model for every computer on your network – especially the mainframe



“Well how do you detect malicious activity?”

- Most of you, hopefully

User Entity Behavior Analytics



**Mainframe
User
Behavior**

**Analytics
Engine**

**Actionable
Intelligence**

Vital Data Types

Connections

- TCP/IP
- FTP
- CICS
- TN3270
- IND\$FILE

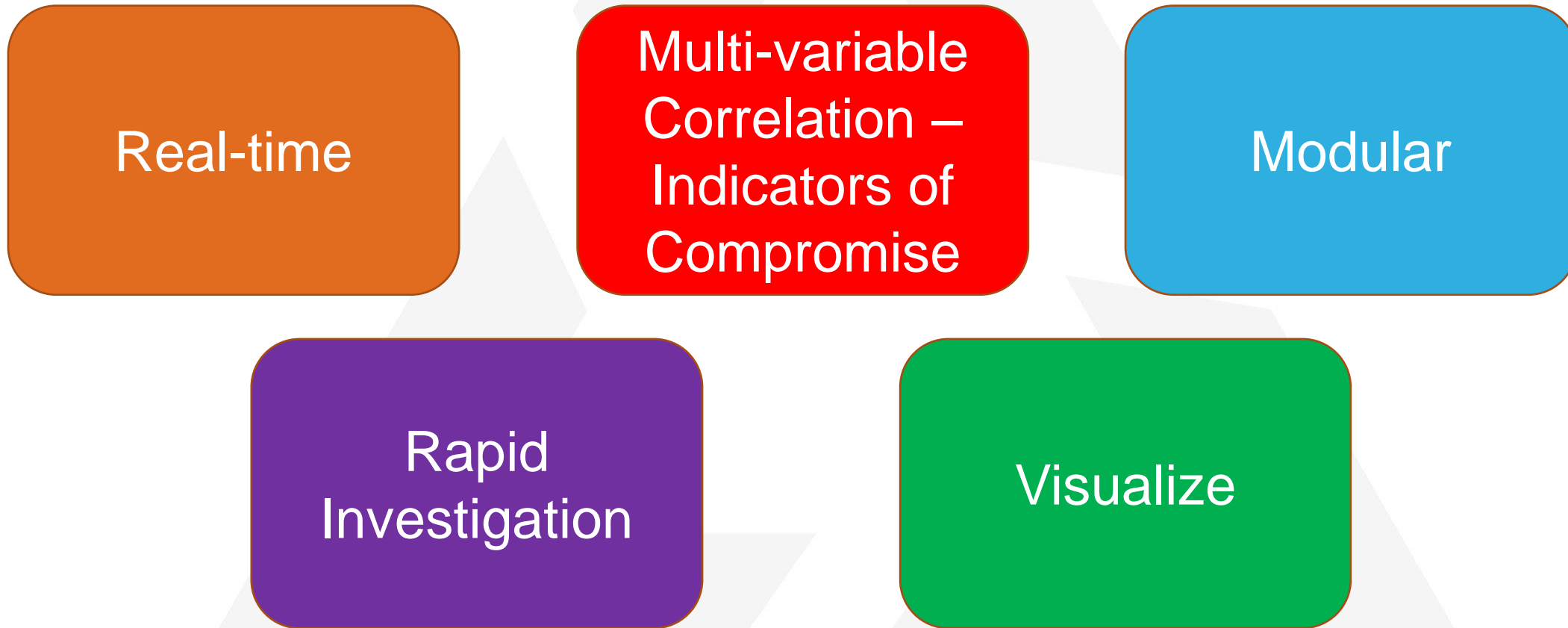
z/OS

- RACF/ACF2/TSS
- USS
- TSO
- JES

Databases

- Db2
- IMS

Analytics Engine



BMC Announces Intent to Acquire RSM Partners

 [View printer-friendly version](#)

[<< Back](#)

Acquisition to enhance the BMC AMI portfolio to support the self-managing, modern mainframe

HOUSTON – February 18, 2020 – **BMC**, a global leader in IT solutions for the digital enterprise, today announced the signing of a definitive agreement to purchase RSM Partners, a global provider of services, software, and expertise with a 100% focus on IBM Z® mainframes.

The ultimate solution to our security problems or vendor snake oil?

Actionable Intelligence Type 2 - Machine Learning

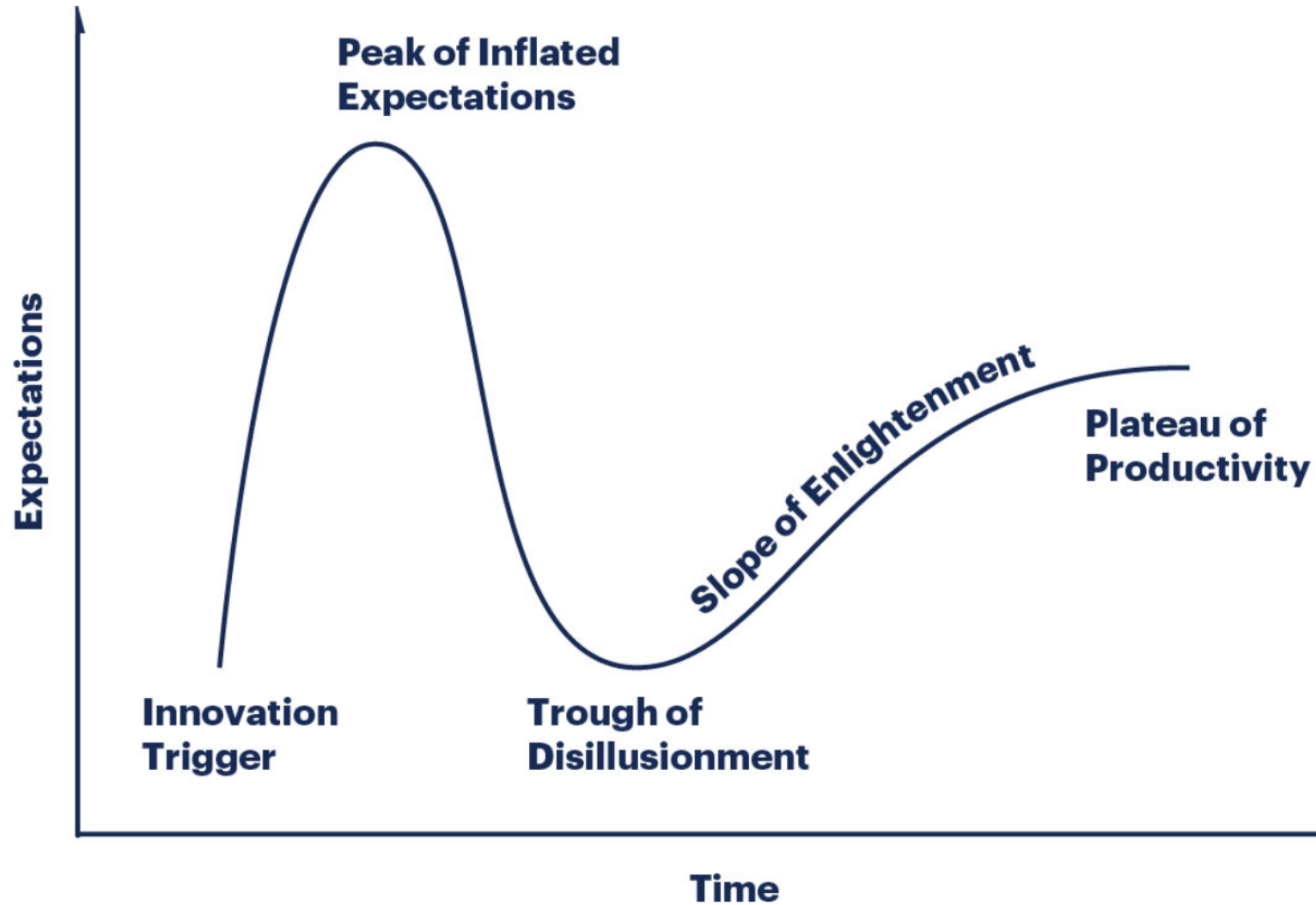
The Good

- Able to 'learn' the environment
- Automated
- Detect anomalous activity
 - Connections
 - File transfers
 - Process output

The Bad

- False Positives
- Dynamic Environments
- Explainability
- Anti-ML Attacks
 - Evasion
 - Data Poisoning

Gartner Hype Cycle



Actionable Intelligence Type 3 – Custom IOCs

Threat Intelligence

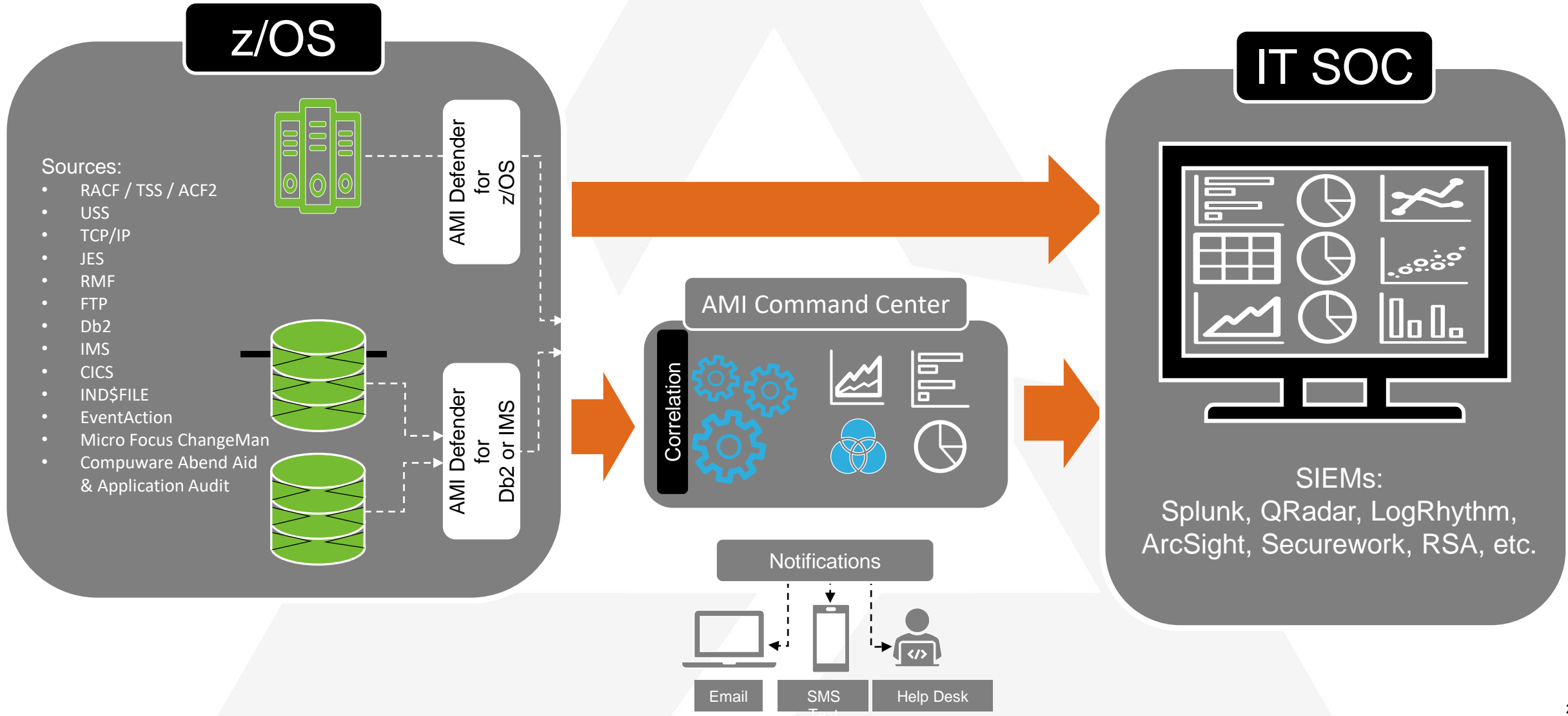
Simulations

Pentests

Canaries

Threat hunt team

Architecture



Example Indicators of Compromise


1. Credential Spraying
2. Multiple Logins
3. Default Credentials
4. Privilege Escalation
5. Anomalous APF Dataset access
6. Unusual Ports
7. Unusual outbound traffic
8. Access RACF/ACF2/TSS Databases

“Hey, we received an alert that someone copied the RACF database. Is this a problem?”

- A SOC Analyst to a SysProg, 72 hours after the alert

Effective Incident Response

1. Establish clear processes and procedures
2. Integrate the mainframe into enterprise processes
3. Educate the SOC team on the platform
4. Resource the SOC with necessary tools (timeline)

Time	UserID	Action
0901	MVSCTP	Failed Login
0902	MVSCTP	Failed Login
0903	MVSCTP	Successful Login
0904	MVSCTP	Check Privileges
0906	MVSCTP	Search for Datasets
0907	MVSCTP	Update BCVM.APFLOAD (APF Library)
0922	MVSCTP	Privilege Escalation 
0923	MVSCTP	Create new privileged user
0926	MVSCTP	Query database
0938	MVSCTP	Update database
0940	MVSCTP	Logoff

Key Takeaways



The mainframe is just as vulnerable to attack as any other TCP/IP connected computer



Companies should follow the NIST framework to apply good security hygiene to the mainframe



Effective detection stems from Indicators of Compromise built around behavior analytics



The best Indicators of Compromise are built on domain expertise



Incident Response teams need to be able to quickly evaluate alerts to decide next course of action

Complete your session evaluations for a chance at daily prizes!

To complete, visit
www.share.org/evaluation
and see your progress on the
leaderboard!

