

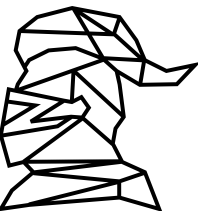
M.U.S.E. on Ransomware Mitigation



Bryan Childs, Product Manager, z/OS Security

Trademarks

See <https://www.ibm.com/legal/copytrade> for a list of trademarks



What If



What if an overview of
your security posture
on z/OS
could be represented
by a card game?



Suits & categories



4 suits

- **Risk:** identify platform-independent use cases
- **Project:** implement IBM Z functionality
- **Guidance:** assist Risk identification
- **Momentum:** assist Project implementation

4 categories

- **M.**anaging access & logging
- **U.**ser authentication & analytics
- **S.**ystem integrity & resiliency
- **E.**ncryption & data privacy



Card format

Title

Logo

Description

Match

Category

Suit

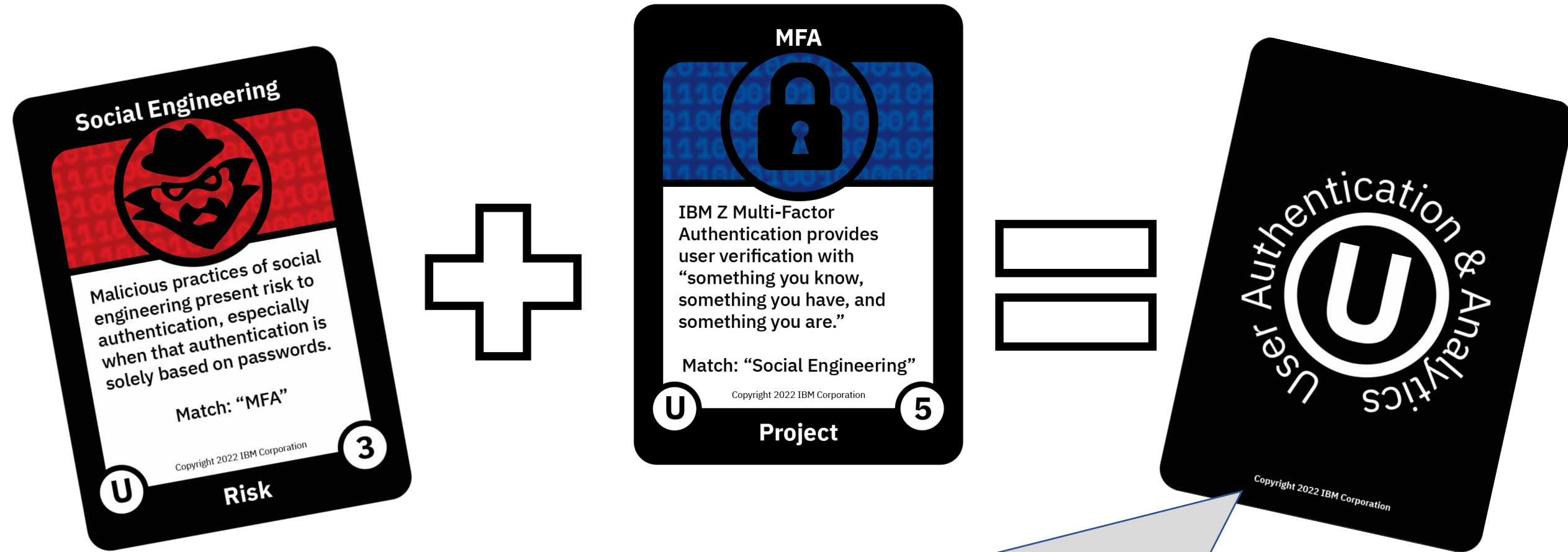


The goal of the game is to earn more Mitigation points than your opponents. Implement a Project card like to gain one Mitigation point.

In the future, this index value will help match a Project card with the corresponding platform-independent Risk card.



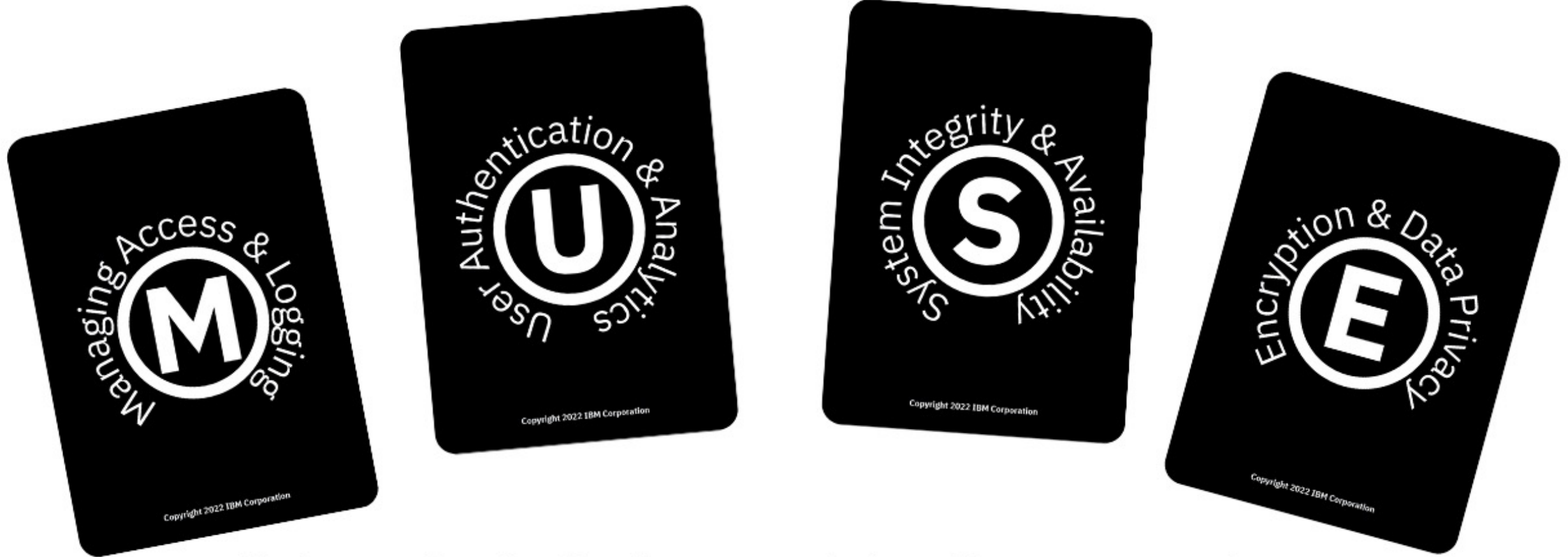
Mitigation category bonus



Match an identified Risk with an implemented Project to gain a M.U.S.E. category bonus. If both players contribute, the second player steals the earlier card and obtains the bonus.



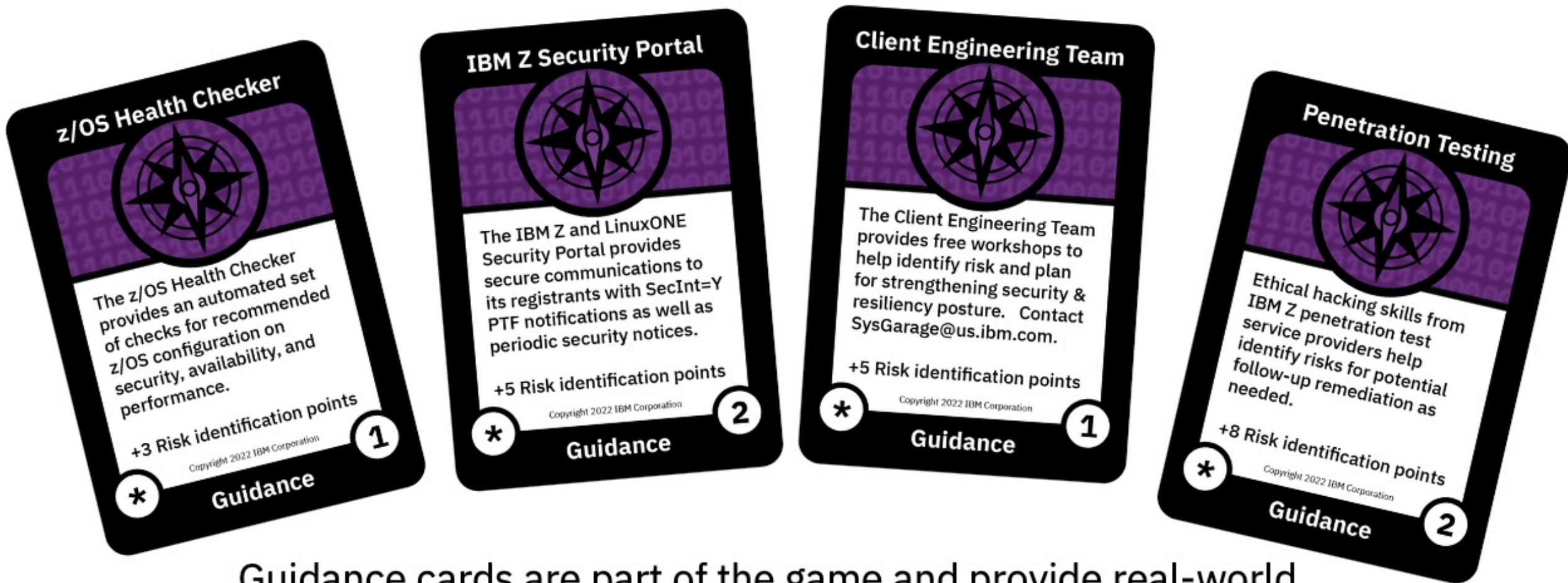
Holistic goal



Collaboratively find a match in all 4 categories to finish the game.



Real-world guidance examples



Guidance cards are part of the game and provide real-world reference points. For example, contact the IBM Client Engineering Team for Systems for a free discovery consultation on your security posture at SysGarage@us.ibm.com



The nearly forgotten suit

“M.U.S.E.” also represents the fictitious “Mock-Up Services Enterprises” company where the competing card players “work” & whose projects can gain some fun momentum...



Distributed ransom reference

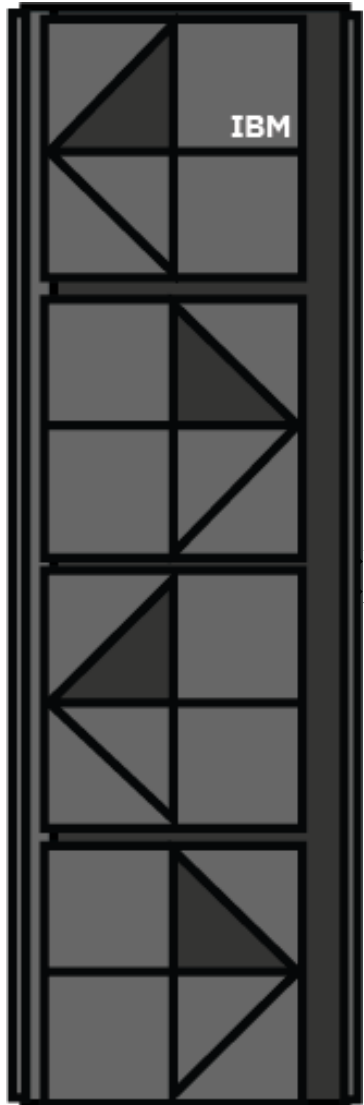
Reference: <https://www.ibm.com/downloads/cas/EV6NAQR4>



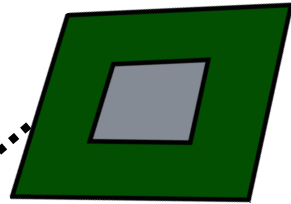
- **Implement** Multi-Factor Authentication
- **Search** for malicious activity with EDR and Threat Intelligence tooling from well known providers
- **Encrypt** data
- **Patch** rapidly with insights from a vulnerability management team
- **Test** backups and confirm they are not connected to the IT environment & test your incident response plan



Quantum-safe encryption components

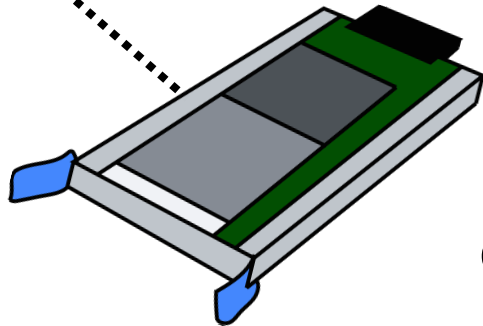


CPACF

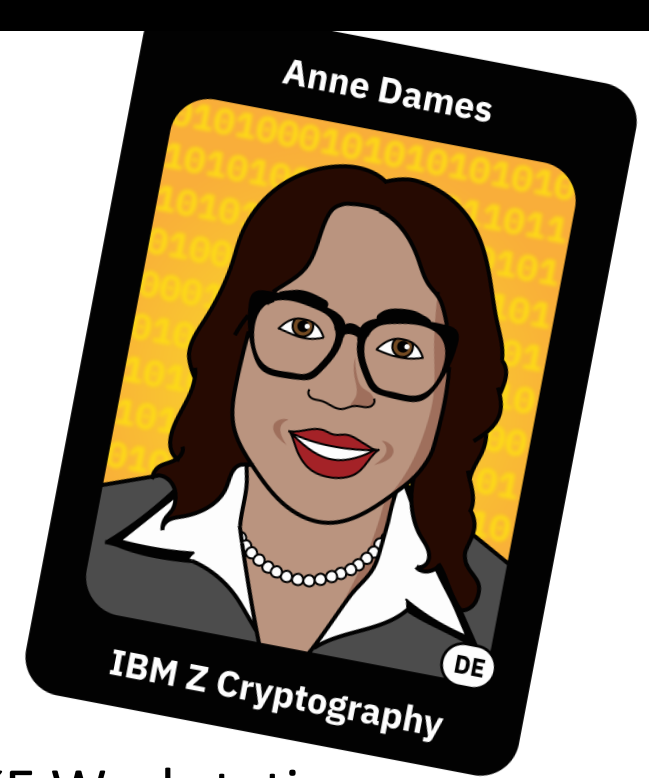


High performance key calculations

Crypto Express 8S (CEX8S)



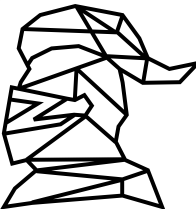
High security key calculations



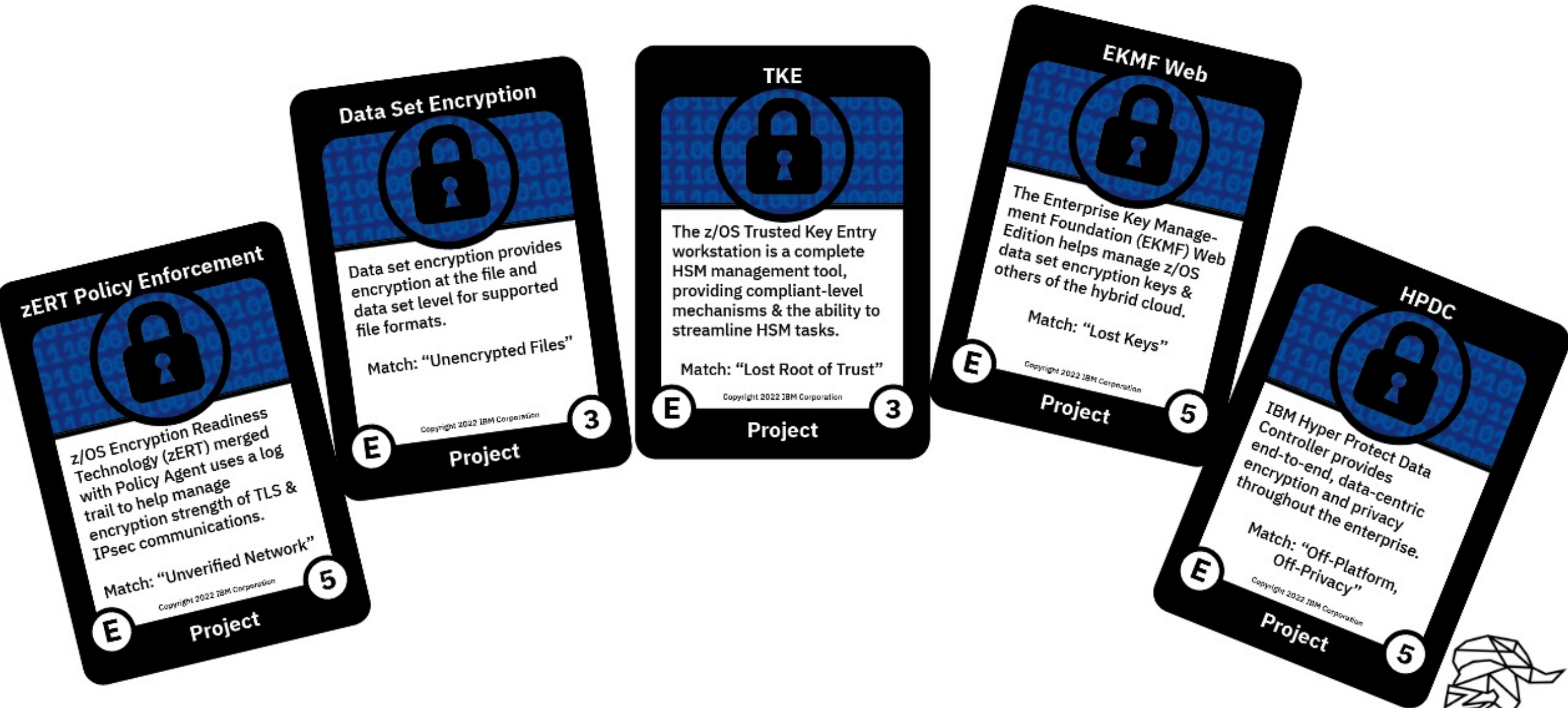
TKE Workstation



Simplified & secure Master Key usage



Encryption cards



System Integrity & Availability cards



Play online at <https://musecues.mybluemix.net/>



Sneha Kanaujia
z/OS Security PM

























Focus: 3
Guidance: 0
Momentum: 0
Multiplier: 1
Score: -5
Turn: 6

Status



Secure Service Process



A secure service process leverages the IBM Z and LinuxONE Security Portal to make informed decisions in applying critical service.

Match: "Downlevel Systems"

S **1**

Project

Critical Code Bugs



The potential for programmer error within applications that run at a high level of privilege warrant specialized scanning to mitigate risk.

Match: "zACS"

S **3**

Risk

Signed SMF



The SMF logstream now supports a Quantum Safe digital signature, helping to validate that its contents have not been maliciously altered.

Match: "Untrusted Logs"

M **3**

Project

Remediation



The Project matching any previously identified Risk is discovered and placed in the player's active hand.

+5 Project implementation points

***** **2**

Momentum

Empty Card



Hand



Legacy Signon Algorithm



Legacy algorithms used for authentication to the system of record need periodic enhancement, not unlike encryption protocols.

Match: "Enhanced PasTickets"

U **3**

Risk

IBM Z Security Portal



The IBM Z and LinuxONE Security Portal provides secure communications to its registrants with SecInt=Y PTF notifications as well as periodic security notices.

+5 Risk identification points

***** **2**

Guidance

Passphrases



RACF's password phrases support mixed case, spaces, numbers, and special characters with a length up to 100.

Match: "Weak Passwords"

U **3**

Project

Recognition



M.U.S.E. executives present you with a corporate award for your efforts. Gain an additional bonus multiplier.

+3 Project implementation points

***** **1**

Momentum

Initiative



A strategic initiative is established at M.U.S.E. this turn, exclusive to a single category of your choosing.

+8 Project implementation points

***** **2**

Momentum



Copyright 2020 IBM Corporation

More Knights with Insights...

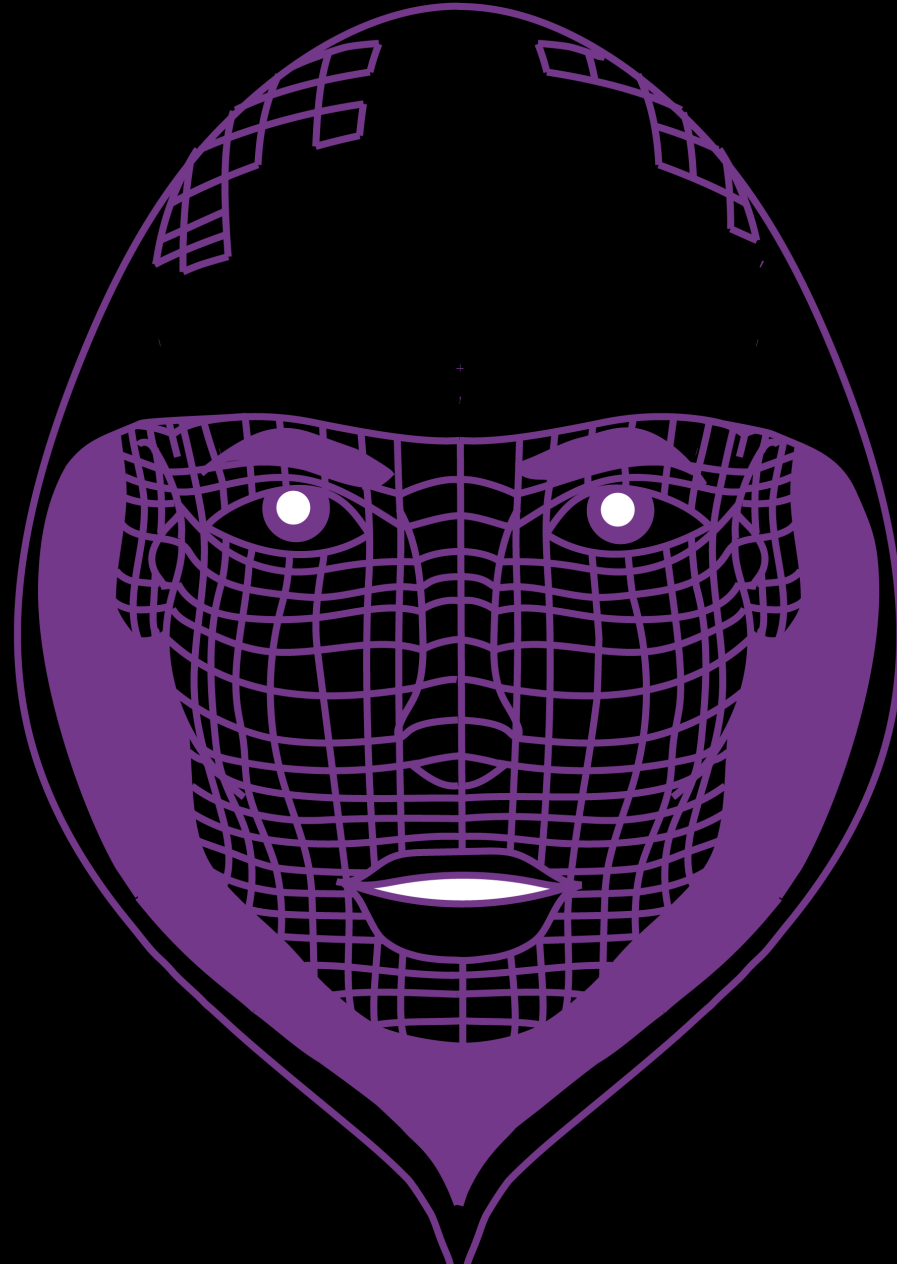


Thwarted by IBM Z! series



Greetings! It's Mike Kelly again, ethical "threat actor"
for Mock-Up Services Enterprises.

...and a new “threat actor” emerges...



Secure Z! F.A.Q.

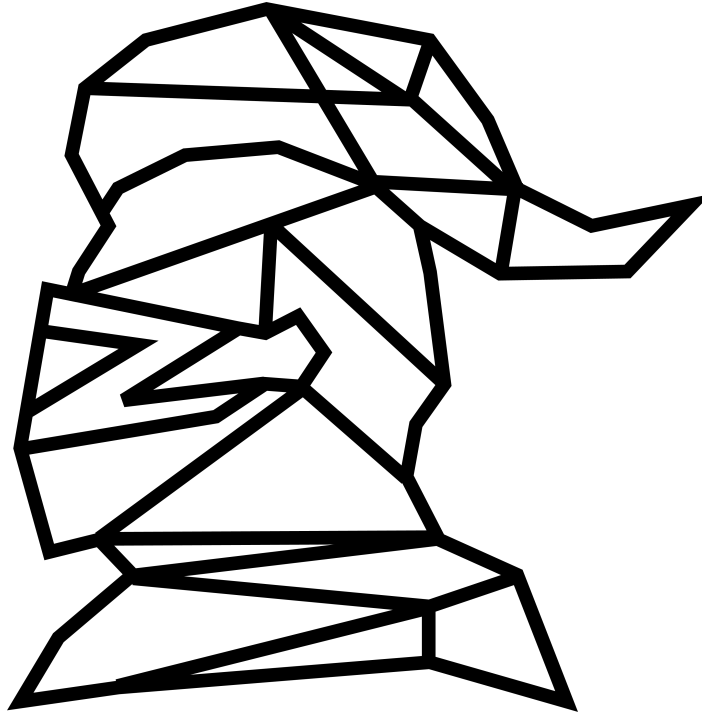


Escape Experience



The Mike Kelly and Michaela Kelly characters, the Mock-Up Services Enterprises and Fictitious Acquisition Quandary businesses, and associated events in this presentation are fictitious. Any resemblance to actual persons, living or dead, or actual events, is purely coincidental. The information in this presentation is provided as is and without warranty of any kind. You remain responsible for the security of your system.

The Enterprise Knights of IBM Z



A grassroots user group
within the IBM Z & LinuxONE Community

ibm.biz/ek-ibm-z