PAINT IT, BLUE

Transitioning from CTI to HUNT

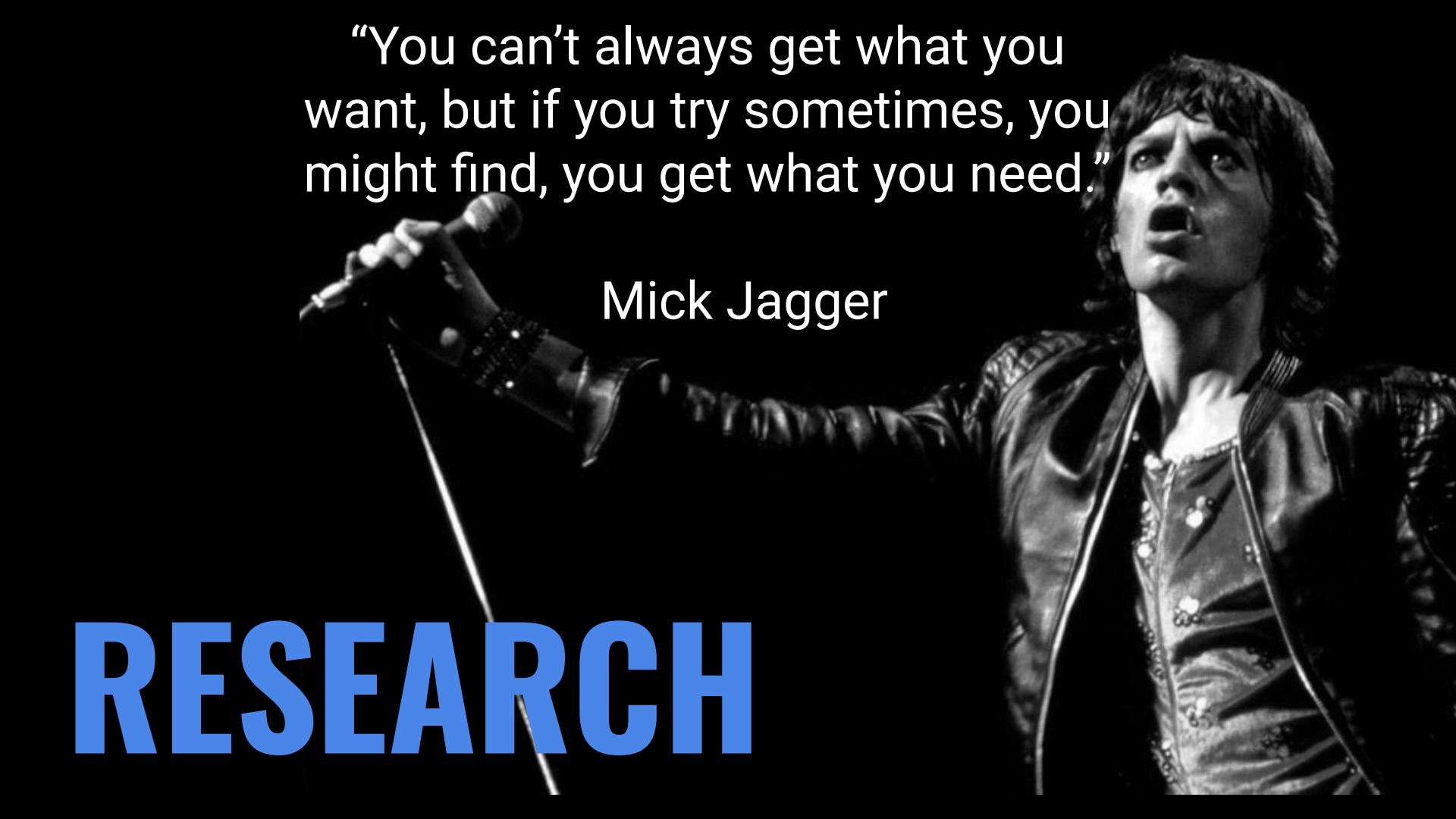
FOR THE LAWYERS

“The opinions expressed in this presentation are those of the presenter, in their individual capacity, and not necessarily those of my employers.”
Use of SCYTHE’s Purple Team Exercise Framework (PTEF) in this talk does not endorse them as a vendor.


TECHNICAL
CHOPS

TAKE ME DOWN TO THE THREAT HUNTING CITY

01 **RESEARCH** Rock’n SOLO	02 **PRACTICE** Pick your set list
03 **RIFF WITH THE PROS** Get set straight...no really.	04 **ROCK’N OUT** Booking a gig


“You can’t always get what you want, but if you try sometimes, you might find, you get what you need.”
Mick Jagger
RESEARCH

GOAL = ASK BETTER ?'s

SOCIAL MEDIA & MORE

#HuntingTipOfTheDay
Follow Threat Hunting Accts EVERYWHERE

SANS

Reading Room & Threat Hunting Summit

WORKSHOPS/TALKS

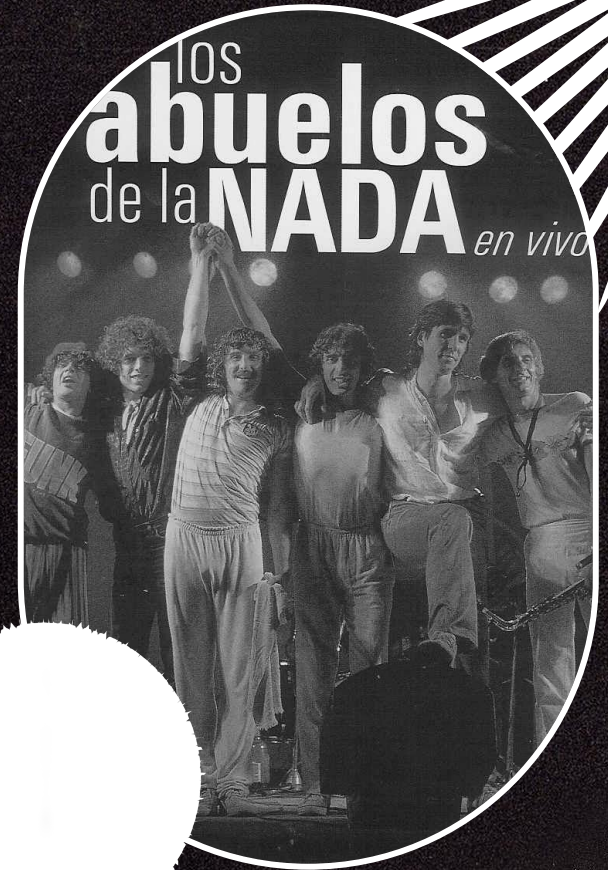
Prioritize Threat Hunting Talks/ Workshops
*YOUTUBE is a friend

DISCORDS/SLACKS

FREE Community Resources

SOME ACCOUNTS TO FOLLOW ON

@blackmatter23
@blueteamsec1
@Cyb3rMonk
@Cyb3rWard0g
@CyberWarship
@DavidJBianco
@JohnLaTwC
@MichalKoczwara
@nas_bench
@SBousseaden
@thedfirreport
@threathunting_
@Wietze



CROWDSTRIKE

Nowhere to Hide

2021 Threat Hunting Report

Insights From the Falcon OverWatch Team

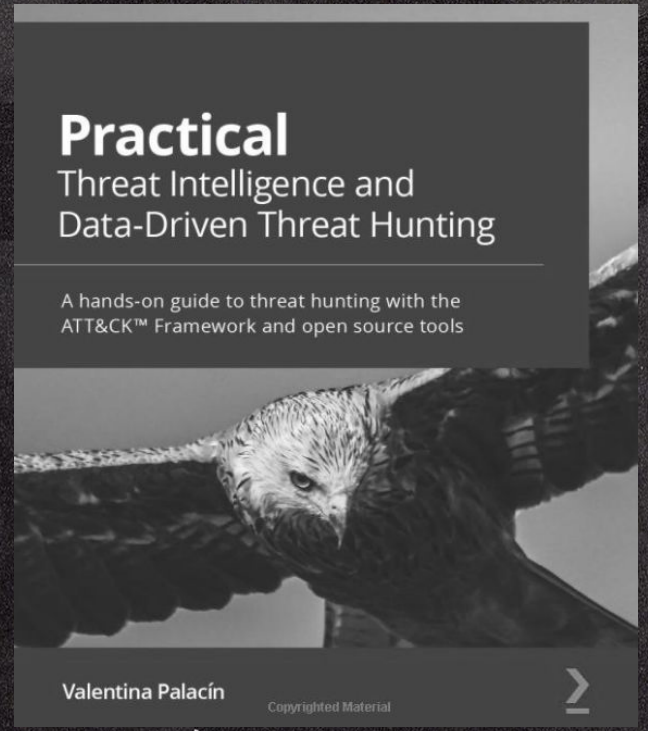
Red Teaming Experiments

#ThreatThursday

SCYTHE

READ

Everything you can



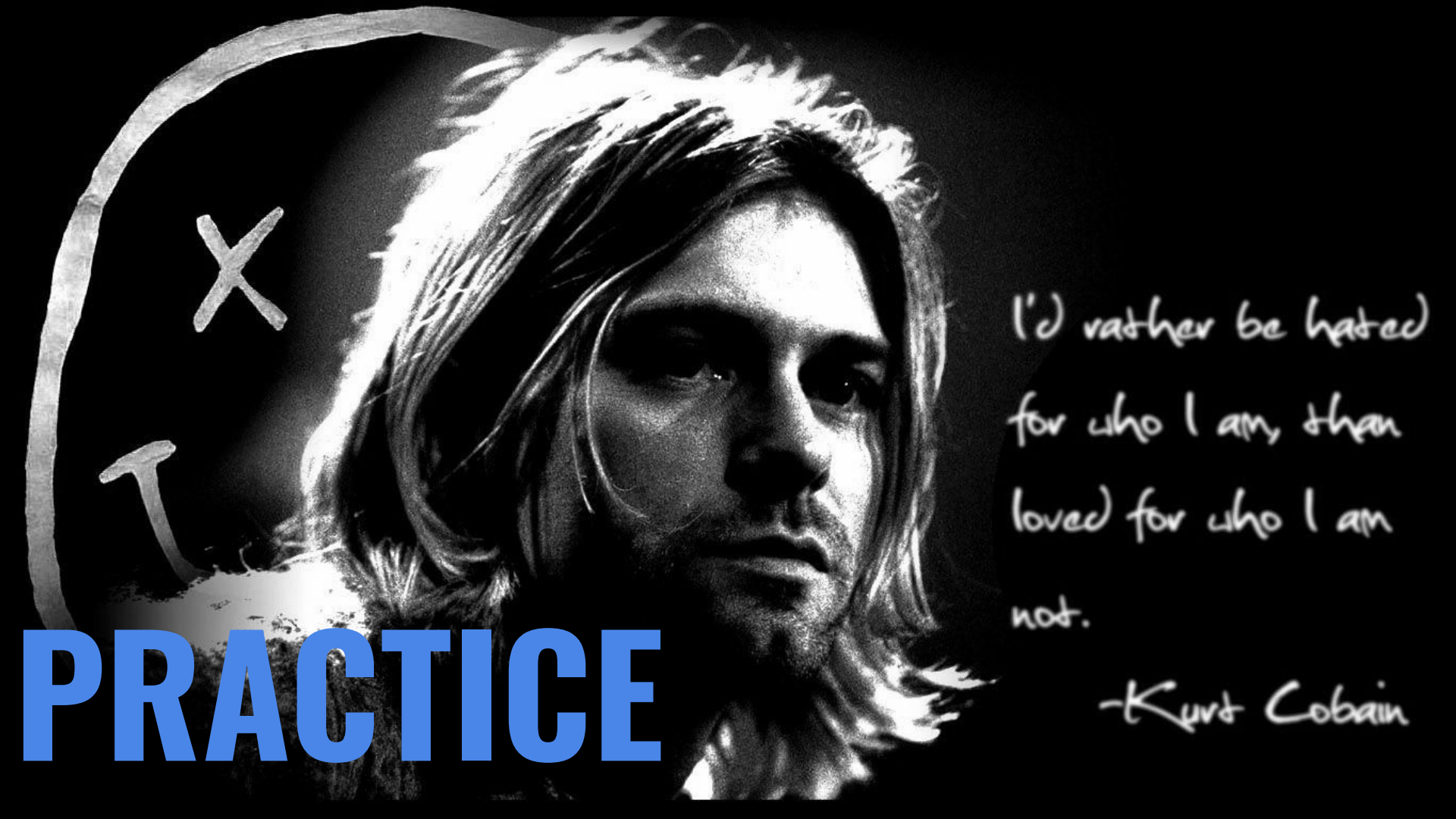
DFIR Report

SIGMA

THREAT HUNTER Playbook

Threat Hunter Playbook

ATT&CK®


I'd rather be hated
for who I am, than
loved for who I am
not.
-Kurt Cobain

PRACTICE

GOAL = PREPARATION

WORK PROJECTS

- ★ SOC tickets
- ★ Volunteer to prep CTI reports 4 Hunt/Purple

HUNT HYPOTHESIS DEV

- ★ Read Threat Reports & Think about how YOU would HUNT it.
- ★ Understand Technical Attack Chain

TRAININGS/HANDS-ON

- ★ Boss of the SOC (BOTS)!
- ★ ATTACK RANGE
- ★ SPLUNK

GIVE A TALK

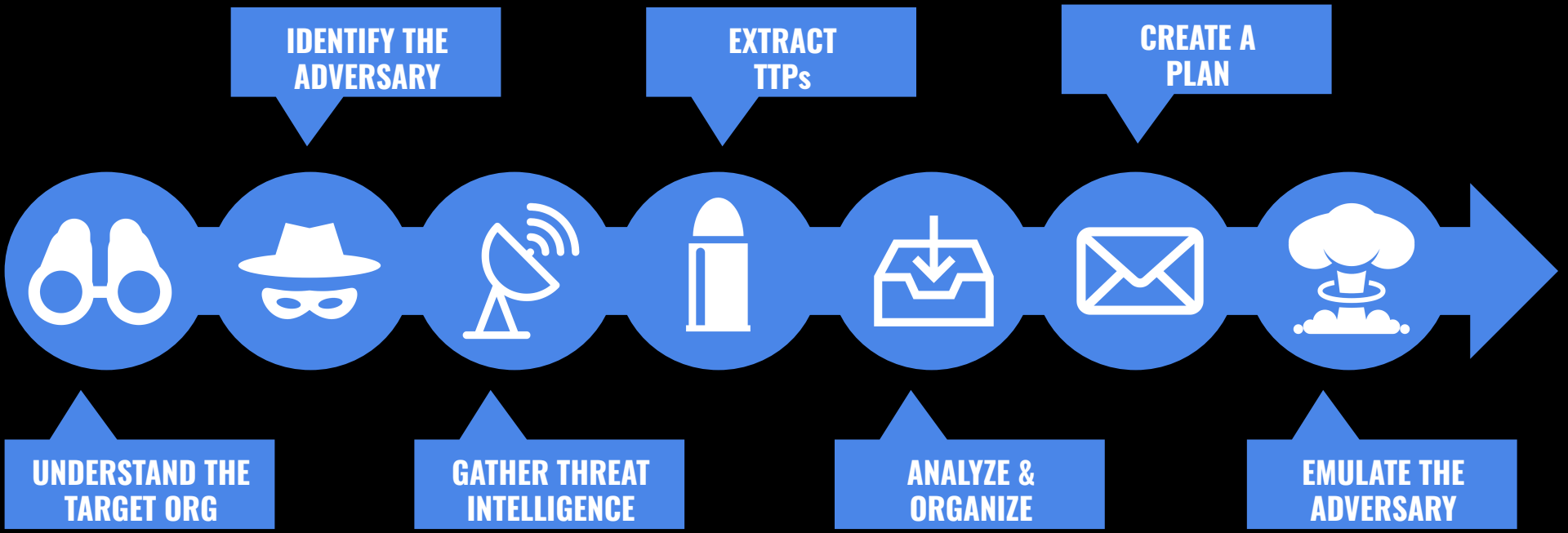
- ★ Talk about something HUNT adjacent

HUNT HYPOTHESIS DEV

What would this badness look like?
Where would I find it?

***Once I got the gig...now I also ask:
How do I do the needful?
Translation: What's that search gonna look like?

THREAT INTEL PROCESS



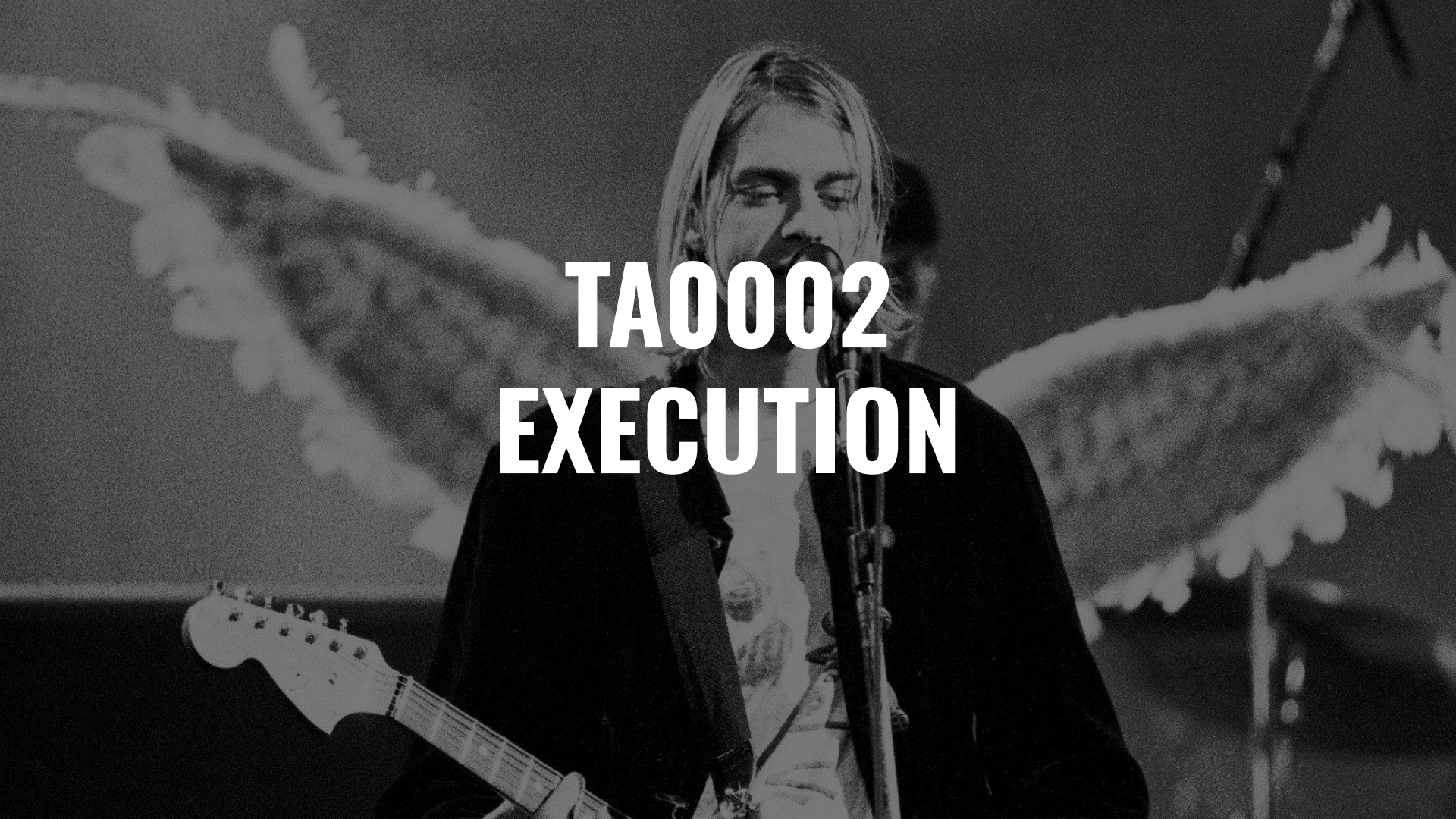
ERIK VAN BUGGENHOUT (@ErikVaBu), Co-Founder at NVISO

MITRE ATT&CK TACTICS

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media 1	Windows Management Instrumentation 1	DLL Side-Loading 1	Process Injection 3 1 1	Masquerading 1	Input Capture 2 1	Security Software Discovery 3 1	Replication Through Removable Media 1	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Modify Registry 1	LSASS Memory	Virtualization/Sandbox Evasion 4	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Remote Access Software 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 4	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1	NTDS	Peripheral Device Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 3 1 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 2 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 2 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	DLL Side-Loading 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact


TA0001
INITIAL ACCESS


TA0002
EXECUTION

T1047 WMI - Windows Management Instrumentation

Checks if AV/Antispyware/Firewall program is installed

WMI Operations

Time	TID	User	Operation
	2896	computer\user	IWbemServices::Connect
	2896	computer\user	IWbemServices::ExecQuery - root\SecurityCenter2 : SELECT * FROM AntivirusProduct
	2896	computer\user	IWbemServices::Connect
	2896	computer\user	IWbemServices::ExecQuery - root\SecurityCenter2 : SELECT * FROM FirewallProduct
	2896	computer\user	IWbemServices::Connect
	2896	computer\user	IWbemServices::ExecQuery - root\cimv2 : select * from Win32_OperatingSystem

STACKOVERFLOW
Wmic /Node:localhost
/Namespace:\\root\SecurityCenter2:SELECT*FROM AntivirusProduct
Wmic /Node:localhost
/Namespace:\\root\SecurityCenter2:SELECT*FROM FirewallProduct

ATOMIC RED TEAM T1518.001
Wmic /Namespace:\\root\SecurityCenter2 Path AntivirusProduct Get
displayName /Format:List


TA0004
PRIVILEGE ESCALATION

T1055 PROCESS INJECTION

- Injects a PE file into a foreign processes
- Maps a DLL or memory area into another process
- Writes to foreign memory regions
- Creates Process in suspended mode
- Spawns Processes

C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext ‘C:\Users\user\AppData\Local\Temp\holdermail.txt’

Rule name:	RAT_HawkEye
Author:	Kevin Breen <kevin@techanarchy.net>
Description:	Detects HawkEye RAT
Reference:	http://malwareconfig.com/stats/HawkEye

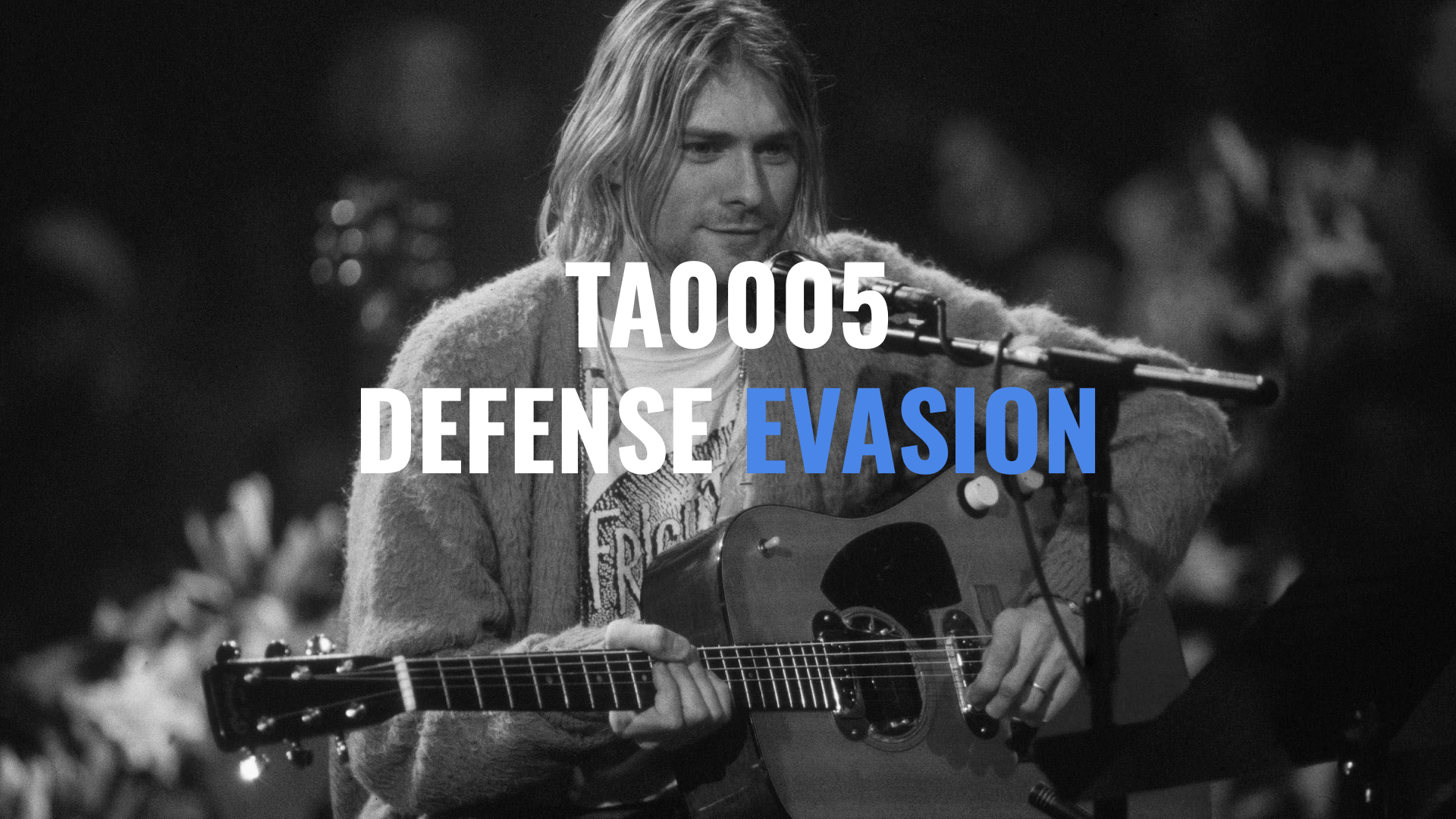
```
ye

ta:
        author = " Kevin Breen <kevin@techanarchy.net>"
        date = "2015/06"
        ef = "http://malwareconfig.com/stats/HawkEye"
        maltype = "KeyLogger"
        filetype = "exe"

strings:
        $key = "HawkEyeKeylogger" wide
        $salt = "099u787978786" wide
        $string1 = "HawkEye Keylogger" wide
        $string2 = "holdermail.txt" wide
        $string3 = "wallet.dat" wide
        $string4 = "Keylog Records" wide
$string5 = "<!-- do not script -->" wide
$string6 = "\\pidloc.txt" wide
$string7 = "BSPLIT" wide
```

2015 😱

Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext "C:\Users\user\AppData\Local\Temp\holdermail.txt"


TA0005
DEFENSE EVASION

T1036 MASQUERADING

Creates files inside user directory

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\08FDeU25BO.exe.log


TA0006
CREDENTIAL ACCESS

T1555.003 CREDENTIALS FROM WEB BROWSERS

Steals PRIVATE Info from Browsers

file: C:\Users\Rebecca\AppData\Roaming\Mozilla\Firefox\Profiles\48wgv2fv.default\pkcs11.txt
file: C:\Users\Rebecca\AppData\Roaming\Mozilla\Firefox\profiles.ini
file: C:\Users\Rebecca\AppData\Roaming\Mozilla\Firefox\Profiles\48wgv2fv.default\key4.db
file: C:\Users\Rebecca\AppData\Roaming\Mozilla\Firefox\Profiles\48wgv2fv.default\cert9.db
file: C:\Users\Rebecca\AppData\Local\Google\Chrome\User Data\Default\Login Data
file: C:\Users\Rebecca\AppData\Local\Google\Chrome\User Data\Default\Web Data
file: C:\Users\Rebecca\AppData\Roaming\Mozilla\Firefox\Profiles\48wgv2fv.default\signons.sqlite

TA0009
COLLECTION

T1114.001 LOCAL EMAIL COLLECTION

Harvests Installed Mail Clients Info

file: C:\Users\Rebecca\AppData\Local\Microsoft\Windows Live Mail*.oeaccount
file: C:\Users\Rebecca\AppData\Local\Microsoft\Windows Live Mail*.*
key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles
key: HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\OMI Account Manager\Accounts
key: HKEY_CURRENT_USER\Identities\{933F0607-9D78-4B29-A477-143EB7D69AEA}\Software\Microsoft\Office\Outlook\OMI Account Manager\Accounts
key: HKEY_CURRENT_USER\Software\Microsoft\Internet Account Manager\Accounts
key: HKEY_CURRENT_USER\Identities\{933F0607-9D78-4B29-A477-143EB7D69AEA}\Software\Microsoft\Internet Account Manager\Accounts

TA0011
COMMAND & CONTROL

C2 MATRIX

THEC2MATRIX.com

C2	TCP	HTTP	HTTP2	HTTP3	DNS	DoH	ICMP	FTP	IMAP	MAPI	SMB
Apfell	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	
Caldera	✗	✓	✗	✗	✗	✗	✗	✗	✗		
Cobalt Strike	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓
Covenant	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓
Dali	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
Empire	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	
EvilOSX	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	
Faction C2	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	
FlyingAFalseFlag	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	
godoh	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	
ibombshell	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗	
INNUENDO	✗	✓	✗	✗	✓	✗	✓	✓	✓	✓	✓
Koadic C3	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	

TA0010
EXFILTRATION


TA0040
IMPACT

Steven Tyler

It's amazing
With the blink of an eye
You finally see the light
It's amazing
That when the moment arrives
You know you'll be alright
It's amazing
And I'm saving a prayer
For the desperate hearts tonight

PRO

Coyote

GOAL = PRO TIPS

TIME = $

Be the best MENTEE EVER!

With **TIME FRAME** XYZ
what would you suggest?

QUESTIONS = SPECIFIC
W/ OUTCOMES/GOALS

INTEGRATE FEEDBACK

Rinse & Repeat until you are a resource.

Remember to let the PRO know how their time impacted your life!

Muchas Gracias @plugxor <3

Soda Stereo

GET A GIG

“I spent my life imagining, this is no time to be a coward.“

Gustavo Cerati


BUILD ON YOUR
CTI SKILLS

THE NEXT STEP FOR ME....

Processes, Windows Event IDs, Sysmon, Registry Keys & MORE.

GOAL = APPLICATION INTERVIEW PREP!

MITRE ATT&CK Techniques

Pick a few and be able to explain them in DETAIL

CISA/PUBLIC THREAT REPORTS

Hunt Hypotheses with 1 hour content to discuss.

INFOSEC CURRENT EVENTS

Dev hunt scenarios & understand technical attack chain

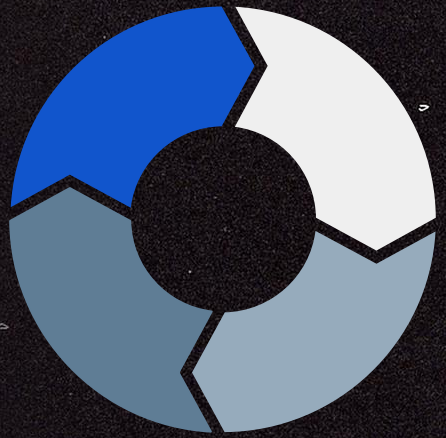
CH33R10'S THREAT HUNTING CYCLE

DETECTIONS

Automate the hunts you can.

RESEARCH

Hypothesis generation, understanding the technical details



CONCLUSIONS

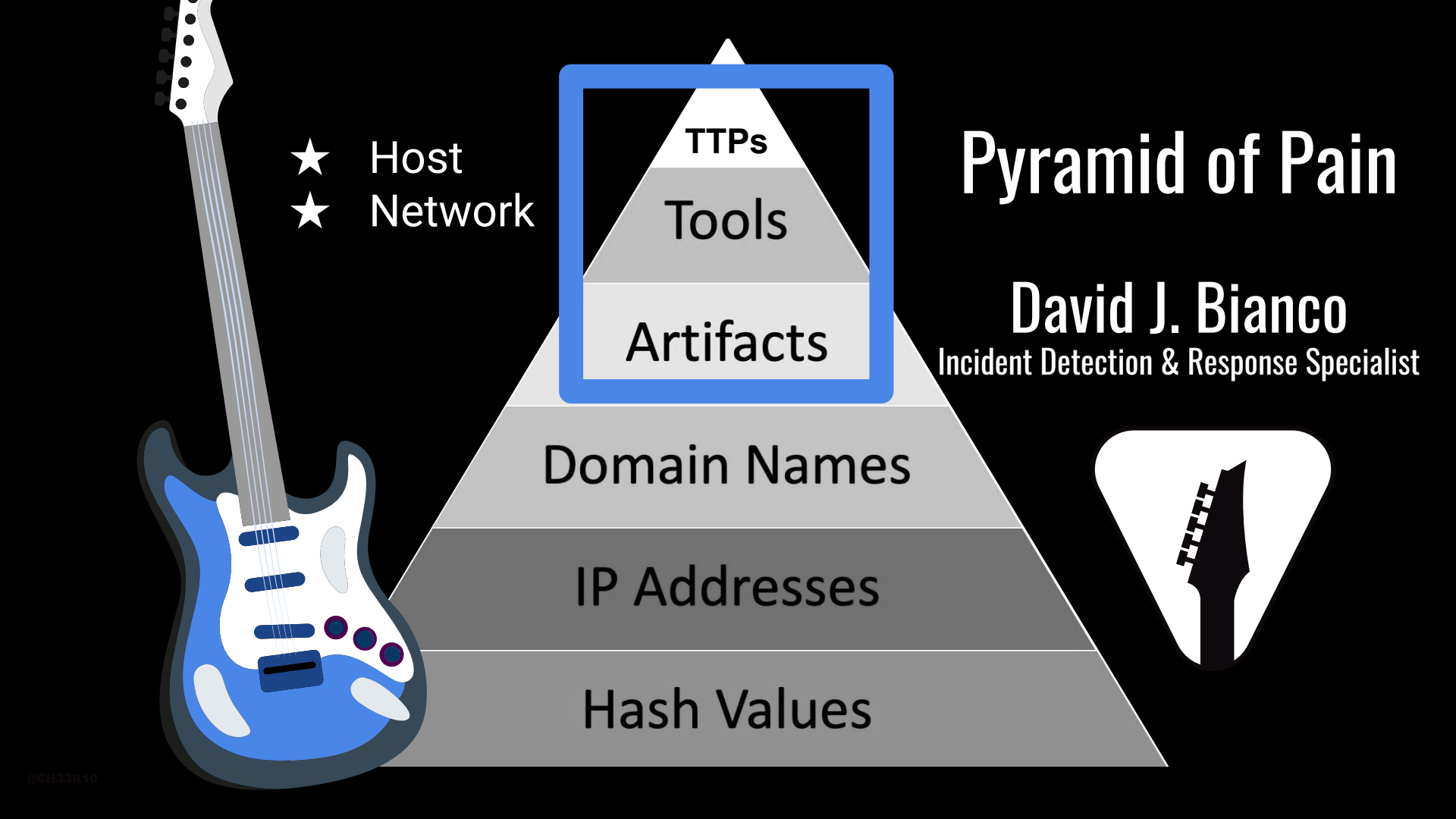
Findings, mitigations, documentation, lessons learned

ANALYSIS

Data > Collect, Create searches, run searches, & analyze results

FOCUS = RESEARCH
THREAT HUNTING CYCLE

- ★ Threat Hunt
  - Structured - Known TTPs, IOCs, artifacts
  - Unstructured - Unknown
- ★ INTERNAL vs. EXTERNAL Threat Hunting
  - Ex: Cobalt Strlke Beacon Hunting in Network vs. ITW


★ Host
★ Network
TTPs
Tools
Artifacts
Domain Names
IP Addresses
Hash Values
Pyramid of Pain
David J. Bianco
Incident Detection & Response Specialist
@CH33R10

LEVEL UP TRACKING

	WK 1	WK 2	WK 3
RESEARCH	1	2	2
PRACTICE	1	1	1
APPLY	4	3	5

TAKEAWAYS

01 RESEARCH

- ★ Know where to find stuff
- ★ Ask better questions

02 PRACTICE

- ★ Day Dream Hunt Hypotheses
- ★ Prepare!!!

03 APPLY

- ★ Practical
- ★ Consistent

THANK YOU!

ROCK ON!

Xena Olsen
@Ch33r10