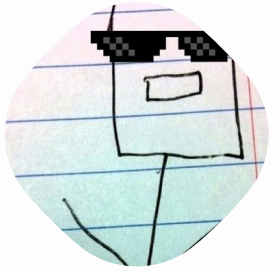
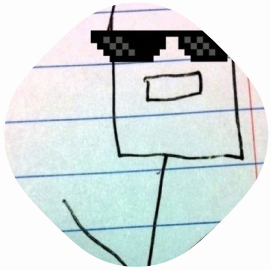

REAL
INCIDENTS
REAL
SOLUTIONS

Our Perspectives



@GHELPLEATJOM4E2

@JQJEOYRNDOANNAME



Building & Assessing Security Programs

Preparing for & Responding to Incidents

Our Story For You

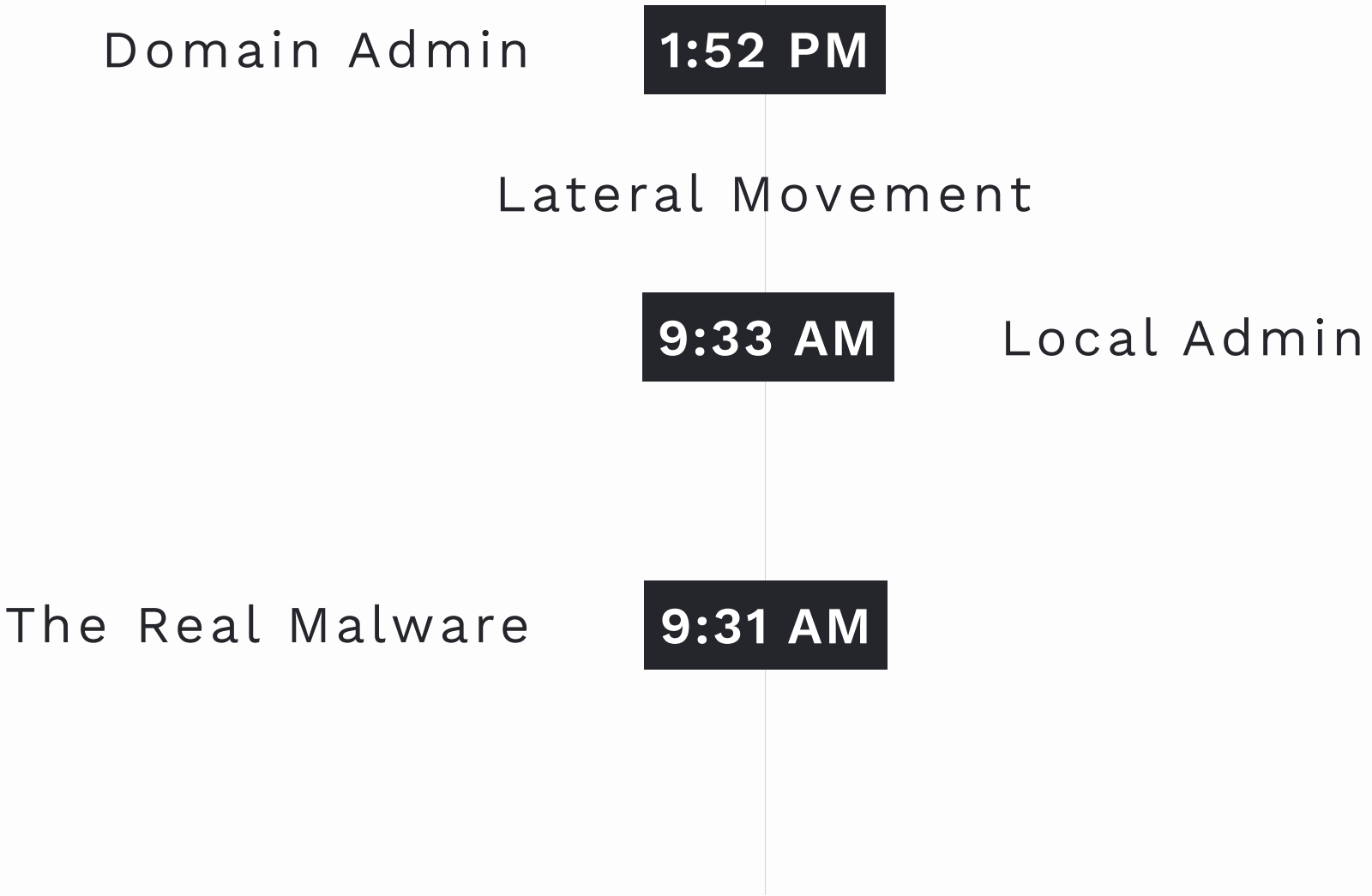
A REALISTIC ATTACK

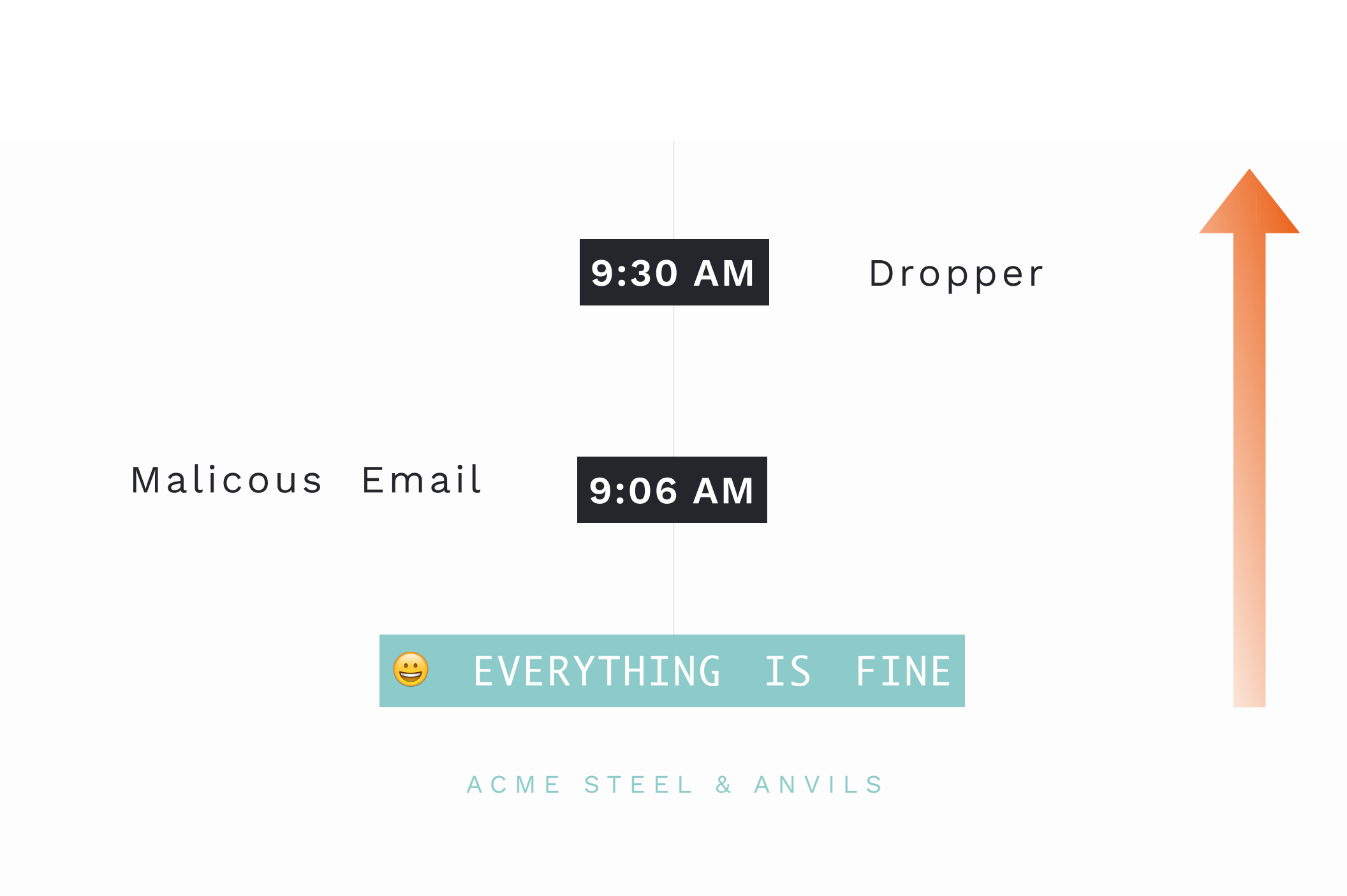
7 PM: 💩

AS&A's IP stolen by competitor

MRP Database Accessed

4:52PM

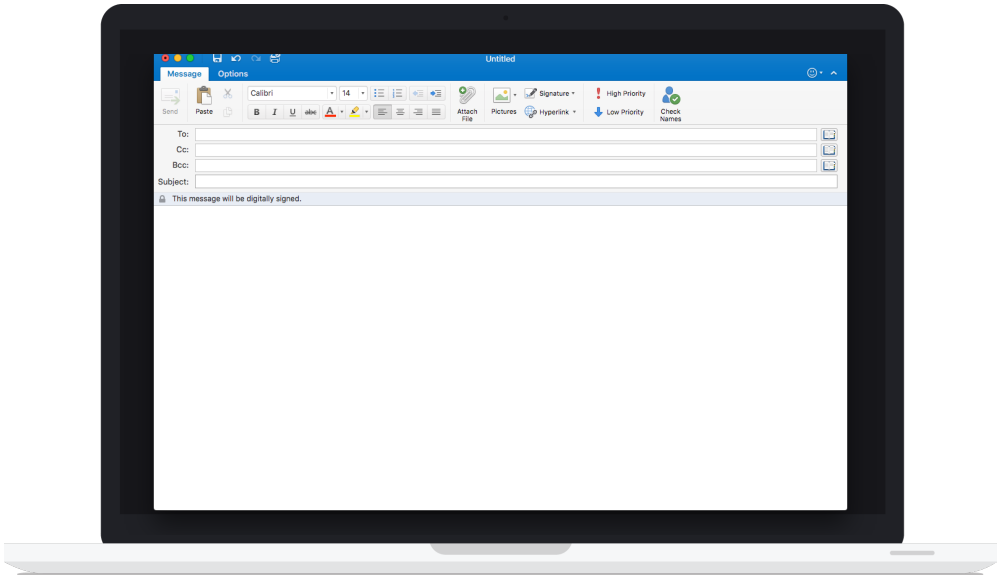

Domain Admin
1:52 PM
Lateral Movement
9:33 AM
Local Admin
The Real Malware
9:31 AM


9:30 AM
Dropper
Malicous Email
9:06 AM
😀 EVERYTHING IS FINE
ACME STEEL & ANVILS

NEXT GEN & BOURBON

Step 1
The Email

From:
Invoicing@Mining.Biz



Typical Defenses

- Anti Spam
- Mail Av
- Endpoint Av
- Sandboxing Technology
- User Awareness

Step 1
The Email Could be...

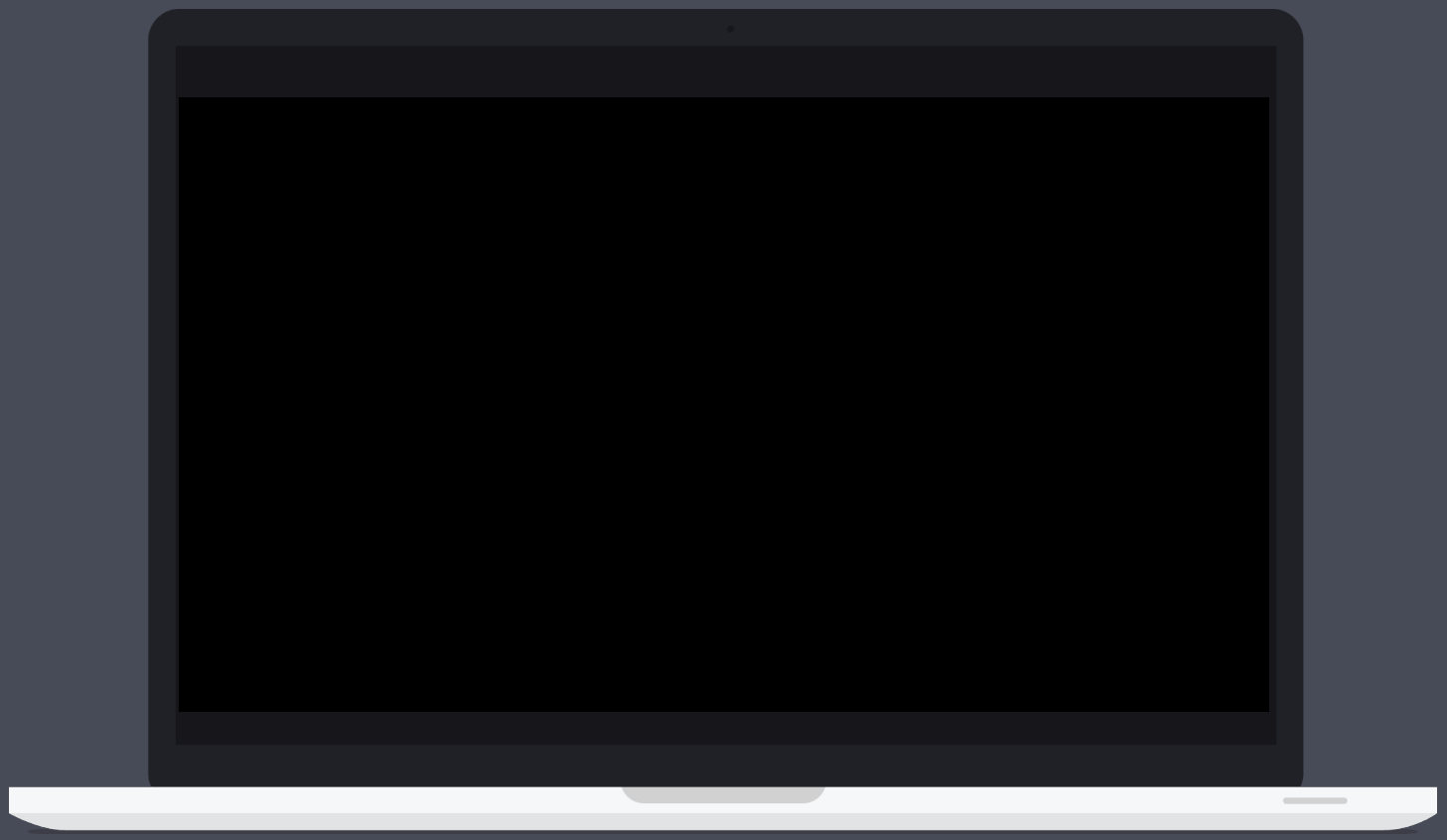
- Ceo Scam
- Malicious Link
- Attachment: Word

- Block Macros (Gpo)
- Harden Office
- Emet: Office

FREE

&

EFFECTIVE



- Click-To-Play
- Whitelist Sites For Plugins
- Deny Old Plugins
- Gpo Available 👍🏻
- Emet Me Too!

FREE

&

EFFECTIVE

- Unclassified Sites
- Recently Registered Dns
- File Type Blocking (.Zip/ Encrypted)
- Link Rewriting

Extra Config

Step 2
Dropper Fetches Malware

https://EvilPlumbing/Lol.Exe

Typical Defenses

- NGFW
- Proxy
- Endpoint AV
- Sandboxing Technology

- Dns/Proxy Stuff
- Tls/Ssl Decryption
- Disallow Exe Downloads
- Block Ads!

Extra Config

Step 3
Real Malware Runs

Credentials Harvested

Typical Defenses

- Endpoint Av
- Advanced Endpoint Things (Tm)
- Ngfw

- Regular Users.
- Vulnerability Management Basics
- Da On Workstations: Not Even Once
- Lsa Hardening
- Windows Device Guard

FREE DEFENSE

Step 4
Local Admin Privileges

?

Typical Defenses

- Everything We Said Before
- Randomize Local Admin With Laps
- Be Careful With Deployment And Logon Scripts/Gpp
- Hardening

FREE DEFENSE

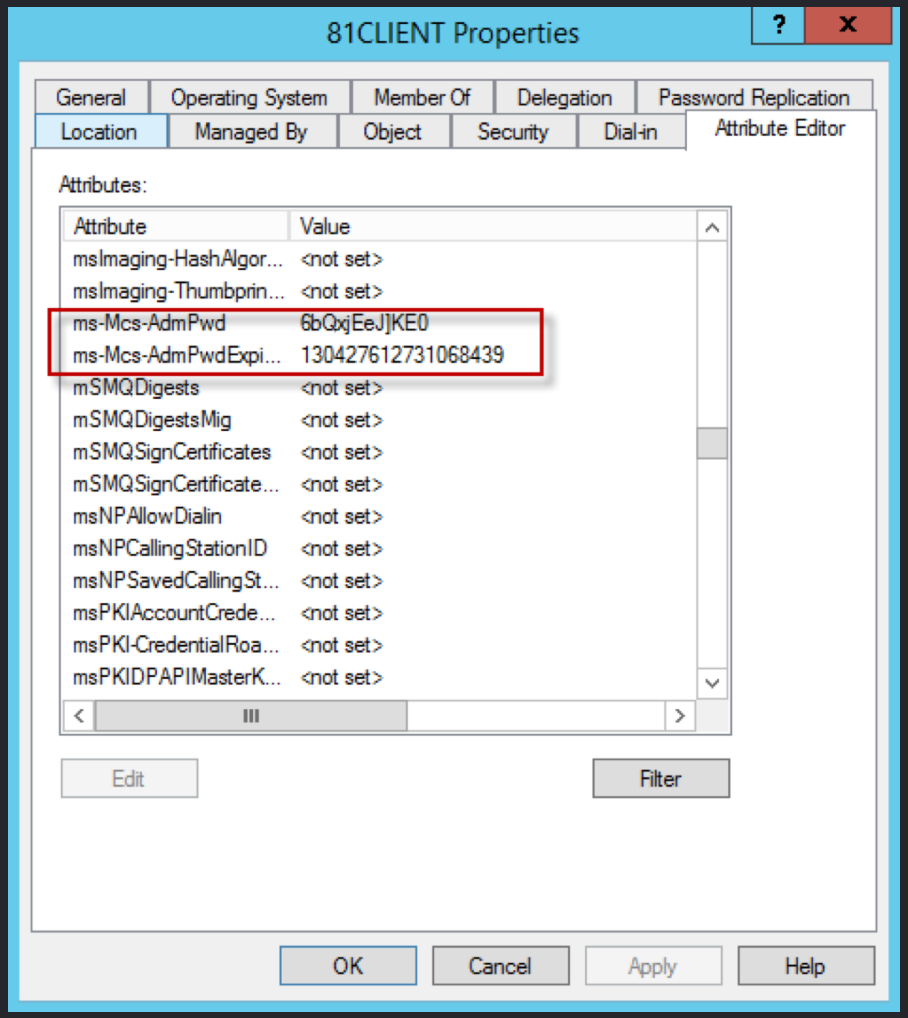
LOCAL ADMINISTRATOR PASSWORD SOLUTION

LAPS

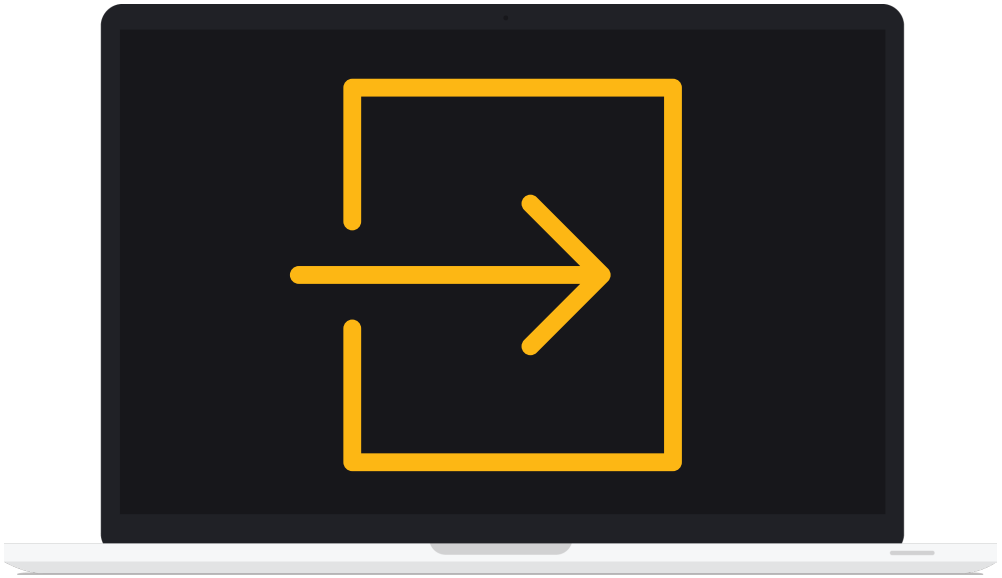
- Randomized
- Automated
- Delegated
  (ms-MCs-AdmPwd)
- FREE as in BEER
  (As in Free beer)

LOCAL ADMINISTRATOR PASSWORD SOLUTION

LAPS



Step 4.5
Lateral Movement



?

Typical Defenses

- Hardening! User Right Assignments! Yay!
- Local Accounts -> Deny All The Things
- Why U No Firewall Smb/Wmi/Netbios?

FREE DEFENSE

Step 5
DOMAIN Admin Privileges

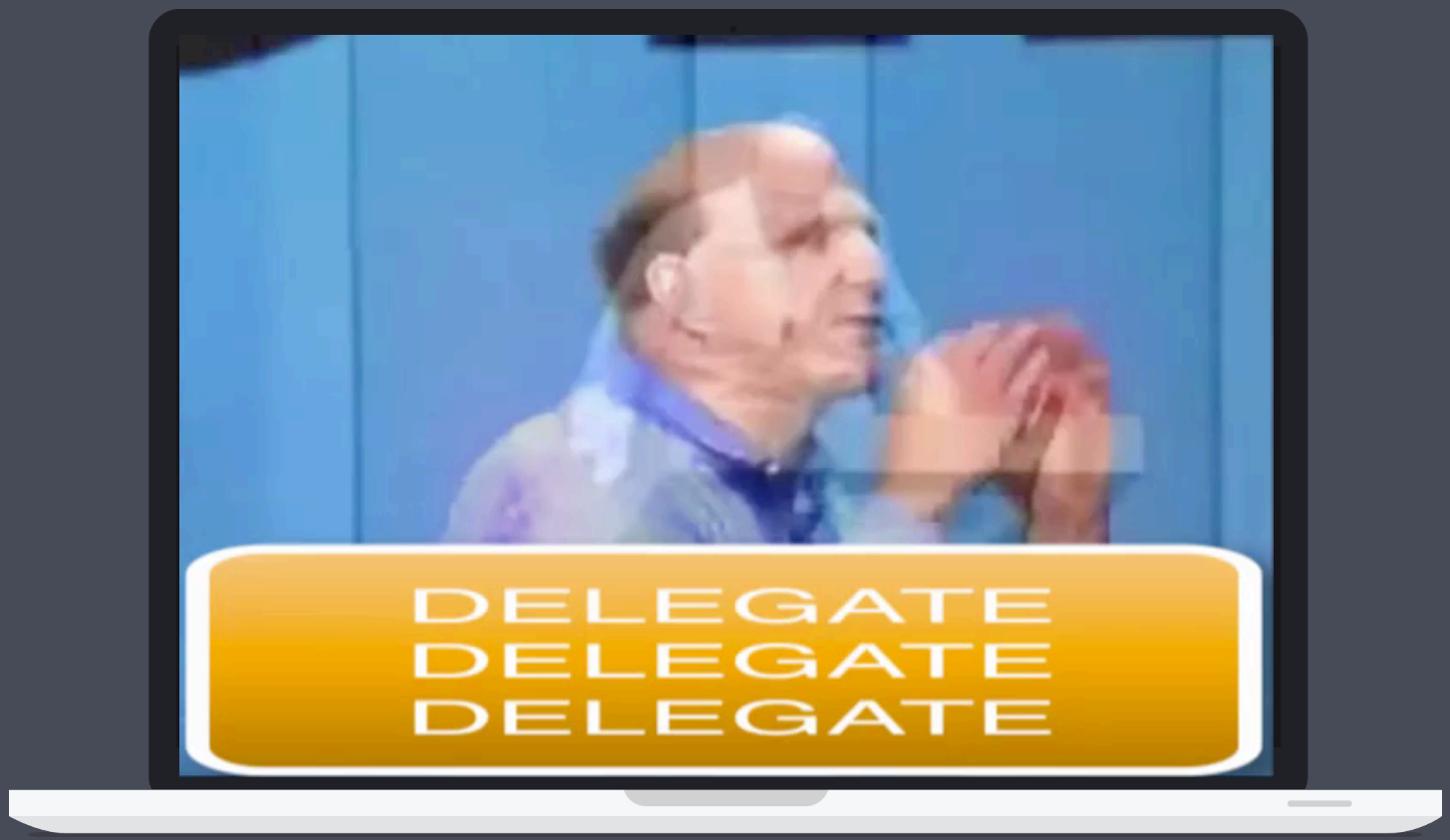
Typical Defenses

- "We Monitor Modifications To The Domain/Enterprise Admins Group"
- "We Use Multiple Domains For Separation"

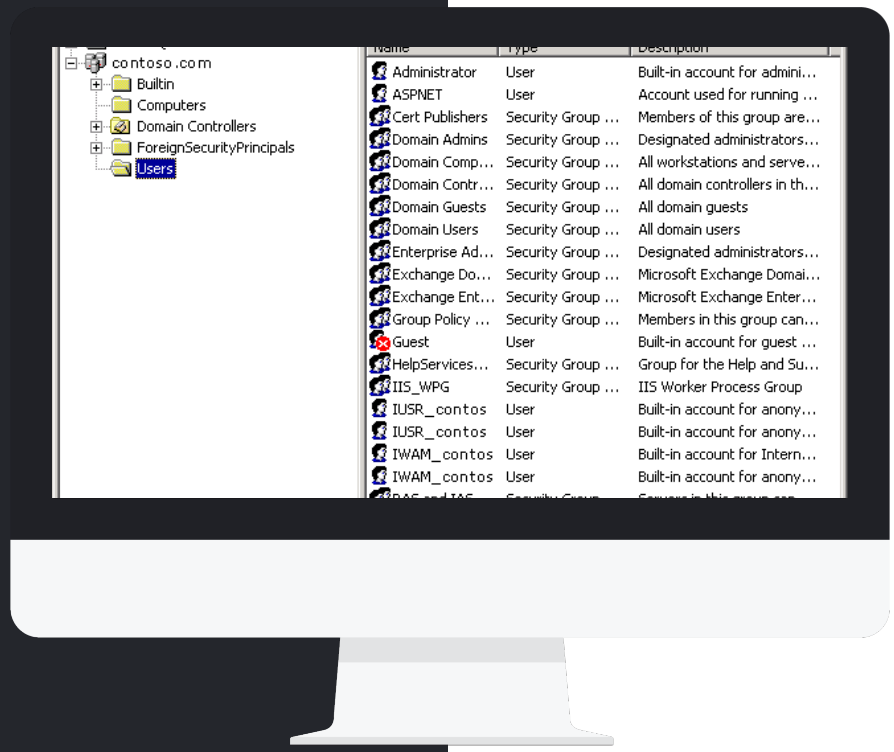
Domains are not security boundaries, forests are.
Domains are not security boundaries, forests are.
Domains are not security boundaries, forests are.
Domains are not security boundaries, forests are.
Domains are not security boundaries, forests are.
Domains are not security boundaries, forests are.
Domains are not security boundaries, forests are.
Domains are not security boundaries, forests are.
Domains are not security boundaries, forests are.
Domains are not security boundaries, forests are.
Domains are not security boundaries, forests are.

- Seriously: Separate Your Service Accounts
- Patch Domain Controllers Like Mad Max Would
- Delegate Delegate Delegate Delegate
- Dedicated Admin Boxes

FREE DEFENSE


DELEGATE
DELEGATE
DELEGATE

PRIVILEGED ACCESS WORKSTATIONS

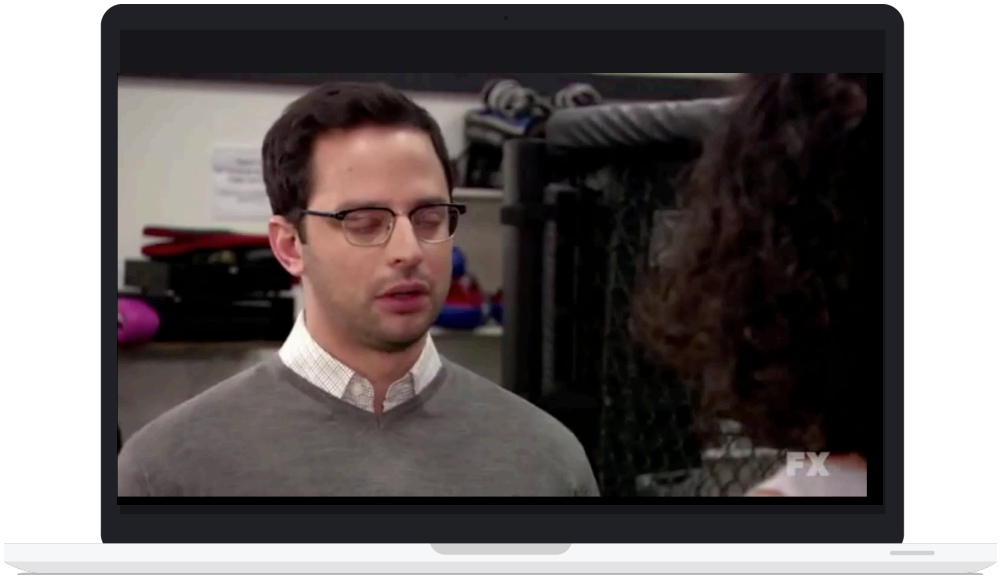


MORE INFO

https://technet.microsoft.com/en-us/library/mt634654.aspx

Step 6
MRP Database Accessed

(and Dumped)



Typical Defenses

- Hoping That Someone Dumping The Db Slows It Down Enough For Someone To Notice
- Some Network Segmentation

- Firewall That Stuff
- Encrypt Connection Strings + Use Tls
- Monitor Events & Performance

FREE DEFENSE

Step 7
All your (data) Base are belong to theM

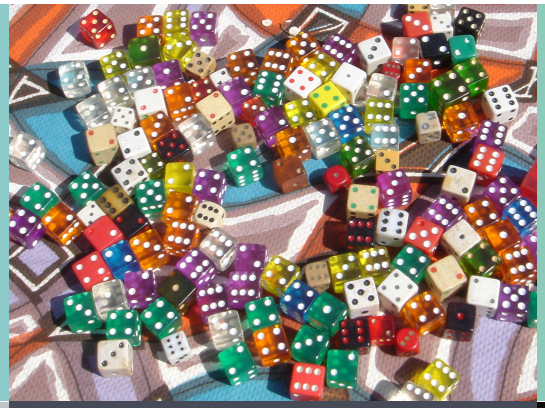
Typical Defenses

- DLP (?)
- Limited Egress Filtering

- Egress Filtering!
- No Seriously, Why Can Your Servers Connect Back To The Net?
- Proper Zoning
- Monitor Wwroots

FREE DEFENSE

SEGMENT SYSTEMS

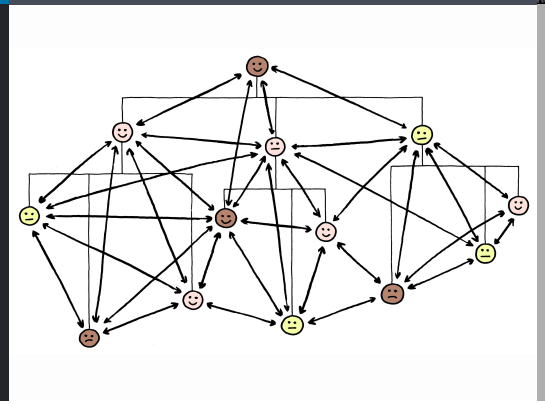


EGRESS + WEB FILTER

CHECK PRIVILEGES

RANDOMIZE PASSWORDS

DELEGATE



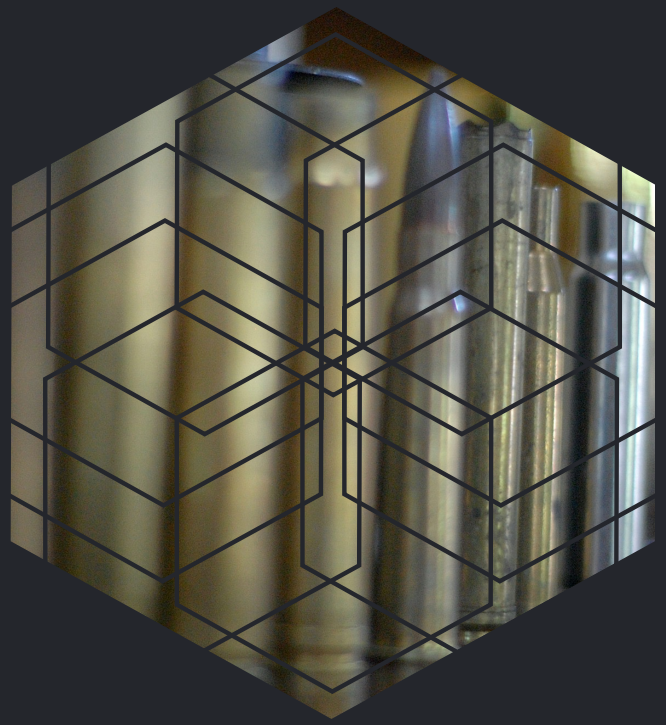
HARDEN SYSTEMS

CONCLUSION

2016–2017 CHALLENGE

LESS BULLETS

MORE SHOVELS



THANK YOU

Troll Us

@Gepeto42

@Joeynoname

Slides And Links: Https://Evil.Plumbing