

Mainframe Security: Its not just about your ESM!

Chad Rikansrud

RSM Partners

DTS04

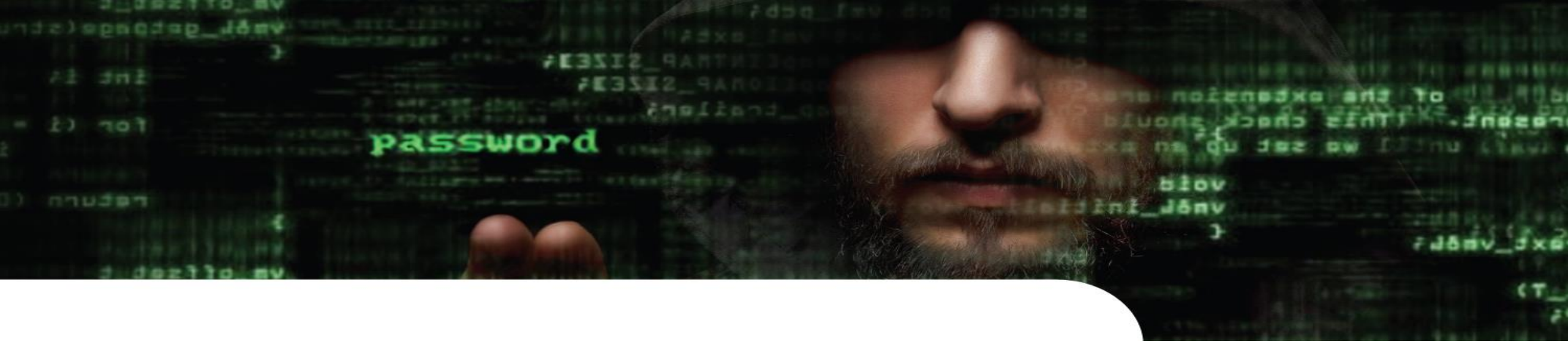
AGENDA



About me

- Director North America, RSM Partners
- Speaker at conferences
 - DEF CON, Derbycon, SHARE, RSA 2017, others
- Worker at large financial company
- Reverse engineering, networking, forensics, development
- Mainframe (z/OS®) researcher
- Doer of other stuff that probably isn't interesting

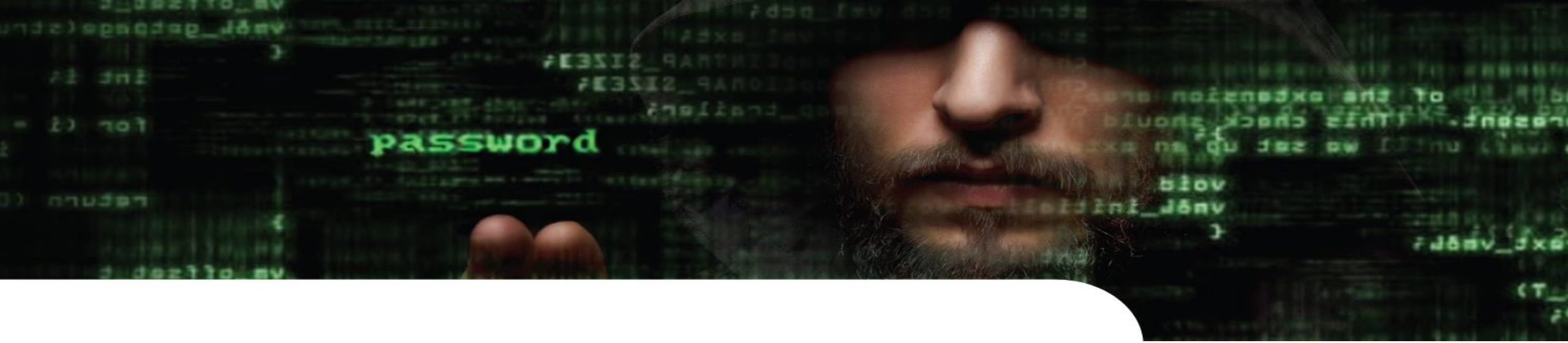




Objectives

Objectives

- Let's start with the basics:
 - ESM stands for External Security Manager
 - RACF[®], ACF2, TSS
 - ESM helps protect the mainframe
- But what does it mean 'protect the mainframe'?
- We will be looking at some of the other security controls available and a number of non ESM related security controls that should be used to protect the mainframe



Some of the Network Controls

We keep hearing non-mainframe people and even some mainframe technicians say:

“The mainframe is fine, it’s behind a firewall...”

Network Controls

- The mainframe is part of an ecosystem of different platforms and devices
- More than likely one or more devices and systems of this ecosystem (including the mainframe) will be connected to the internet
- This means that potentially there are many different ways to reach the mainframe
- We need to consider:
 - Intrusion detection services (IDS), TCPIP security, SENDMAIL and SMTP Security

Network Controls

- Ask yourself: “How much do I actually know about network security and what features/facilities IBM® have built into the system?”
- Who in this room has a clear understanding of:
 - The SERVAUTH class
 - TLS/SSL vs AT-TLS vs IPsec
 - IP Filtering
 - Intrusion Detection Services (IDS)
 - Defence Manager (DM)



SERVAUTH Class

- The SERVAUTH resource class supports TCP/IP security
- Profiles in the SERVAUTH class are prefixed with EZB
- Second qualifier specifies the function (for example):
 - EZB.**STACKACCESS**.** to protect access to the TCP stack
 - EZB.**NETACCESS**.** to specify who can access a specified network
 - EZB.**TN3270**.** to protect TN3270 Secure Telnet Port Access
 - EZB.**PORTACCESS**.** to specify who can use which TCP and UDP ports
- SERVAUTH class must be RACLISTed

SERVAUTH Class

- EZB.**STACKACCESS**.sysname.tcpname
- EZB.**NETACCESS**.sysname.tcpname.netname
- EZB.**PORTACCESS**.sysname.tcpname.portname
- EZB.**TN3270**.sysname.tcpname.PORTnnnnn
- EZB.**NETSTAT**.sysname.tcpname.netstatoption
- EZB.**FRCAACCESS**.sysname.tcpname
- EZB.**MODDVIPA**.sysname.tcpname
- EZB.**SOCKOPT**.sysname.tcpname.SO_BROADCAST
- EZB.**NETMGMT**.sysname.tcpname.SYSTCPDA
- EZB.**NETMGMT**.sysname.tcpname.SYSTCPCN
- EZB.**NETMGMT**.sysname.tcpname.SYSTCPSM

TLS/SSL vs AT-TLS vs IPsec

- They all provide encryption/certificate for TCP/IP...
- But what else can you do with them?
- Who knows the differences?
- Who knows the restrictions?



TLS/SSL

- TLS – Transport Layer Security
- SSL – Secure Sockets Layer (prev. version of ^^)
- Encrypts end-to-end to the application buffers
- Application must support System SSL
- Development maintenance overhead
- Mostly does not work for UDP services (DNS, SNMP, etc)

AT-TLS

- AT-TLS – Application Transparent Transport Layer Security
- Encrypts to TCP/IP stack on z/OS
- Component of Communications Server
- Defined per application
- Removes need for application to support System SSL
- IBM recommended solution
- Requires policy agent (pagent)

IPsec

- IPsec – Internet Protocol security
- Provides an encrypted “tunnel” at IP link layer
- Component of Communications Server
- Tunnel can be shared by multiple applications/services
- Tunnel can be used for TCP and UDP services
- Data can flow in clear to application within datacentre
- Requires policy agent

IP Filtering

- Effectively a firewall for z/OS
- Component of Communications Server
- Requires policy agent
- Configure to allow/reject any IP packet
- You can use the:
 - Target/Origin IP address
 - Target/Origin Port
 - Plus other metrics...
- Audit log written to SyslogD

Intrusion Detection Services (IDS)

- A hacker detection mechanism for z/OS
- Component of Communications Server
- Looks for a wide range of intrusion attacks
 - ICMP attacks
 - UDP attacks
 - Port scans
 - TCP state violations
 - TCP malformed packets
 - Many more...
- Requires policy agent
- Audit log written to SyslogD

Intrusion Detection Services (IDS)

- We all understand the business disaster that is a data breach and the millions that can cost an organisation
- But a denial of service can cost an organisation just as much
- What if one of your major competitors hired someone from the “Dark Web” to take down your systems...
- What if they have mainframe knowledge?
- Hackers learn quickly and they are platform agnostic. As long as they get paid, they don't care. Ever heard of Hacking as a service?

Intrusion Detection Services (IDS)

Welcome Guest | Sign In

E-BUSINESS | TECHNOLOGY | CRM | LINUX | ECTNEWS.COM



CYBERCRIME

SEARCH



Business E-Commerce Enterprise IT Mobile Security SMB Social Media Trends

Reader Services

E-Commerce Times > Security > Cybercrime | [Next Article in Cybercrime](#)

September 24, 2016 12:13:52 PM

Hacking as a Service Hits the Mainstream

By Katherine Noyes
Jan 19, 2015 7:37 AM PT

Print
 Email

A fledgling website created last fall connects hackers with clients willing to pay for their services.



Nearly 50 hackers have listed their services on [Hacker's List](#) so far, for tasks including data recovery, penetration testing and computer forensics.

More than 500 hacking jobs had been out to bid as of last week, with prices ranging from US\$100 to \$5,000, according to a *New York Times* report.

One bidder reportedly offered up to \$2,000 to get a list of clients from a competitor's database; another sought access to a boyfriend's social-media accounts.



Most Popular Newsletters News Alerts



What do you think of politically inspired Internet memes?

- ☐ They tend to be brutally honest about their targets.

VANGUARD

SECURITY & COMPLIANCE

SyslogD

- Given this is typically where all the useful information is written...
- How many of us actually monitor or even alert on what's written in here?
- Borrowed the next slide from a comms server manual



SyslogD

- The syslogd facility uses a common mechanism for segregating messages
- The table shows the facilities used by z/OS Communications Server functions which write messages to syslogd
- The Primary syslog facility column shows the syslog facility used for most messages logged by the application
- Some applications use other facilities for certain messages

Table 3. syslogd facilities

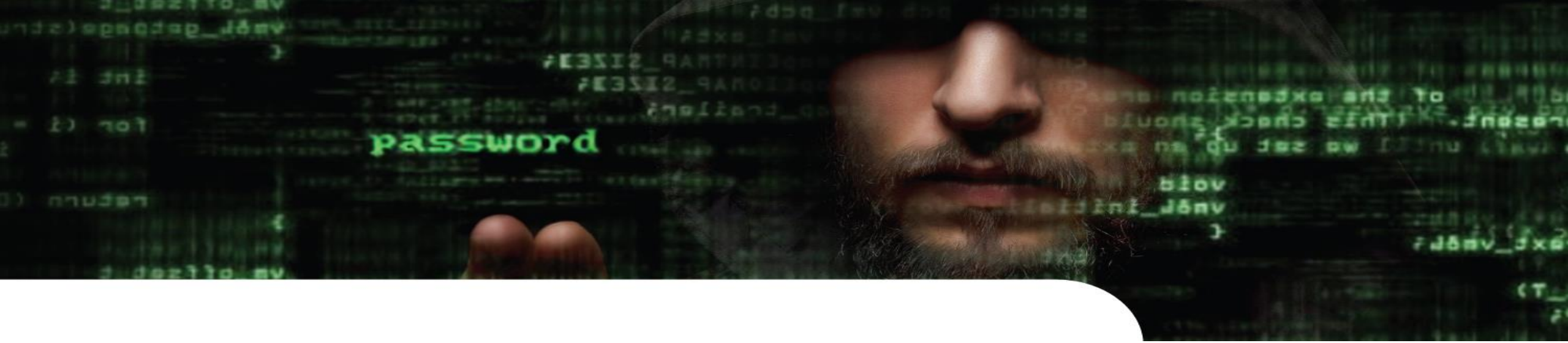
Application	syslogd record identifications	Primary syslog facility	Other syslog facility
Application Transparent Transport Layer Security (AT-TLS)	TTLS	daemon	auth
Automated domain name registration (ADNR)	adnr	daemon	None
Communications Server SMTP (CSSMTP)	CSSMTP	mail	None
Defense Manager daemon (DMD)	DMD	local4	None
FTP server	ftpd, ftps	daemon	None
IKE daemon	IKED	local4	None
NAMED	named	daemon	None
Network security services (NSS) server	NSSD	local4	None
Network SLAPM2 subagent	NSLAPM2	daemon	None
OMPROUTE	omproute	user	None
OPORTMAP server	oportmap	daemon	None
OREXCD	rexecd	daemon	auth
ORSHD	rshd	daemon	auth
OTELNETD	telnetd	local1	auth
Policy Agent	Pagent	daemon	None
POPPER	popper	mail	None
PWCHANGE command	pwchange	daemon	None
PWTOKEY command	pwtkey	daemon	None
rpcbind	rpcbind	daemon	None
SENDMAIL	sendmail	mail	None
Simple Network Time Protocol daemon	sntpd	daemon	None
SNMP agent (OSNMPD)	snmpagent	daemon	None
syslogd	syslogd	daemon	None
TCP/IP subagent	M2SubA	daemon	None
TFTP server	tftpd	user	None
TIMED daemon	timed	user	None
TN3270E Telnet subagent	TNSubA	daemon	None
Traffic Regulation Management Daemon (TRMD)	TRMD	daemon (used for IDS logging)	local4 (used for IPSEC logging and defensive filter logging)
Trap Forwarder daemon	trapfwd	daemon	None
z/OS Load Balancing Advisor	lbadv	daemon	None
z/OS Load Balancing Agent	lbagent	daemon	None

File Transfer

- Another key area is FTP
- Obviously the SERVAUTH profiles help to some extent, but you really need an additional layer of security for FTP/FTPS which you have to write yourself or purchase additional software to get all that you need
- How about sftp and OpenSSH?
- Less support for security here and they need to be carefully considered

SMTP

- How many of you are running SMTP?
- How are you controlling it?
- What would be the business and reputational impact for your company if someone was able to email sensitive data from the mainframe to the outside world?
- 'Panama Papers' anyone?



Other Controls

Other Controls

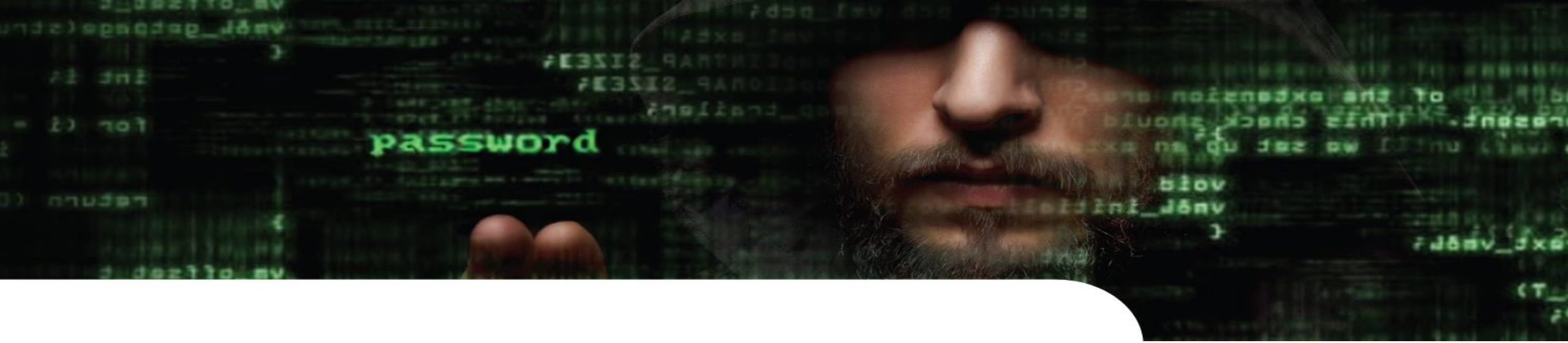
- It's not just about mainframe security controls
- It's about your end-to-end security posture
- You need to work through what a well motivated hacker, or a disgruntled employee may do
- You need to start thinking like them
- It's about the all ecosystem: mainframe, other platforms and devices



What about all the other stuff?

- Subsystems (CICS[®], IMS[™], DB2[®], MQ)
- Scheduler
- Automation
- Source Control and 4 eye checking
- All the ISV products you have...
- How about vulnerability scanning:
 - IBM
 - ISV
 - Internally developed





Real Life Examples

Real Life Examples

- Recently performed a mainframe security audit at a financial institution in Europe (51 risks identified)

Classification	Score
Critical	11
Serious	23
Important	17

- Large number of users with READ access to a daily backup copy of the RACF database, Network controls not properly protected,...

Real Life Examples

- Mainframe security audit at a large energy company in the US this summer (72 risks identified)

Classification	Score
Critical	27
Serious	30
Important	15

- Network controls not defined
- READ access to sensitive data!!

Real Life Examples

- Security analysis of a production RACF DB at a government agency in the UK last month
- 33 security problems identified in the RACF DB
- SERVAUTH class not active!!
- Large number of users with ALTER access to Master Catalog
- All OPERCMDS profiles in Warning mode including JES2.* and MVS.*
- RACF Databases with UACC of READ and several users with ALTER and UPDATE access

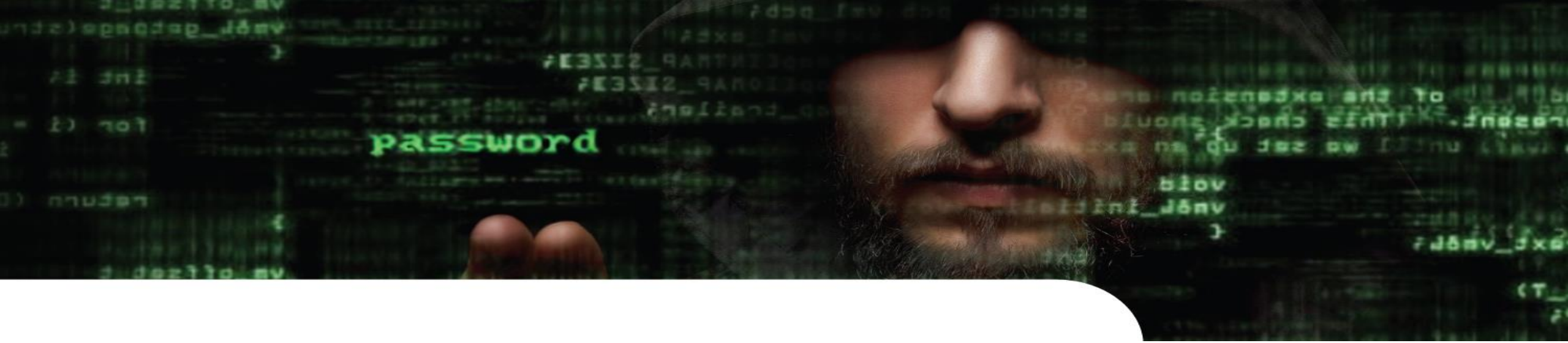
GAME OVER

PLAY AGAIN

CURSE AND SCREAM

▶ BLAME EVERYTHING AND
EVERYONE BUT YOURSELF

SMOSH2



Taking security seriously (or not)

On a nice Sunday morning...



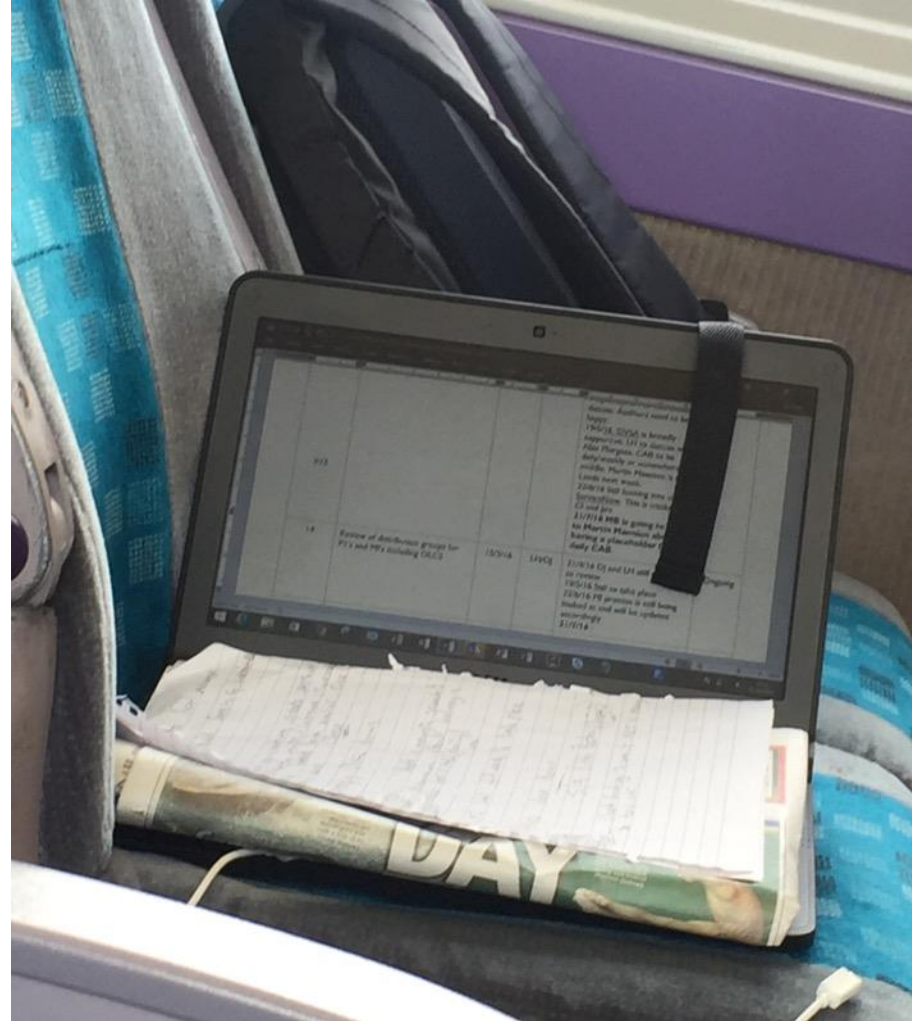
On its TV screen facing the street



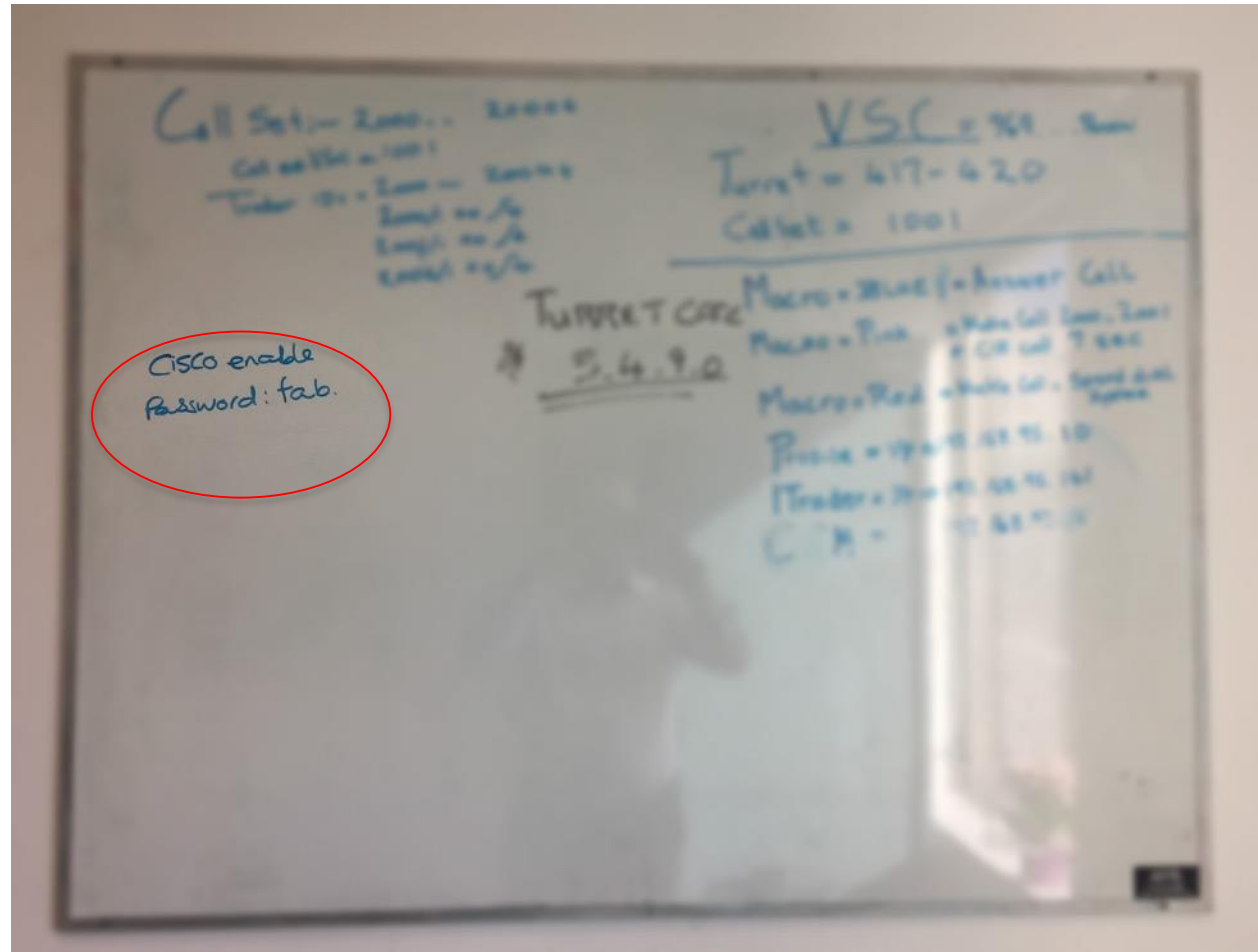
On the train on a business trip...



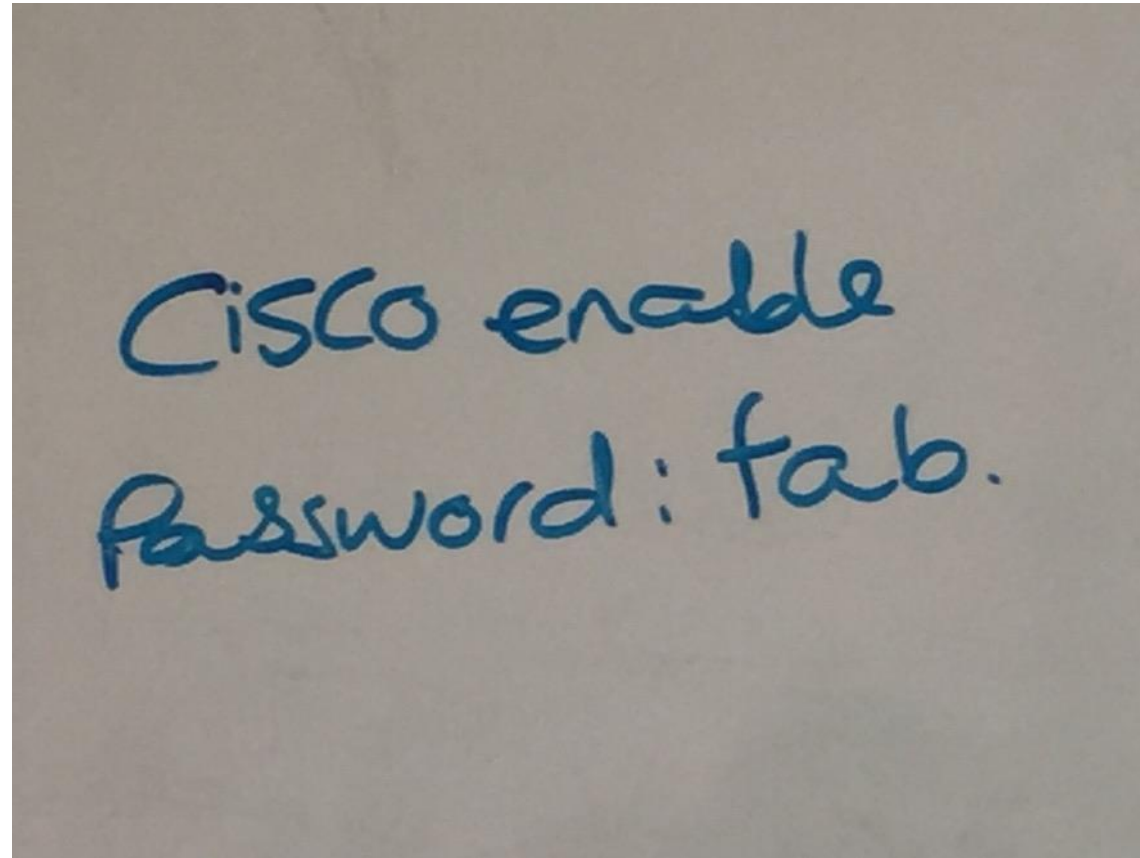
On the train on a business trip...



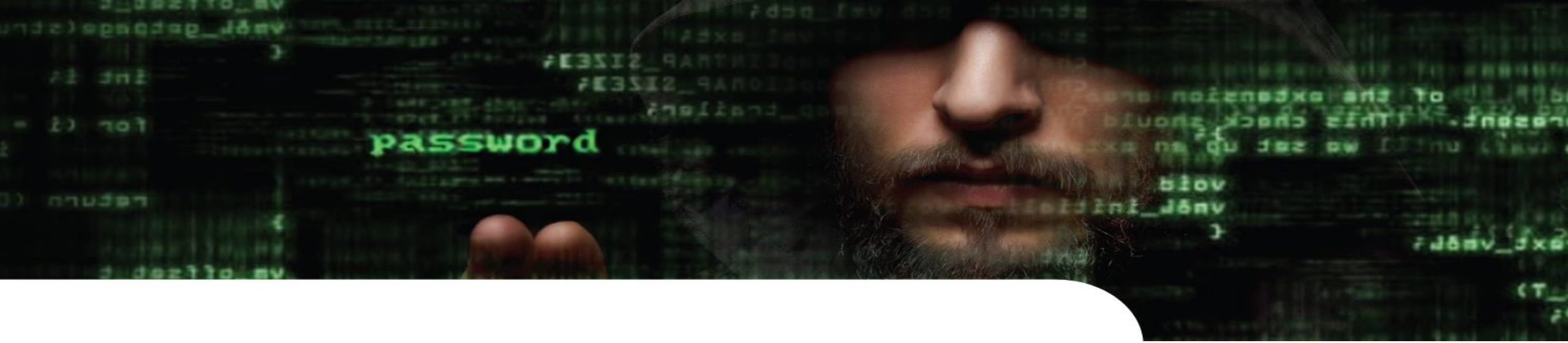
On a site, somewhere in Europe...



On a site, somewhere in Europe...

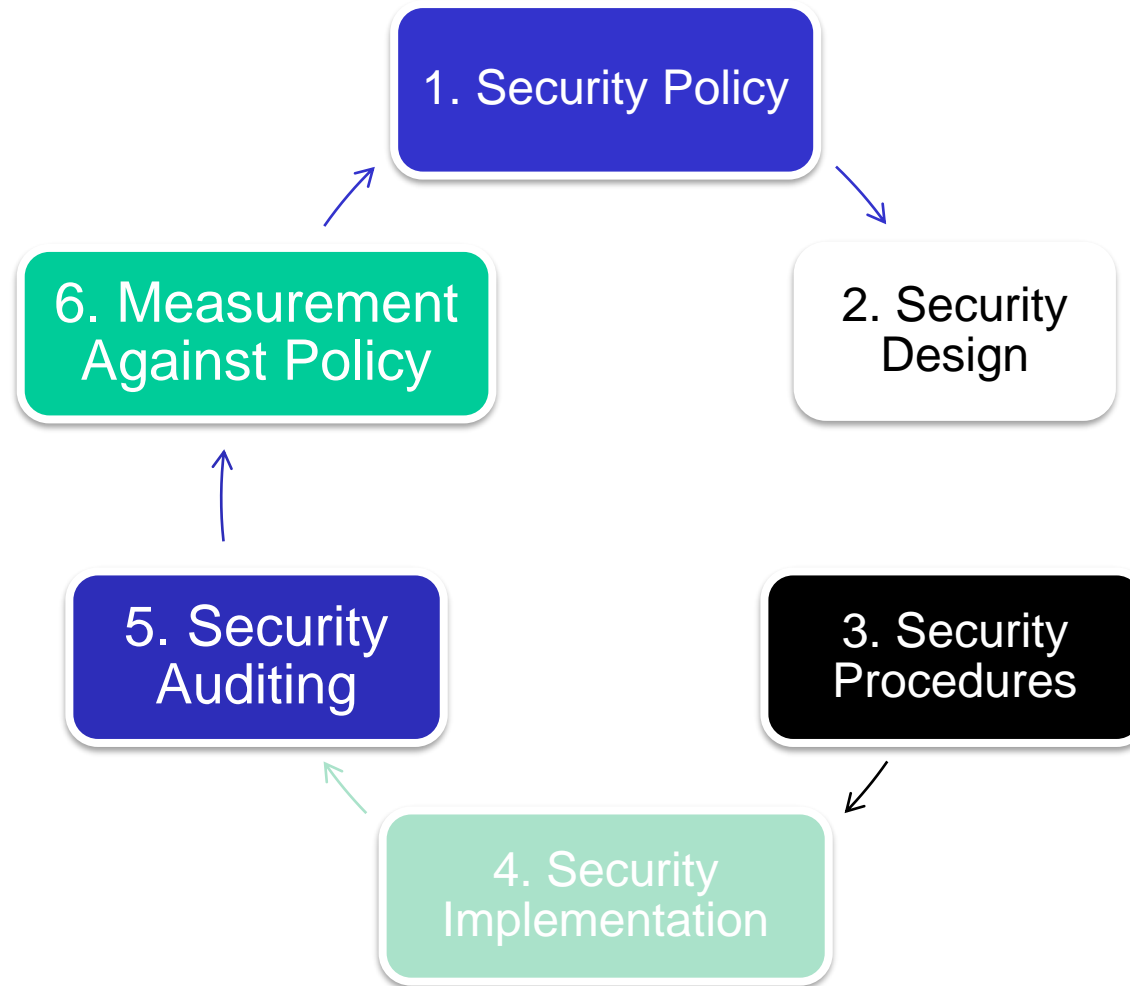
A photograph of a piece of light-colored paper with handwritten text in blue ink. The text is written in a casual, cursive style. The first line reads "Cisco enable" and the second line reads "Password: fab.".

Cisco enable
Password: fab.

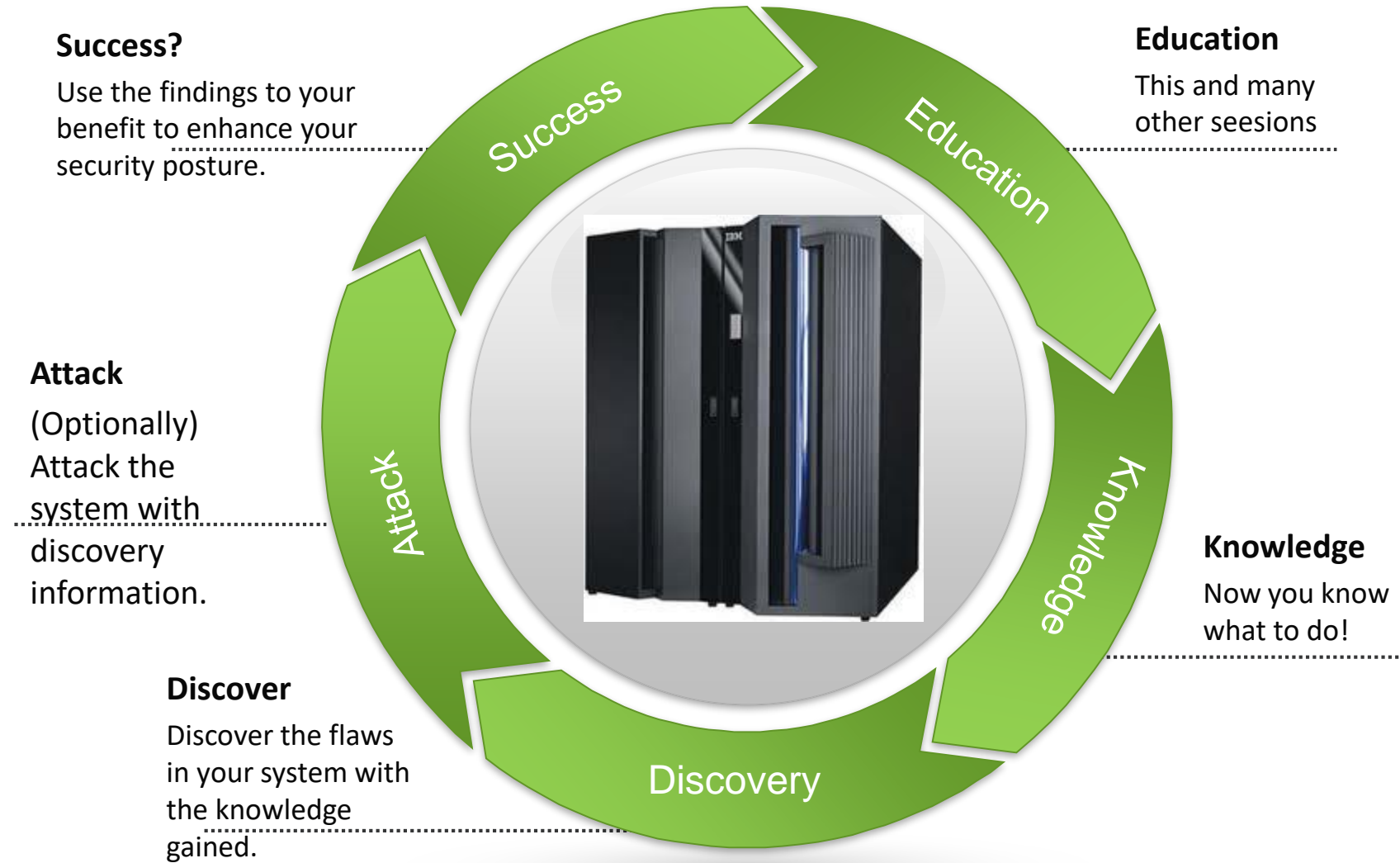


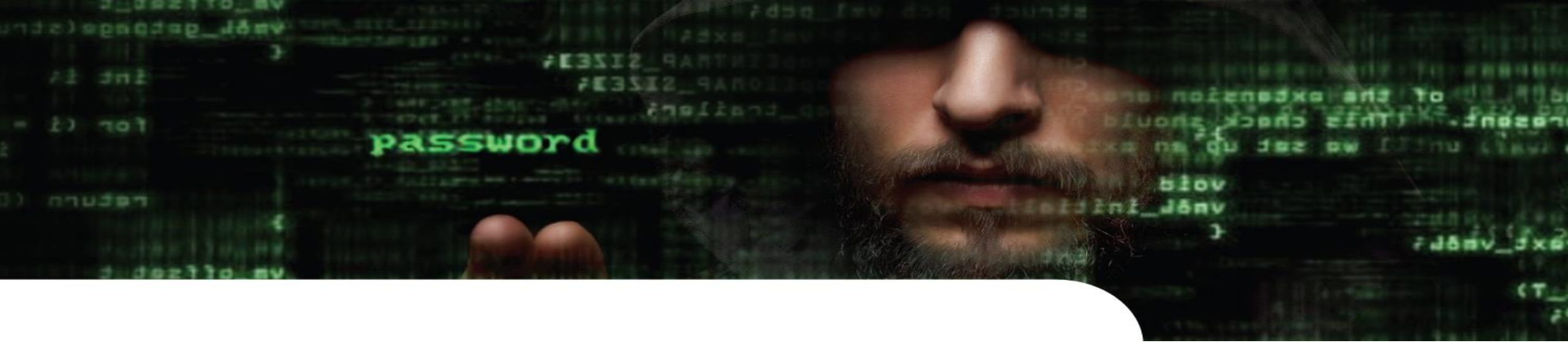
Conclusions

You need a plan



It's a continuous process





Questions

Session Evaluation

Be sure to rate your experience
in the Guidebook app

guidebook

Using the built-in star rating system, and evaluation forms, you'll be able to share your feedback on sessions and speakers.

Your opinions help us to bring you the best possible conference experience. Please let us know your thoughts.

<

Basics of Mainframe Computing Boo...
9-10:30 AM

· How to Create a File

· What is a Batch Job?

Upon completion of this session, the attendee will have an understanding of commands in TSO, be able to navigate in ISPF, be able to create a data set and have a basic understanding of batch jobs. A glossary of terms will be included.

PDFS

Basics of Mainframe Computing Boot Camp >

FORMS

Session Evaluation

Fill out this form

>

SPEAKERS

John Hilman

Vanguard Integrity Professionals; Professional Ser... >

Add to my schedule?

Add now >

<

1

The objectives for this session were clearly stated.

Stongly Agree

Agree

Neutral

Disagree

Strongly Disagree

N/A

Contact

Chad Rikansrud
RSM Partners

Email: chadr@rsmpartners.com
Mobile: (612) 547-0089

www.rsmpartners.com