Rapid Endpoint Investigations

[with Velociraptor and KAPE]

BLACK HILLS

Information Security

Agenda/Schedule

[Session Length: 1 hour]

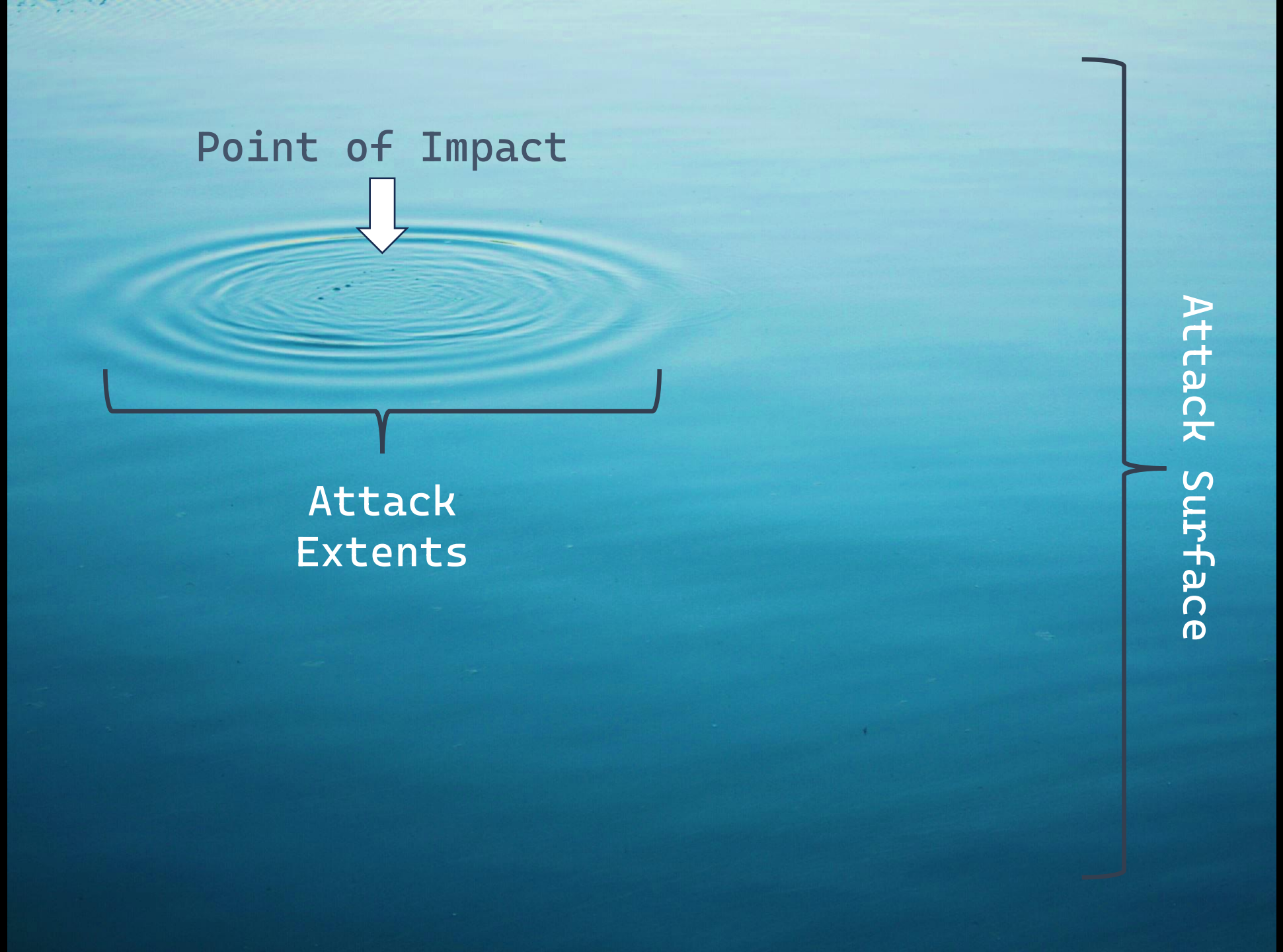
- Introduction
- Rapid Triage Workflow
- RTW with Velociraptor & KAPE
- References/Contact
- Q&A

“...since no amount of subsequent planning can solve a problem insufficiently understood, framing the problem is critical”

~USMC Planning Process for Battlefield Commanders

Patterson Cake

DFIR Consultant


Point of Impact
Attack
Extents
Attack Surface

Detection → Analysis → Containment → Eradication → Recovery

Attack Surface → Indicators → Capabilities

Point of Impact

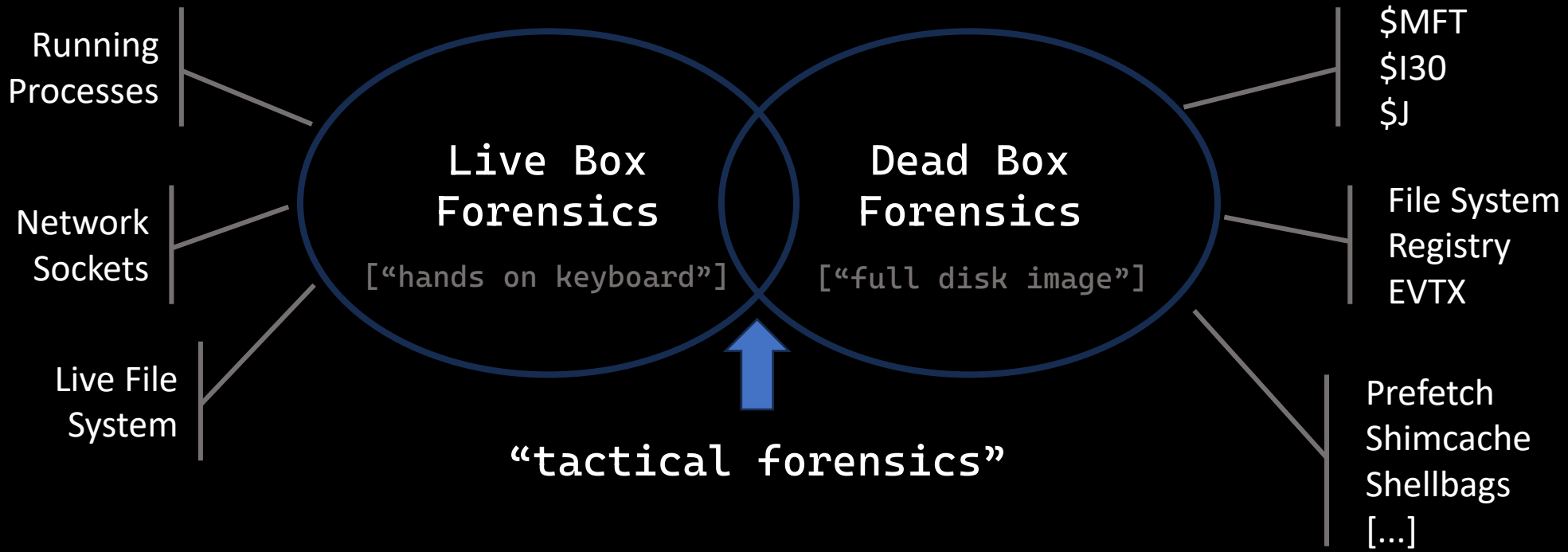
- [application]
- [identity]
- [endpoint]
- [network]
- [third party]
- [other]

- [memory]
- [identity]
- [network]
- [disk]

- [EDR]
- [Antivirus]
- [Proxy]
- [SIEM]
- [Firewalls]
- [Azure/M365]
- [OS Tools]
- [..]

Visibility & Containment

[frameworks: broadly-applicable guidelines upon which to build something useful]


Running Processes
Network Sockets
Live File System
Live Box Forensics
["hands on keyboard"]
Dead Box Forensics
["full disk image"]
$MFT
$I30
$J
File System
Registry
EVTX
Prefetch
Shimcache
Shellbags
[...]
"tactical forensics"

X-Ways Forensics*

Source	Event	IOC
File System	File Creation	401k_forms.doc.ps1
File System	Archive Creation	zip.zip
PSReadline	PoSh Rev Shell	54.227.12.227
Registry; System.evtx	Service Creation	ptjhkc
Web History	Browser Tab (Creation)	tinyurl.com/401KForms
Web History	Edge Proto_DB	http://54.227.12.227
Prefetch	NET.EXE	net.exe
Registry	Mapped Drive N:	\\sta2\share

Axiom Cyber*

Source	Event	IOC
File System	File Creation	401k_forms.doc.ps1
File System	Archive Creation	zip.zip
PSReadline	PoSh Rev Shell	54.227.12.227
Registry; System.evtx	Service	ptjhkc
Web History	Browser Tab (Creation)	tinyurl.com/401KForms
Web History	Edge Proto_DB	http://54.227.12.227
Prefetch	NET.EXE	net.exe
Registry	Mapped Drive N:	\\sta2\share

Autopsy*

Source	Event	IOC
Web History	File Creation	401k_forms.doc.ps1
File System	Archive Creation	zip.zip
PSReadline	PoSh Rev Shell	54.227.12.227
Registry	Service Existence	ptjhkc
Web History	Browser Tab (Creation)	tinyurl.com/401KForms
Registry	Mapped Drive N:	\\sta2\share

VR Offline & KAPE

Source	Event	IOC
Netstat Enriched	PoSh Rev shell	PowerShell to 54.227.12.227:88
Netstat Enriched	Network Socket	[socket] to 54.227.12.227:888
Edge\Sessions\Tabs	Browser Tab	tinyurl.com "tab"
PSReadLine	PoSh Rev shell	Rev Shell to 54.227.12.227
System.evtx	Service Creation	ptjhkc
Web History	Web Access	http://54.227.12.227
MFT	Archive Creation	zip.zip
LNK; Edge	File Access	401k_forms.doc LNK files

*Based on full forensic image analysis

Rapid Triage Workflow

- Acquire Artifacts {point of impact}
- Analyze Artifacts {start from event context}
- Identify IOCs {m...i...n...d}
- Expand Context {find attack extents}
- Contain {from attack extents}

“Relax. Look around. Make a call.” ~Willink

RTW: Collection

- Windows Artifacts
  - EVTX
  - MFT
  - Netstat w/PID-Path-Cmd-User
  - Running Processes w/Command Line
  - Autoruns
  - Artifacts of Execution
  - Web Actions/History

[tactical: “adroit in planning or maneuvering to accomplish a purpose”]

RTW: Collection

- Velociraptor Offline Collector
  - Artifacts
    - KAPE Triage
    - Netstat Enriched
    - Autoruns
    - PSList
  - Misc:
    - ZIP or upload to S3
    - Execute as Admin on Endpoint/s (GPO?!)
    - Pre-stage!

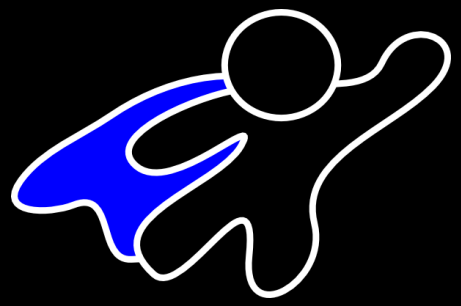
[tactical: “relating to the methods used to achieve a particular result”]

RTW: Collection – VR Offline

>velociraptor-v0.7.40-4-windows-amd64.exe gui:

- Server Artifacts\Build Offline Collector
  - Windows.KapeFiles.Targets (_KapeTriage)
  - Windows.Network.NetstatEnriched
  - Windows.System.Pslist
  - Windows.Sysinternals.Autoruns
- Configure Parameters
- Configure Collection
- Download/Rename
- Distribute, “run as” Admin!

RTW: Analysis



- KAPE & PowerShell
  - Modules
    - Hindsight
    - NirSoft BrowsingHistoryView
    - NirSoft WebBrowserDownloads
    - AppCompatCacheParser
    - PECmd
    - AmcacheParser
    - SBECmd
    - EVTXECmd
    - !EVTXECmd-Triage (Custom)
    - Hayabusa Offline Logon and EventLogs
    - MFTeCmd FileListing
  - Misc:
    - Expand-Archive
    - Invoke-KAPE (scalable!)
    - Export to Excel

RTW: Components

- AWS EC2: T2.Xlarge; W2K22; 150 GB OS; 2 TB Data
- Velociraptor (Velocidex GitHub)
- KAPE (Register and $$$ if you can!)
  - Hindsight (obsidianforensics GitHub)
  - BrowsingHistoryView (NirSoft
  - WebBrowserDownloads (NirSoft)
  - Hayabusa (Yamato-security GitHub)
- Invoke-Kape (swisscom/invoke-forensics GitHub)
- KAPE_Rapid_Triage_Excel.ps1 (secure-cake GitHub)
- expand-archive-triage-data.ps1 (secure-cake GitHub)
- Microsoft Excel
- PowerShell 7.x
- AWS S3 (optional)

[github.com/secure-cake/rapid-endpoint-investigations]

RTW: Collection – Stage Data

- OS Volume = Tools
  - C:\Tools\KAPE
    - ..\modules\bin\
- Data Volume = Case Files
  - D:\cases\2023-08-abc
    - ..\triage_data (zip files)
    - ..\kape_output (processed KAPE output files)

["expand-archive-triage-data.ps1"]

RTW: Event Context & IOCs

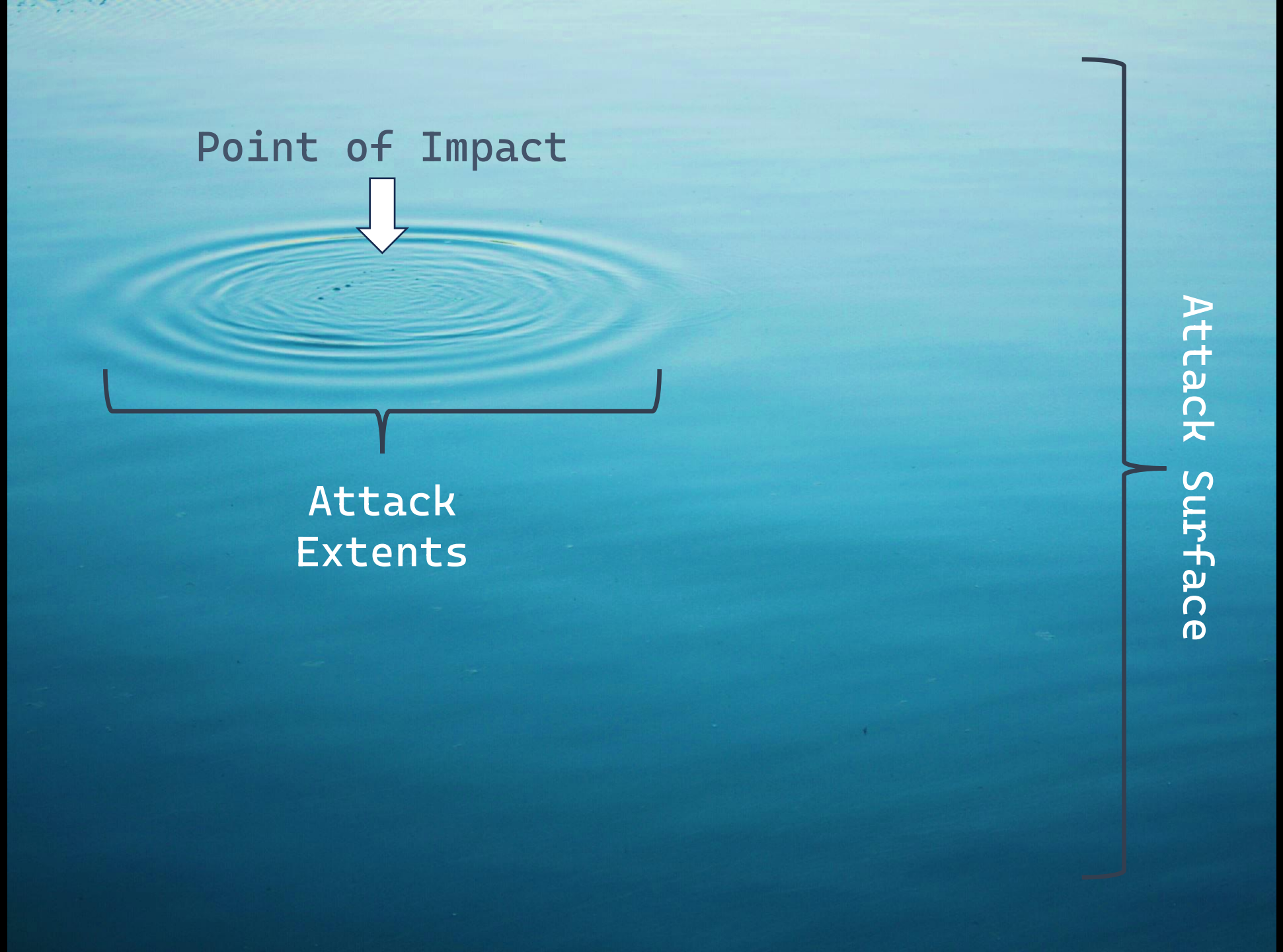
- Start from Event Context
- Filter out “Normal”
- Focus on Meaningful Impact (MIND)

[tactical: “adroit in planning or maneuvering to accomplish a purpose”]

RTW: Investigate!

- PSlist w/CMD*
- Netstat Enriched (Raddr.Port)
- MFT FL (exe & archive)
- EVTX, Web & Execution
  - Hayabusa (High & Critical)
  - EVTX (filtered)
  - BrowserDownloadsView
  - Timeline
  - SBE – UsrClass

NOTE: No PSList for STA1*


Point of Impact
Attack
Extents
Attack Surface

Q&A

Patterson Cake

@SecureCake

github.com/secure-cake

patterson@blackhillsinfosec.com

Thank you!