Enterprise DFIR Investigation Scenario

with Markus Schober

Blue Cape Security

Disclaimer!

- I do not assume and hereby disclaim any liability to any party for any errors, disruptions, damages, or other negative consequences resulting from applying the information that I share.

- No legal advice - Please consult with your own legal counsel regarding cyber security incident handling and specific legal questions you have.

💙

Why this presentation?

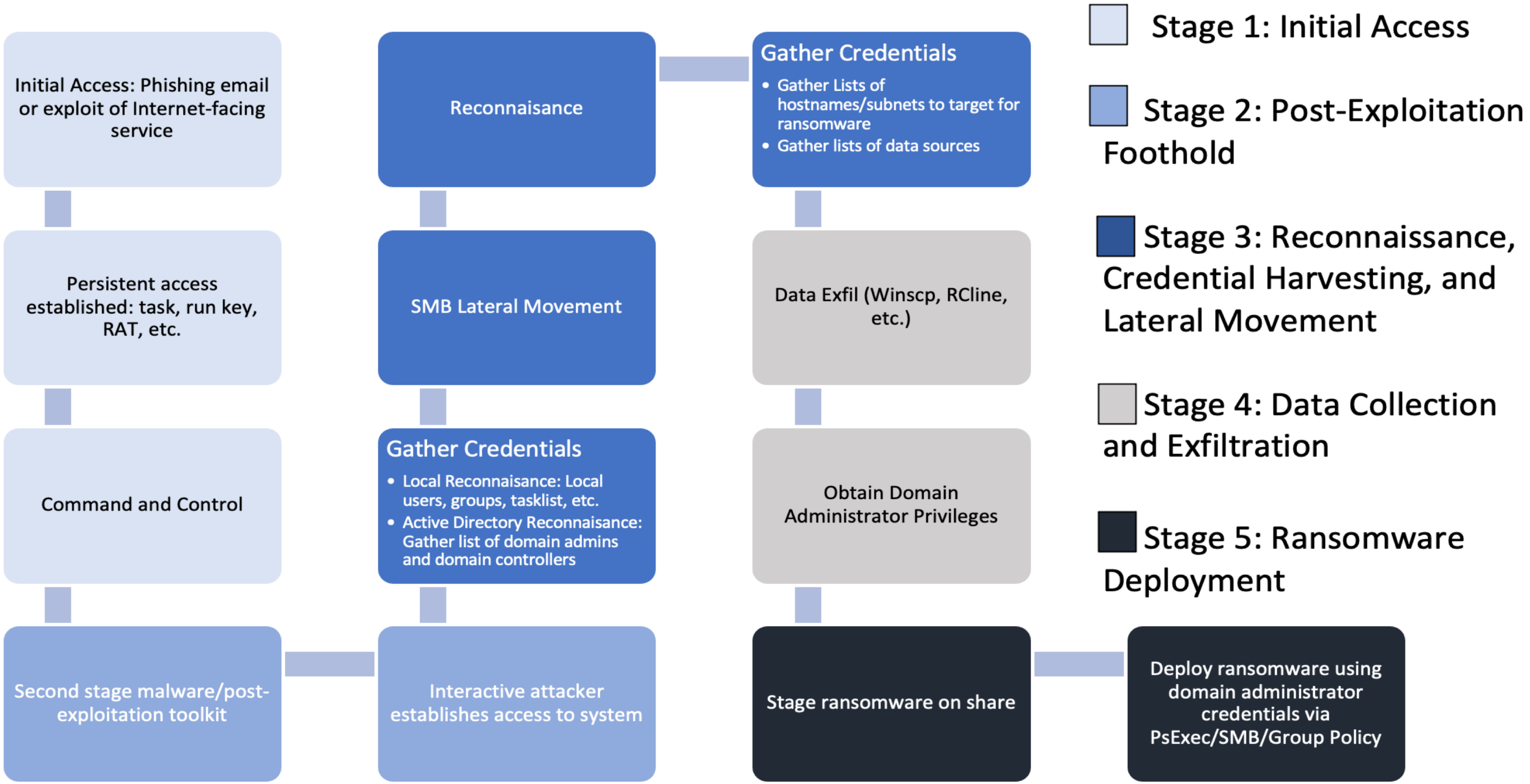
You've taken training, but are wondering how you apply your skills in a real world scenario?

You don't know what skills you need in a real world scenario?

Are you looking to improve your processes and procedures to prepare for real world scenarios?

You never had the chance to work on any exciting real world scenarios?

Ransomware Attack Lifecycle



Initial Access: Phishing email or exploit of Internet-facing service

Persistent access established: task, run key, RAT, etc.

Command and Control

Second stage malware/post-exploitation toolkit

Interactive attacker establishes access to system

Gather Credentials

- Local Reconnaisance: Local users, groups, tasklist, etc.
- Active Directory Reconnaisance: Gather list of domain admins and domain controllers

SMB Lateral Movement

Reconnaisance

Gather Credentials

- Gather Lists of hostnames/subnets to target for ransomware
- Gather lists of data sources

Data Exfil (Winscp, RCline, etc.)

Obtain Domain Administrator Privileges

Stage ransomware on share

Deploy ransomware using domain administrator credentials via PsExec/SMB/Group Policy

□ Stage 1: Initial Access

▨ Stage 2: Post-Exploitation Foothold

■ Stage 3: Reconnaissance, Credential Harvesting, and Lateral Movement

▩ Stage 4: Data Collection and Exfiltration

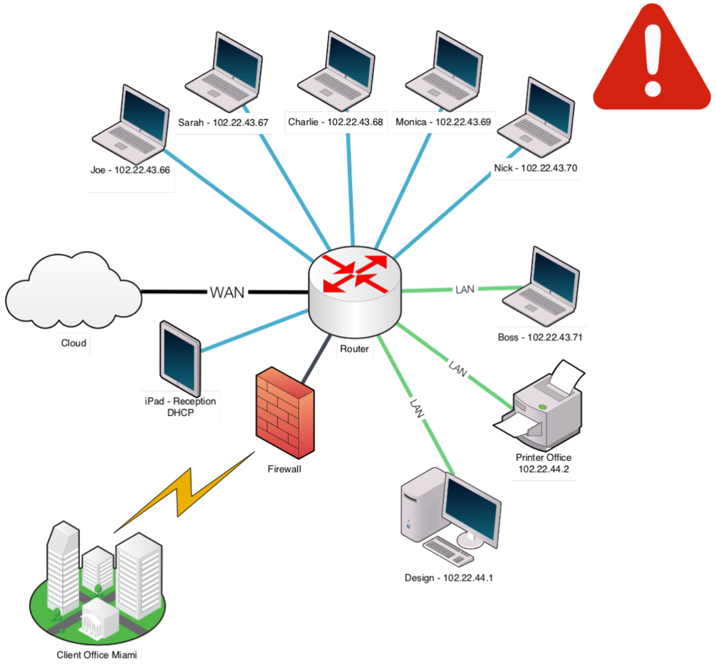
■ Stage 5: Ransomware Deployment

IBM Security: https://securityintelligence.com/posts/how-ransomware-attacks-happen/

Scenario: Compromised Employee Workstation

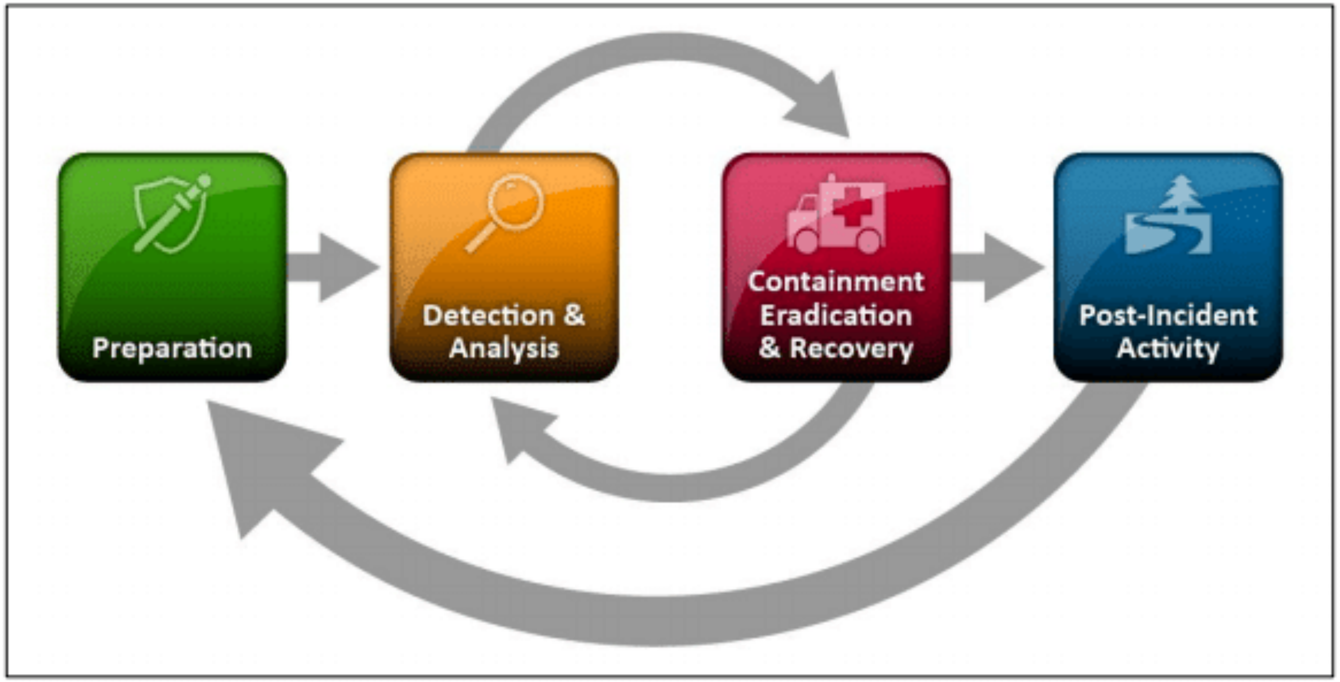
ALERT!

- Employee in HR
- Windows Workstation
- Stores sensitive information (PII data)
- EDR notification “Suspicious traffic to bupula[.]com”



Source: http://tentouchapps.com/grafio/solutions-area/network-diagram/

Have a Plan! The Incident Response Process

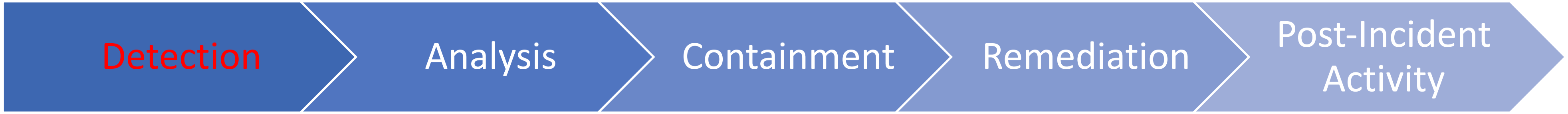


NIST SP800-61r2: Computer Security Incident Handling Guide

Tactical Response: Detection & Analysis

Detection

- Review the EDR notification
- Create ticket for response coordination
  - Document event information
- Document event timeline
- Curate a list of IOCs
  - Host-, network-, behavior based



Tactical Response: Detection & Analysis

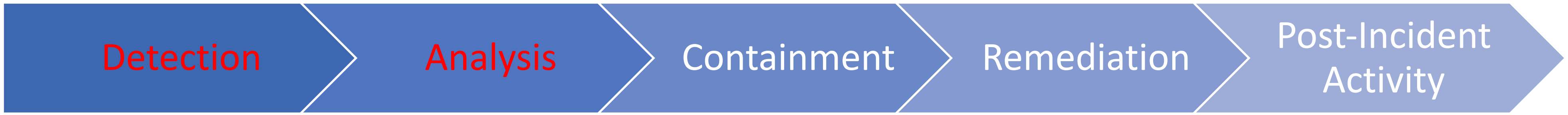
Detection

- Review the EDR notification
- Create ticket for response coordination
  - Document event information
- Document event timeline
- Curate a list of IOCs
  - Host-, network-, behavior based

Rapid Analysis / Triage

- Perform host analysis
  - Processes, network connections, files
  - Check for lateral movement
- Perform enterprise-wide searches
  - Search for IOCs across the EDR telemetry
- Classify the incident
  - False Positive?
  - Severity: critical / high / medium / low
  - Data privacy implications

Evidence preservation or further forensic analysis and incident response needed?



Detection

Analysis

Containment

Remediation

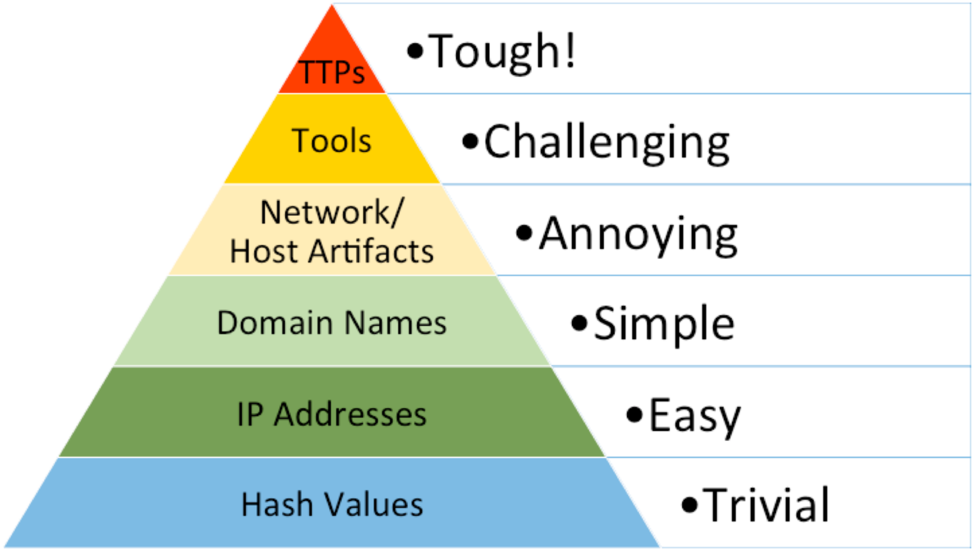
Post-Incident Activity

Tactical Response: Containment

Containment

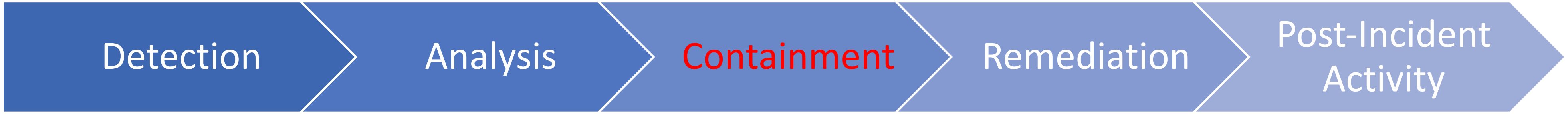
- Isolate the workstation(s)
- Deactivate affected user accounts
- Respond to IOCs

Pyramid of Pain: IOCs to respond to attacks



TTPs	•Tough!
Tools	•Challenging
Network/ Host Artifacts	•Annoying
Domain Names	•Simple
IP Addresses	•Easy
Hash Values	•Trivial

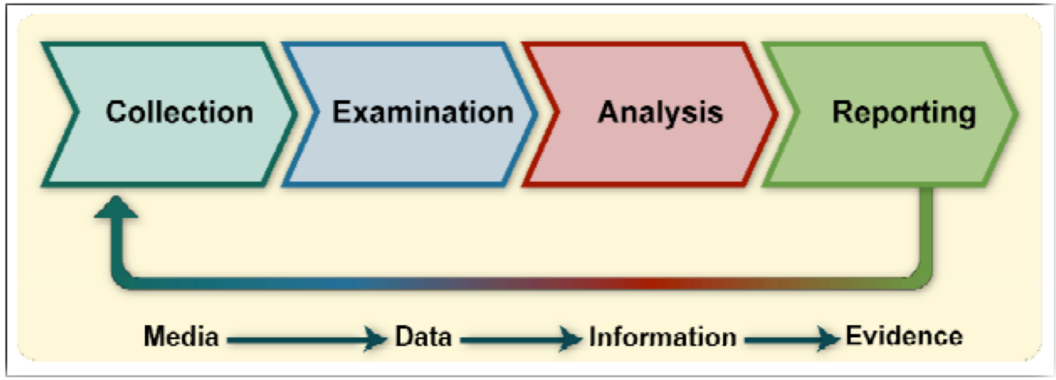
The Pyramid of Pain, originally developed by David Bianco:
http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html



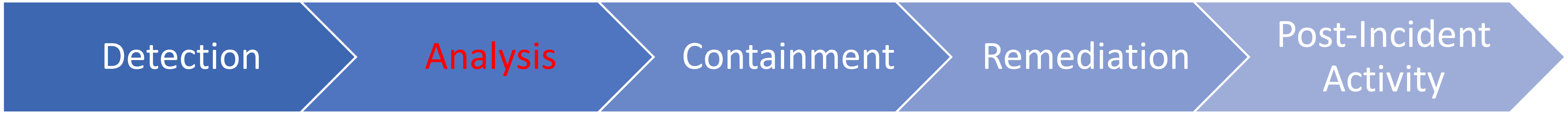
Detection → Analysis → Containment → Remediation → Post-Incident Activity

Tactical Response: Forensic Analysis

Forensic Analysis Process

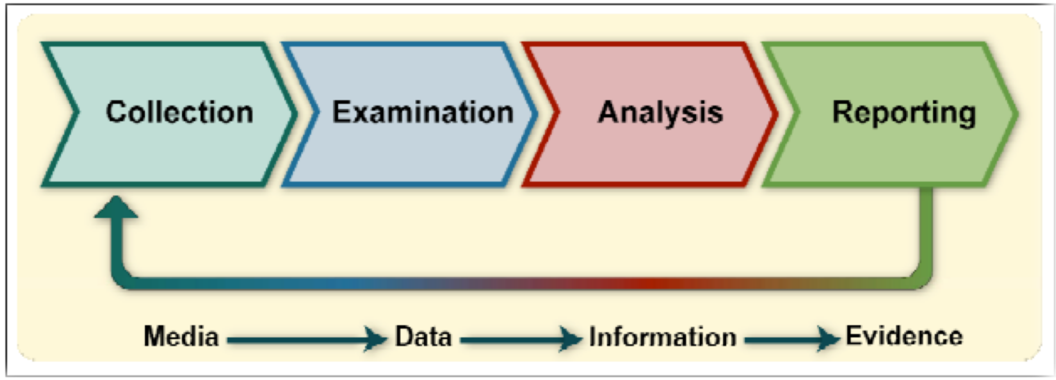


NIST SP800-86: Forensic Process



Tactical Response: Forensic Analysis

Forensic Analysis Process



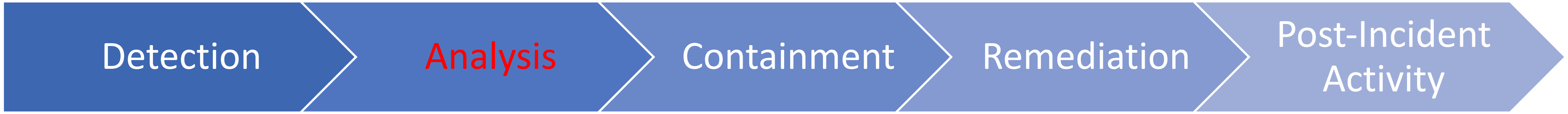
NIST SP800-86: Forensic Process

Collection

- Follow order of volatility
- Maintain chain of custody
- Verify integrity – create hash values

Important Considerations!

- Timeliness
- Physical vs. virtual host?
- Type of information:
  - Live response collection
  - Full disk and memory images



Detection

Analysis

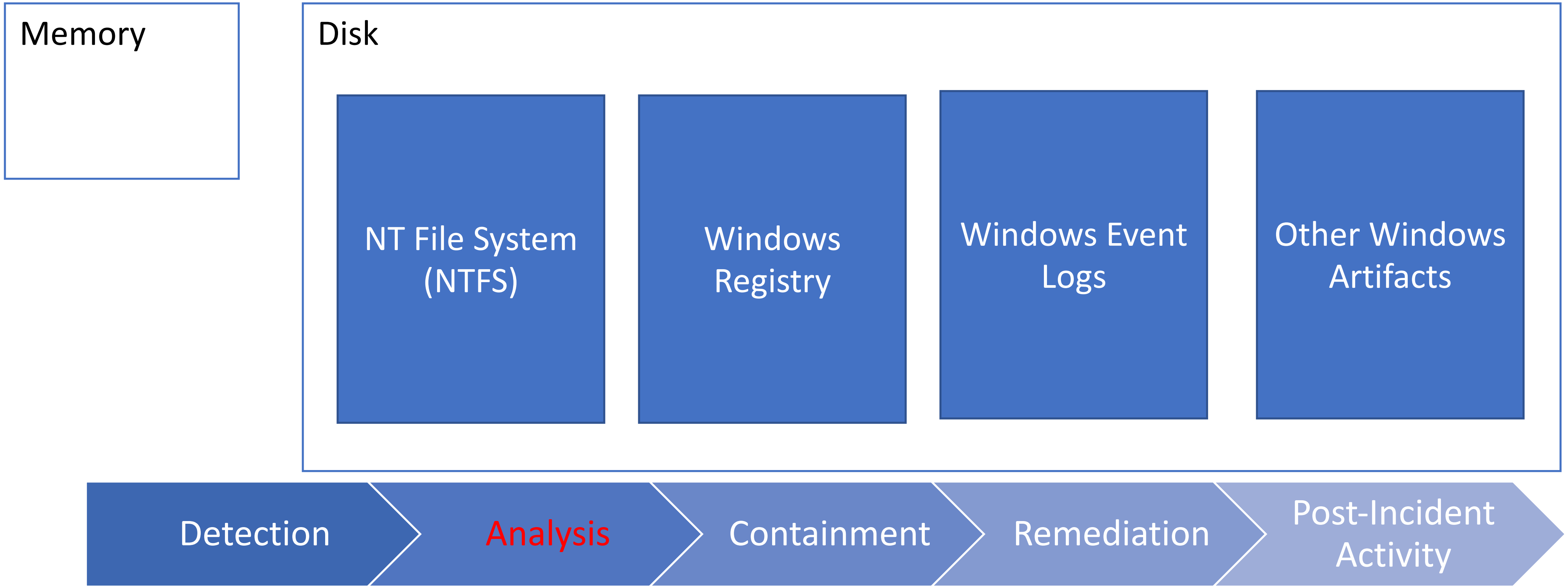
Containment

Remediation

Post-Incident Activity

Tactical Response: Forensic Analysis

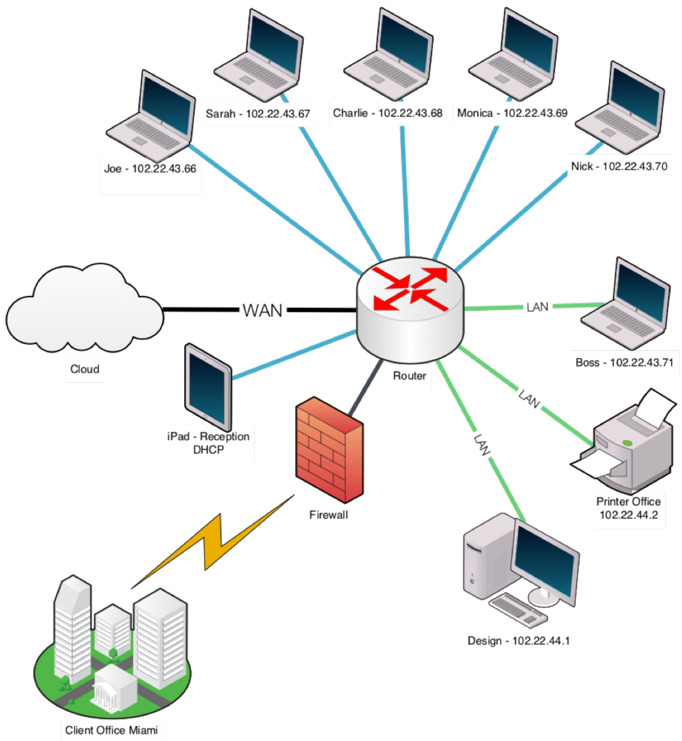
Fundamental sources of forensic evidence on Windows systems

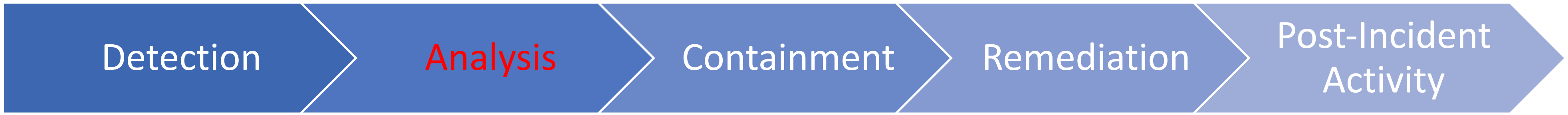


Data Collection Options: Live Response

Deploy collection tools. Acquire and upload important forensic artifacts from the live systems.

- KAPE (Kroll Artifact Parser & Extractor)
- MagnetResponse
- Velociraptor

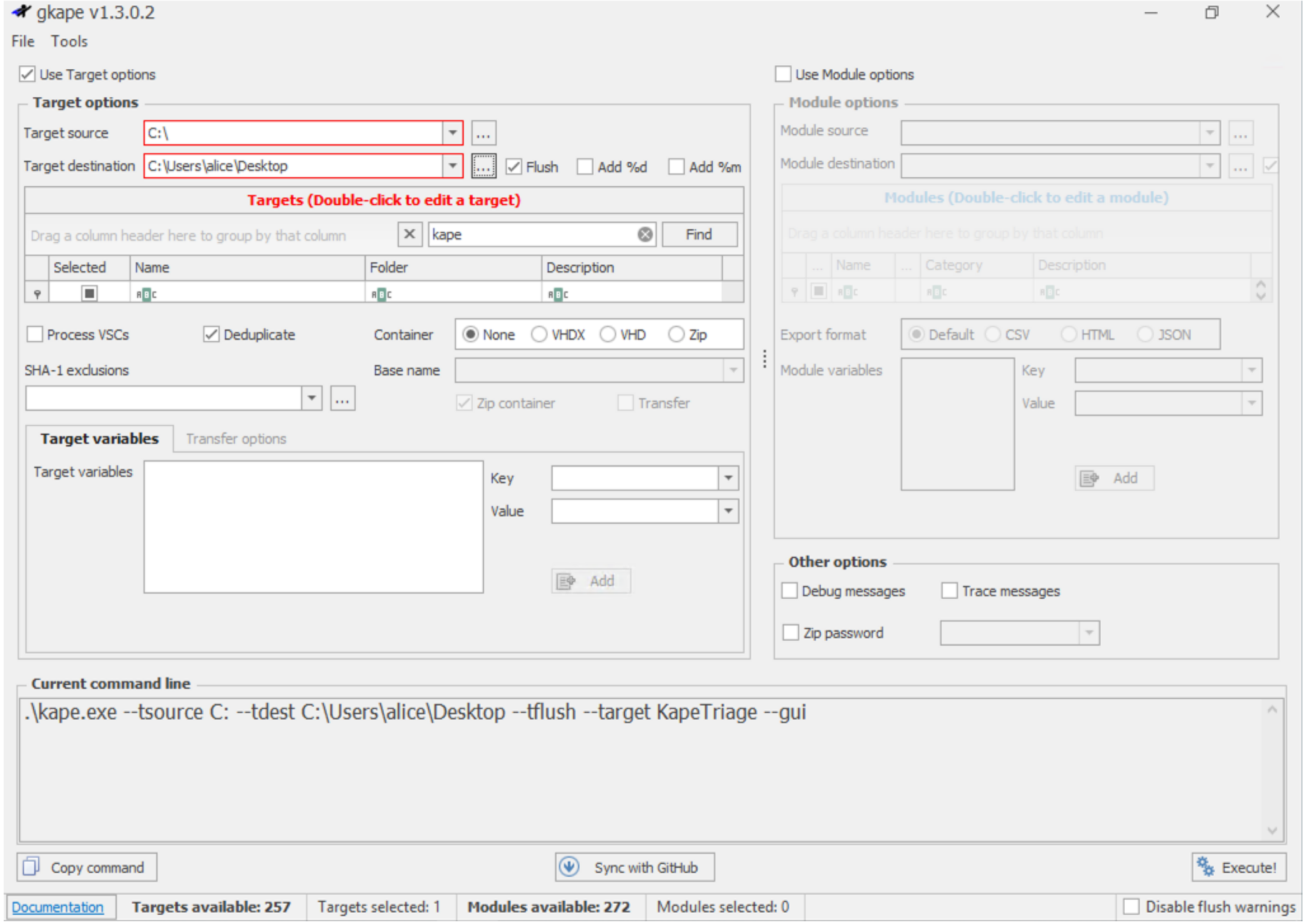




KAPE - Triage Collection

One of the quickest way to collect triage data for forensic analysis is using the Kroll Artifact Parser Extractor (KAPE).

You can select to collect individual or compound artifacts at once. There’s also options to apply modules and parse the artifacts in one go.



gkape v1.3.0.2

☑ Use Target options

Target options

Target source: C:\

Target destination: C:\Users\alice\Desktop

☑ Flush ☐ Add %d ☐ Add %m

Targets (Double-click to edit a target)

Search: kape

Selected	Name	Folder	Description

☐ Process VSCs ☑ Deduplicate

Container: ● None ○ VHDX ○ VHD ○ Zip

☐ Use Module options

Other options

☐ Debug messages ☐ Trace messages

☐ Zip password

Current command line

```
.\kape.exe --tsource C: --tdest C:\Users\alice\Desktop --tflush --target KapeTriage --gui
```

Targets available: 257 | Targets selected: 1 | Modules available: 272 | Modules selected: 0

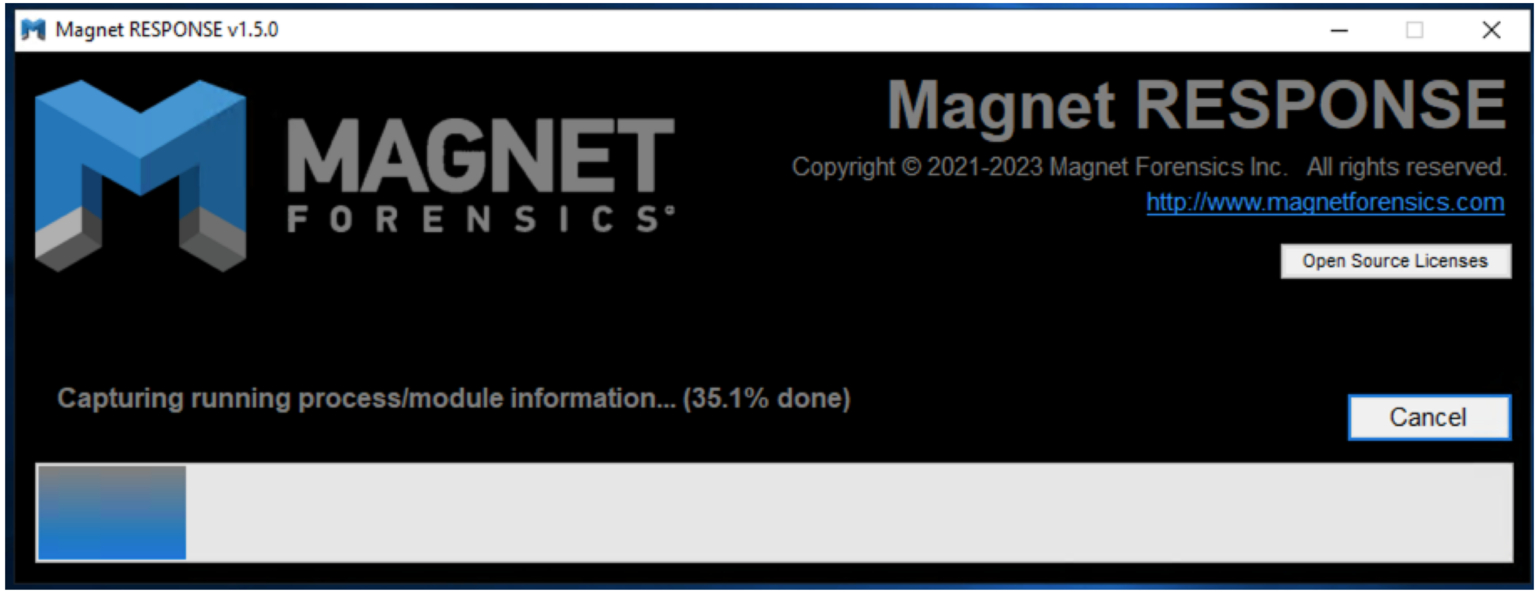
☐ Disable flush warnings

MagnetRESPONSE – Volatile Data Collection

RESPONSE is an evidence collection and preservation tool.

Collects:

- RAM
- Volatile data information
- System Files



Magnet RESPONSE v1.5.0

Magnet RESPONSE

Copyright © 2021-2023 Magnet Forensics Inc. All rights reserved.

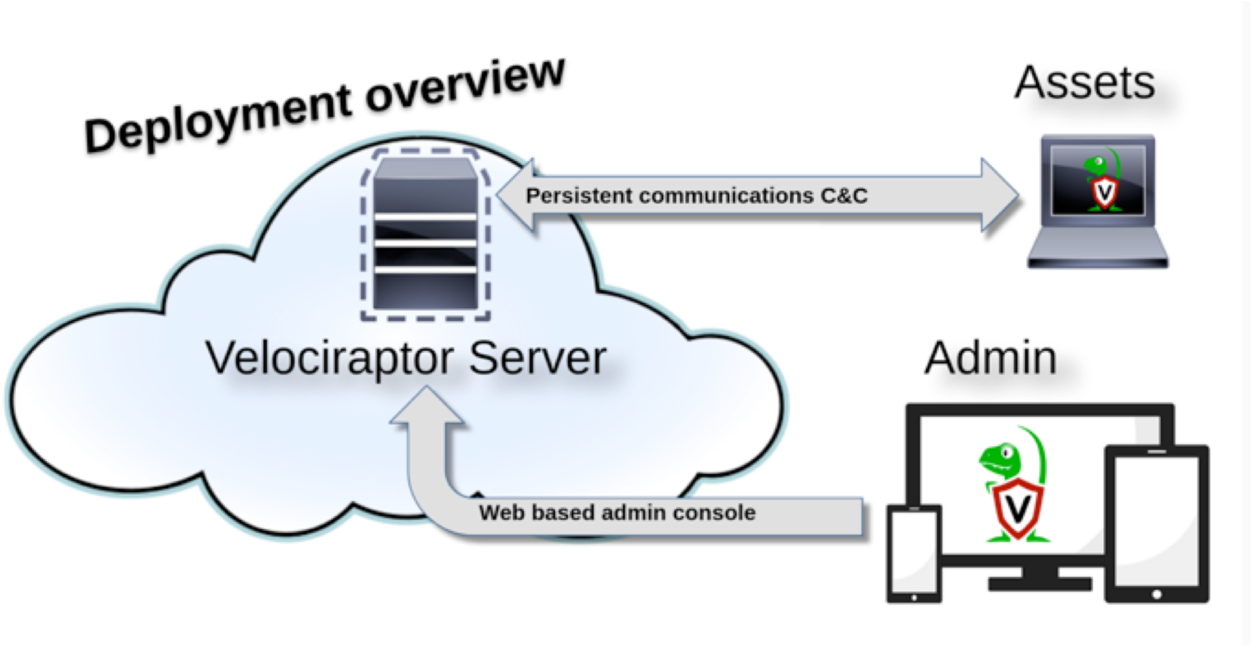
http://www.magnetforensics.com

Capturing running process/module information... (35.1% done)

Velociraptor Overview

- Velociraptor is a unique Free and Open Source DFIR tool
- Hunt for artifacts at scale over thousands of end points within minutes!

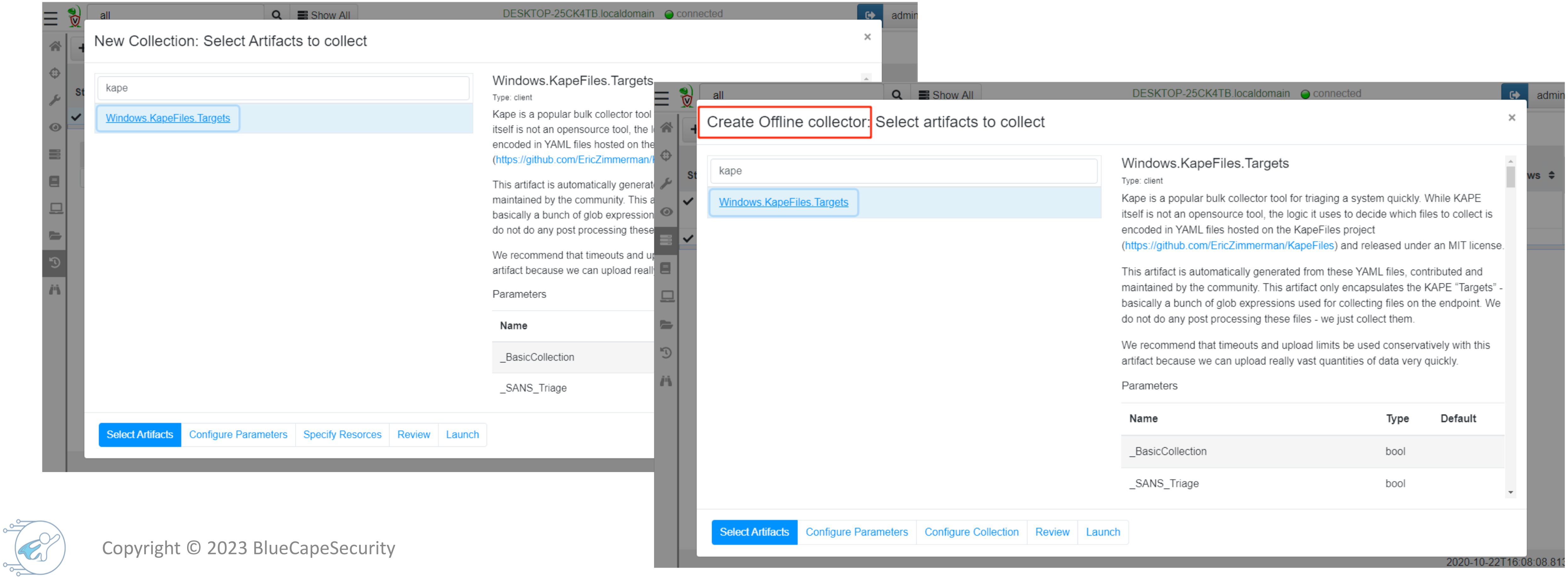
➢ Collect
➢ Monitor
➢ Hunt



Velociraptor – Live Response Data Collection

a) Collect data at scale via hunts leveraging KAPE artifacts

b) Create a custom offline collector



New Collection: Select Artifacts to collect

kape

Windows.KapeFiles.Targets

Windows.KapeFiles.Targets

Type: client

Kape is a popular bulk collector tool itself is not an opensource tool, the l encoded in YAML files hosted on the (https://github.com/EricZimmerman/

This artifact is automatically generat maintained by the community. This a basically a bunch of glob expression do not do any post processing these

We recommend that timeouts and u artifact because we can upload reall

Parameters

Name
_BasicCollection
_SANS_Triage

Create Offline collector: Select artifacts to collect

kape

Windows.KapeFiles.Targets

Windows.KapeFiles.Targets

Type: client

Kape is a popular bulk collector tool for triaging a system quickly. While KAPE itself is not an opensource tool, the logic it uses to decide which files to collect is encoded in YAML files hosted on the KapeFiles project (https://github.com/EricZimmerman/KapeFiles) and released under an MIT license.

This artifact is automatically generated from these YAML files, contributed and maintained by the community. This artifact only encapsulates the KAPE "Targets" - basically a bunch of glob expressions used for collecting files on the endpoint. We do not do any post processing these files - we just collect them.

We recommend that timeouts and upload limits be used conservatively with this artifact because we can upload really vast quantities of data very quickly.

Parameters

Name	Type	Default
_BasicCollection	bool	
_SANS_Triage	bool	

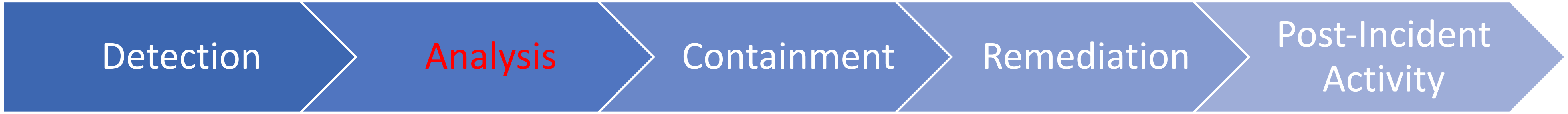
Data Collection Options:
Full Disk and Memory Images

a) Virtual Machines

- Cloud:
  1. Run memory acquisition tool
  2. Take snapshot and create disk image

- Hypervisor-level access:
  1. Take snapshot
  2. Acquire memory and disk related VM files

b) Physical Systems



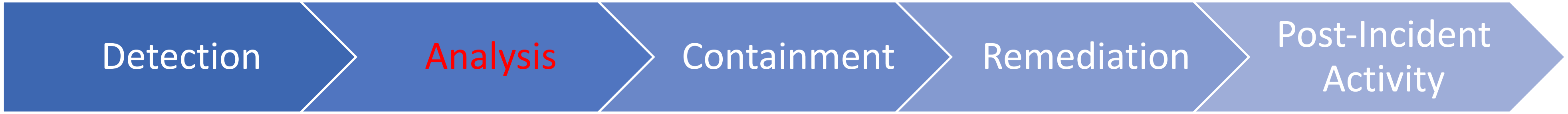
Data Collection Options:
Full Disk and Memory Images

a) Virtual Machines

- Cloud:
  1. Run memory acquisition tool
  2. Take snapshot and create disk image
- Hypervisor-level access:
  1. Take snapshot
  2. Acquire memory and disk related VM files

b) Physical Systems

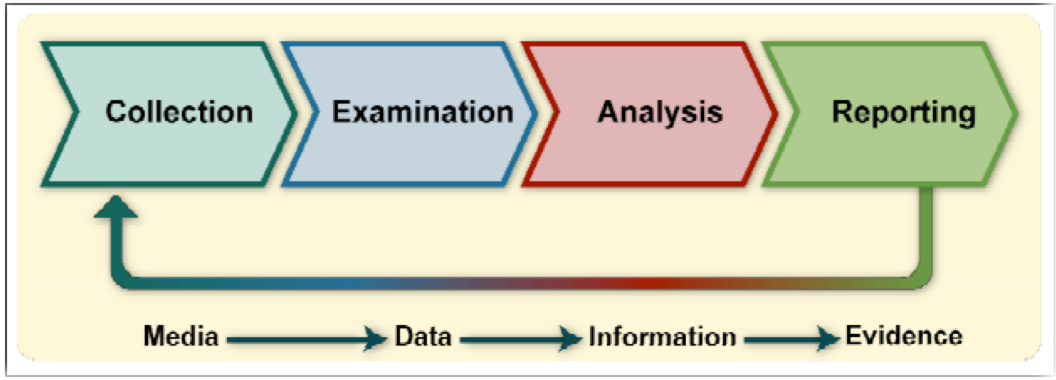
1. Run memory acquisition tool
2. Create disk image
   a) Online: Using tools such as FTK Imager
   b) Offline: Extract and copy physical disk via write-blocker



Detection → Analysis → Containment → Remediation → Post-Incident Activity

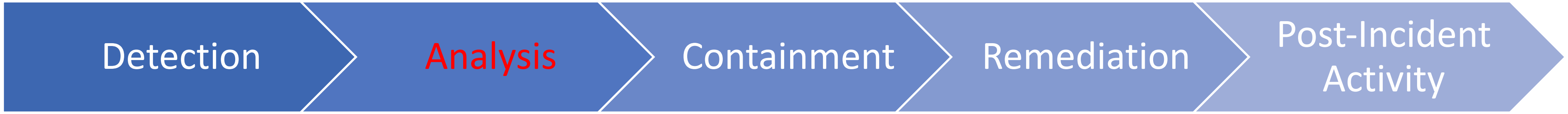
Tactical Response: Forensic Analysis

Forensic Analysis Process



NIST SP800-86: Forensic Process

- **Collection**
  - Follow order of volatility
  - Maintain chain of custody
- **Examination**
  - Process and assess collected data
- **Analysis**
  - Windows memory and disk artifacts
- **Reporting**
  - Document findings and recommendations



Detection

Analysis

Containment

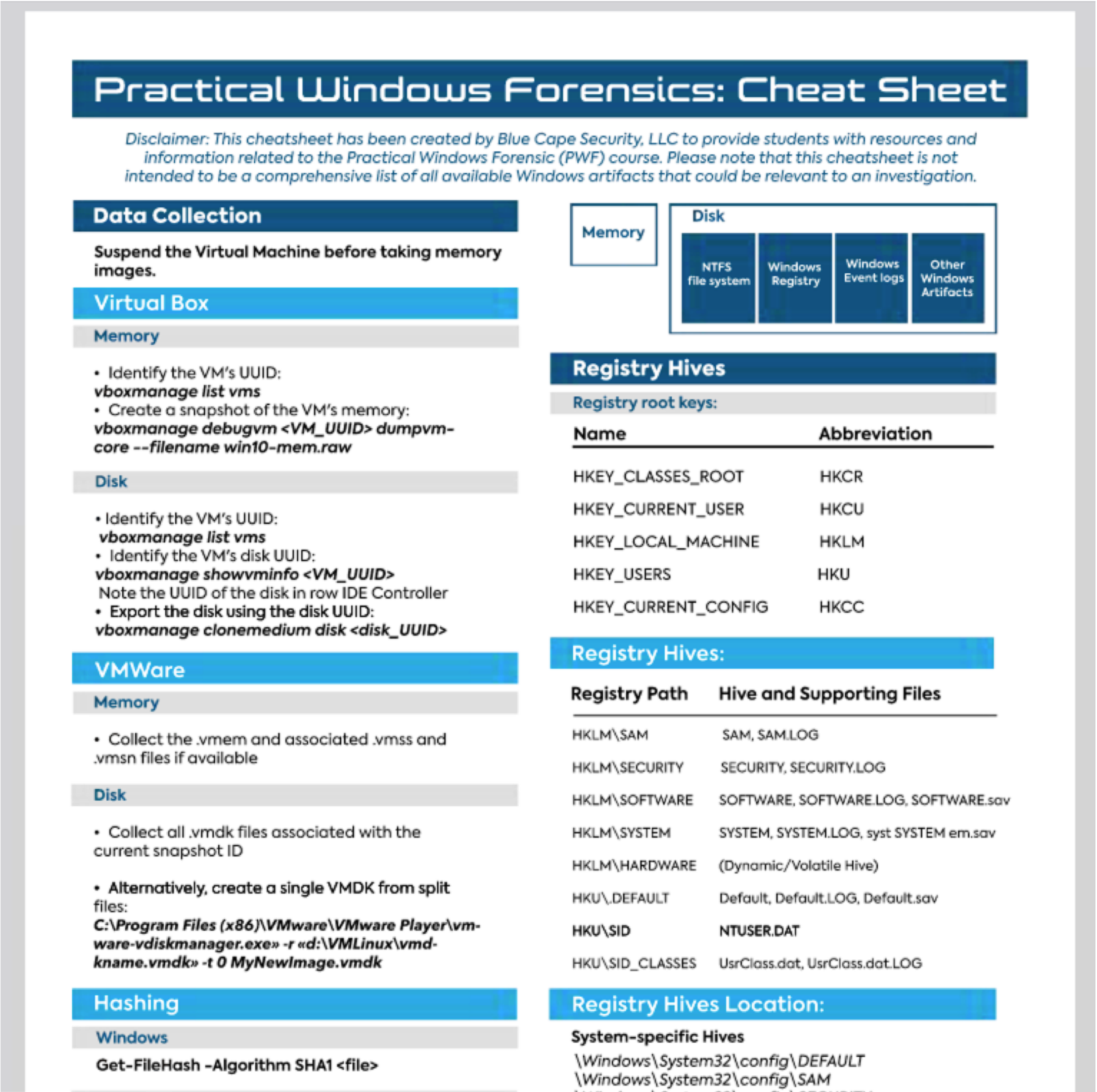
Remediation

Post-Incident Activity

Forensic Analysis

Practical Windows Forensics Cheat Sheet:

https://github.com/bluecapesecurity/PWF



Practical Windows Forensics: Cheat Sheet

Disclaimer: This cheatsheet has been created by Blue Cape Security, LLC to provide students with resources and information related to the Practical Windows Forensic (PWF) course. Please note that this cheatsheet is not intended to be a comprehensive list of all available Windows artifacts that could be relevant to an investigation.

Data Collection

Suspend the Virtual Machine before taking memory images.

Virtual Box

Memory

- Identify the VM's UUID:

vboxmanage list vms

- Create a snapshot of the VM's memory:

vboxmanage debugvm <VM_UUID> dumpvm-core --filename win10-mem.raw

Disk

- Identify the VM's UUID:

vboxmanage list vms

- Identify the VM's disk UUID:

vboxmanage showvminfo <VM_UUID>

Note the UUID of the disk in row IDE Controller

- **Export the disk using the disk UUID:**

vboxmanage clonemedium disk <disk_UUID>

VMWare

Memory

- Collect the .vmem and associated .vmss and .vmsn files if available

Disk

- Collect all .vmdk files associated with the current snapshot ID

- **Alternatively, create a single VMDK from split** files:

C:\Program Files (x86)\VMware\VMware Player\vm-ware-vdiskmanager.exe» -r «d:\VMLinux\vmd-kname.vmdk» -t 0 MyNewImage.vmdk

Hashing

Windows

Get-FileHash –Algorithm SHA1 <file>

Memory

Disk

NTFS file system

Windows Registry

Windows Event logs

Other Windows Artifacts

Registry Hives

Registry root keys:

Name	Abbreviation
HKEY_CLASSES_ROOT	HKCR
HKEY_CURRENT_USER	HKCU
HKEY_LOCAL_MACHINE	HKLM
HKEY_USERS	HKU
HKEY_CURRENT_CONFIG	HKCC

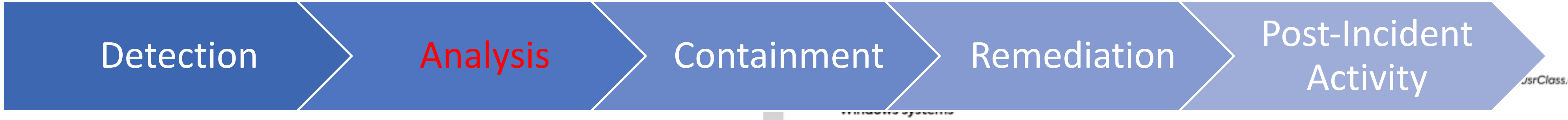
Registry Hives:

Registry Path	Hive and Supporting Files
HKLM\SAM	SAM, SAM.LOG
HKLM\SECURITY	SECURITY, SECURITY.LOG
HKLM\SOFTWARE	SOFTWARE, SOFTWARE.LOG, SOFTWARE.sav
HKLM\SYSTEM	SYSTEM, SYSTEM.LOG, syst SYSTEM em.sav
HKLM\HARDWARE	(Dynamic/Volatile Hive)
HKU\.DEFAULT	Default, Default.LOG, Default.sav
HKU\SID	**NTUSER.DAT**
HKU\SID_CLASSES	UsrClass.dat, UsrClass.dat.LOG

Registry Hives Location:

System-specific Hives

\Windows\System32\config\DEFAULT
\Windows\System32\config\SAM



Detection

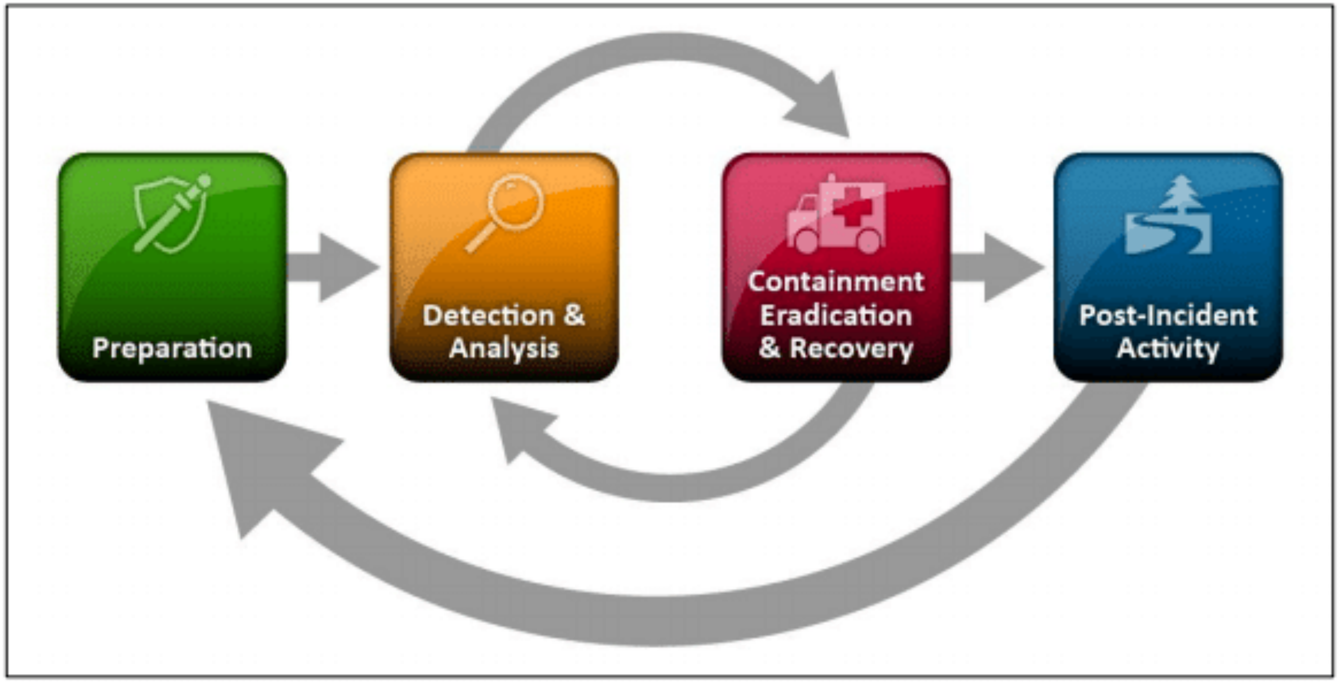
Analysis

Containment

Remediation

Post-Incident Activity

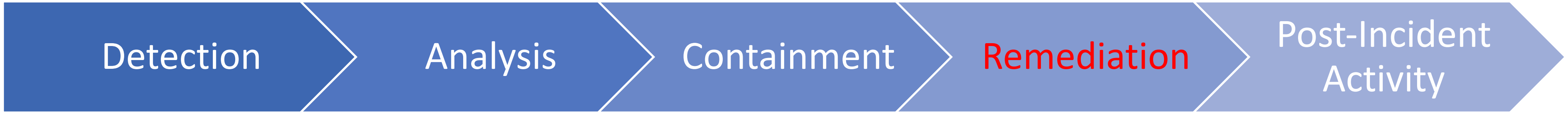
Have a Plan! The Incident Response Process



NIST SP800-61r2: Computer Security Incident Handling Guide

Tactical Response: Remediation

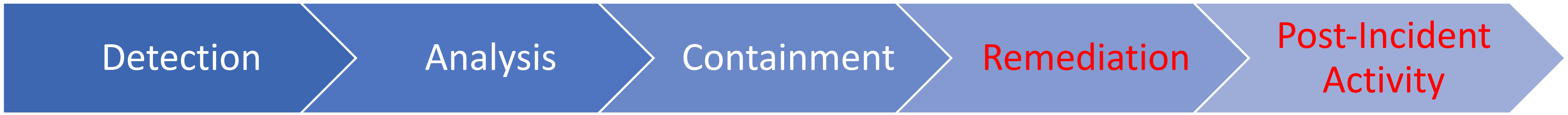
- Reimage or issue new systems
- Reset all affected user accounts
  - Ensure MFA is activated
- Block IOCs as needed
- Update rules for monitoring
  - TTPs based on threat intelligence
- Patch potential vulnerabilities
- Increased monitoring on affected accounts



Tactical Response: Post-Incident Activity

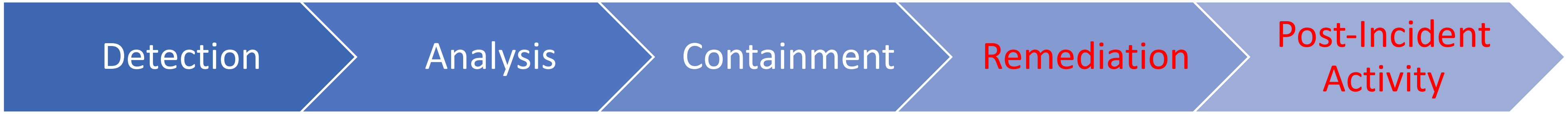
Types of Reporting

Forensic Report	• Legal cases, Expert witness testimony • Consultant engagements
High-Level Presentation	• Executive debriefs • Q&A documents
System Timeline	• Events listed in temporal order
etc.	• Resolving tickets



Tactical Response: Post-Incident Activity

- Lessons learned
- Gap analysis
- Risk assessment
- Evidence Retention
  - Prosecution – legal actions
  - Regulatory requirements



Detection

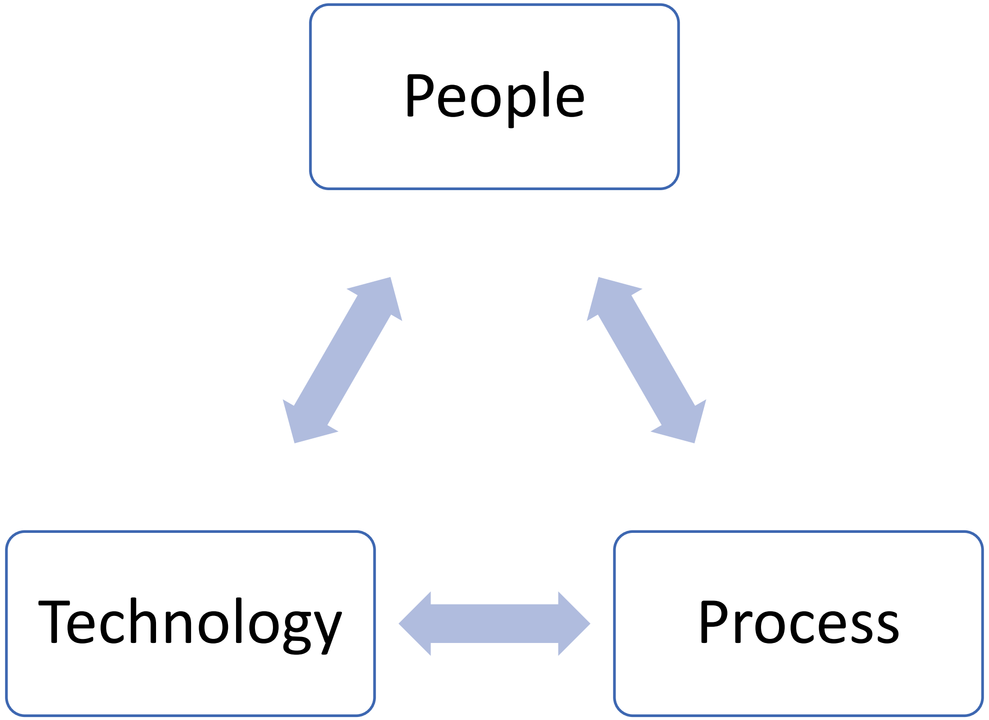
Analysis

Containment

Remediation

Post-Incident Activity

DFIR Recommendations



DFIR Recommendations

-> People

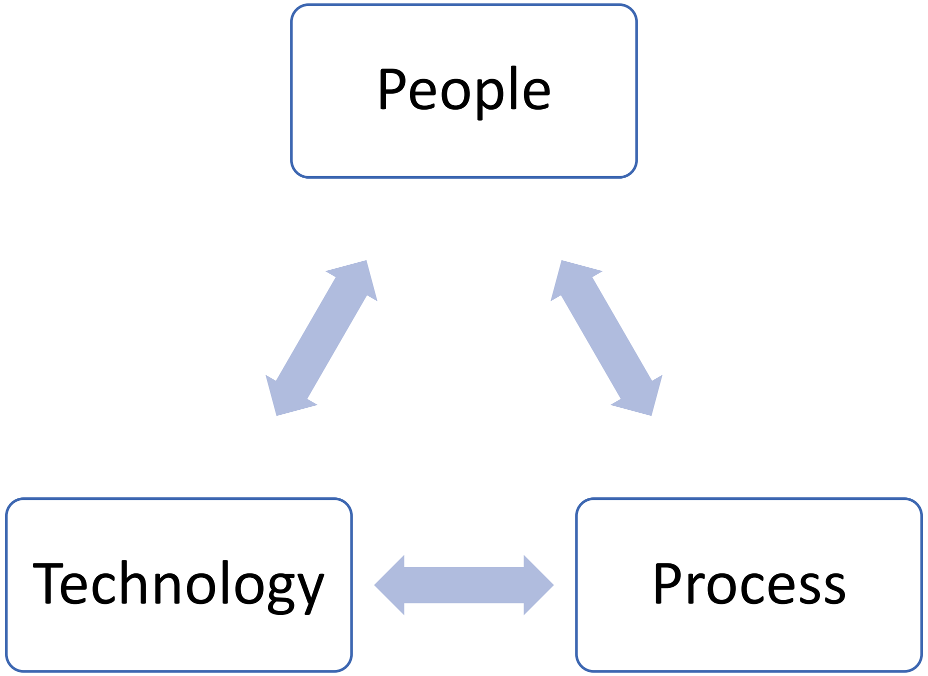
- Invest in people / in your skills!
  Everything starts with people!
  - Hands-on training
  - Discussion based scenarios (TTX)

-> Process

- Who does what, when, where, how?
  - Expectations, SLAs, Responsibilities, Liability
  - Processes and Procedures (Playbooks)

-> Technology

- Monitoring, Visibility, Controls, Detection and Response



Q & A

THANKS!

Markus Schober

Blue Cape Security