Effective DFIR Investigation With Limited Resources For IT/OT

Ahmad Zaidi & Salman Shaikh

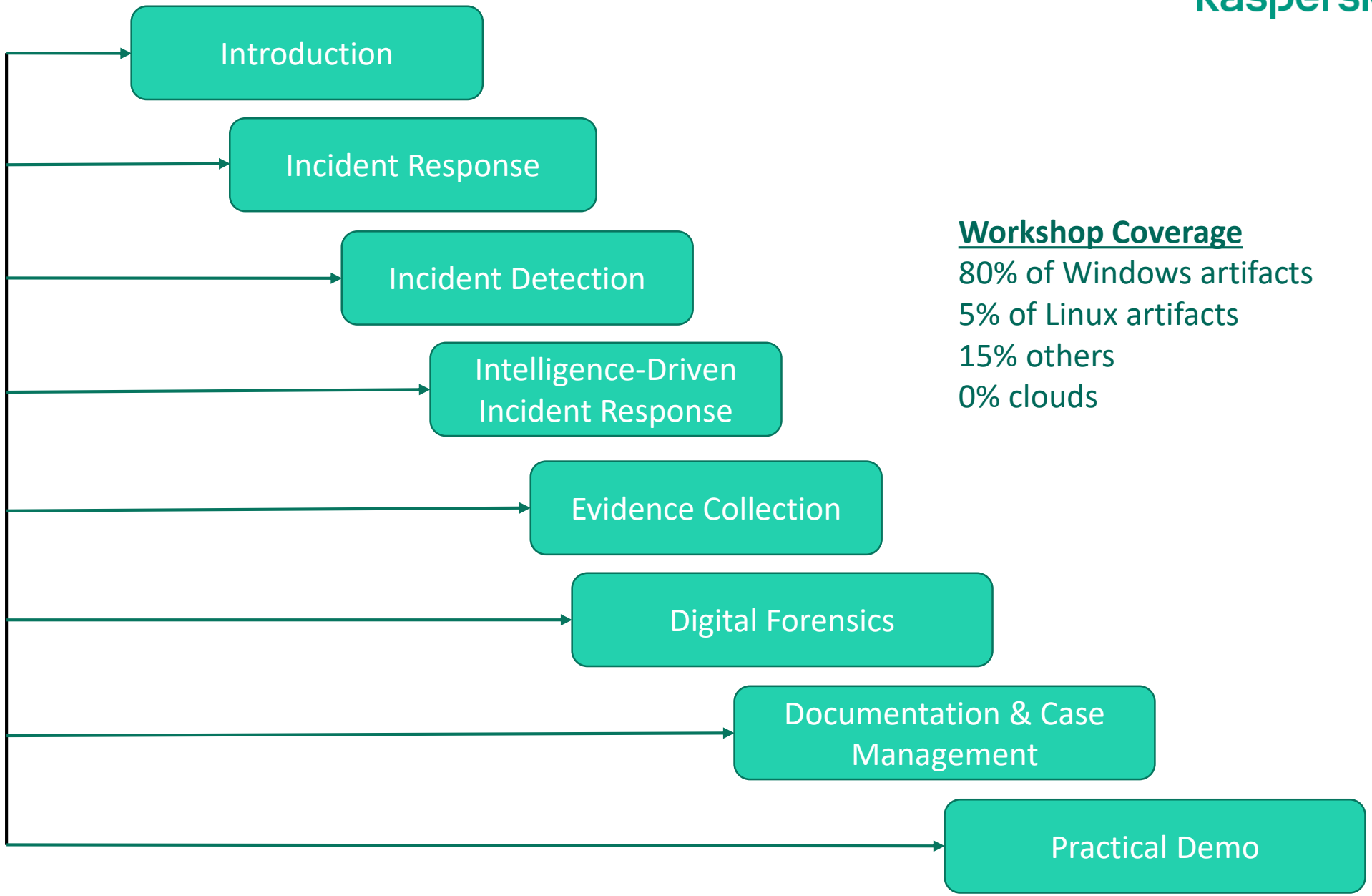
21/09/2023

Port Vila, Vanuatu

AGENDA

kaspersky

EFFECTIVE DFIR INVESTIVAGATION



Workshop Coverage

80% of Windows artifacts
5% of Linux artifacts
15% others
0% clouds

Introduction

Background – Ahmad **Zaidi** Said

- Work as Digital Forensics and Incident Response Specialist at Kaspersky Global Emergency Response Team (GERT)
- 12+ years of experience in Digital Forensics & Incident Response (DFIR) , Malware Analysis & Reverse Engineering, Threat Intelligence, Threat Hunting.

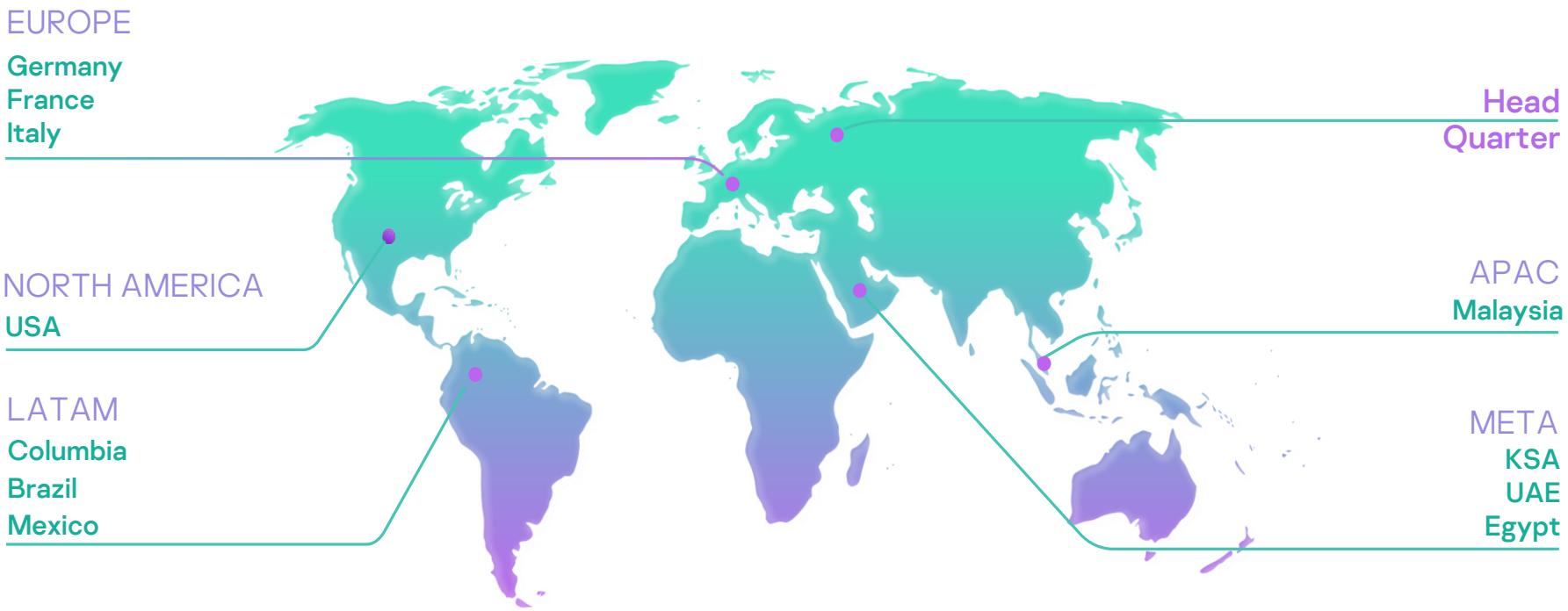
- Certification:
  - GIAC Reverse Engineering Malware (GREM)
  - GIAC Cloud Forensics Responder (GCFR)
  - Foundation - IT Service Management (ITILv3)

- Past Working Experience: Malaysia CERT (MyCERT), MNCs, Financial Institution
- Active Member of High Technology Crime Investigation Association (HTCIA)
- Active Member of Malaysia CyberSecurity Community (rawSEC)
- Speaker for international & local event
- https://www.linkedin.com/in/ahmadzaidi/

Global Emergency Response Team (GERT)

kaspersky

Kaspersky Incident Response



We speak English, Arabic, German, Italian, Russian, Spanish, French, Bahasa

Reactive

- Incident Response
- Digital Forensics
- Malware Analysis

GERT | Global Emergency Response Team

We provide DFIR services:

- **Retainer and Emergency**
- **Remote and onsite**

Proactive

- Trainings and workshops
- Tabletop Exercise (TTX)

Just a view of them

kaspersky

Background – **Salman** Shaikh

- Work as Senior Security Researcher at Kaspersky Industrial Control System (CERT)
- 8+ years of experience in Digital Forensics & Incident Response (DFIR) , Malware Analysis & Reverse Engineering, Threat Intelligence, Threat Hunting, Detection Engineer.
- Hunt for adversary infrastructure. https://twitter.com/salmanvsf
- Certification:
  - GIAC Reverse Engineering Malware (GREM)
  - Certified Red Team Professional (CRTP)
  - Hunt APTs with Yara like a GReAT ninja (Kaspersky)

- Past Working Experience: Notable Security Vendors, IT & OT sectors, Manufacturing, Banking, Energy, Oil & Gas industry.
- Speaker for international & local event. OT-ISAC, CyberPeace Summit, ICS-OT Scada Professionals etc

Kaspersky ICS CERT: key facts

kaspersky

Established
in 2016

The first ICS CERT created by
a commercial organization

CVE Numbering
Authority (CNA)

Who we are

A global project by Kaspersky to coordinate the efforts of industrial automation system vendors and industrial facility owners and operators.

More than 30 experts in ICS threat and vulnerability research, incident response and security analysis

Membership

ISO
IEC
ITU
IEEE Advancing Technology for Humanity
Industry IoT Consortium
GLOBALPLATFORM

Kaspersky ICS CERT – What we do ?

kaspersky

Research cyberthreats
and detect attacks on industrial facilities
providing early alerts to those in danger

Investigate cybersecurity **incidents** at industrial enterprises and critical infrastructure facilities helping to mitigate similar cases in future

Analyze popular industrial control system products and technologies for **vulnerabilities** and help eliminate any vulnerabilities identified

Provide **training** in industrial cybersecurity basics and practical skills to investigate cybersecurity incidents and perform vulnerability research

---

Additionally Kaspersky ICS CERT:

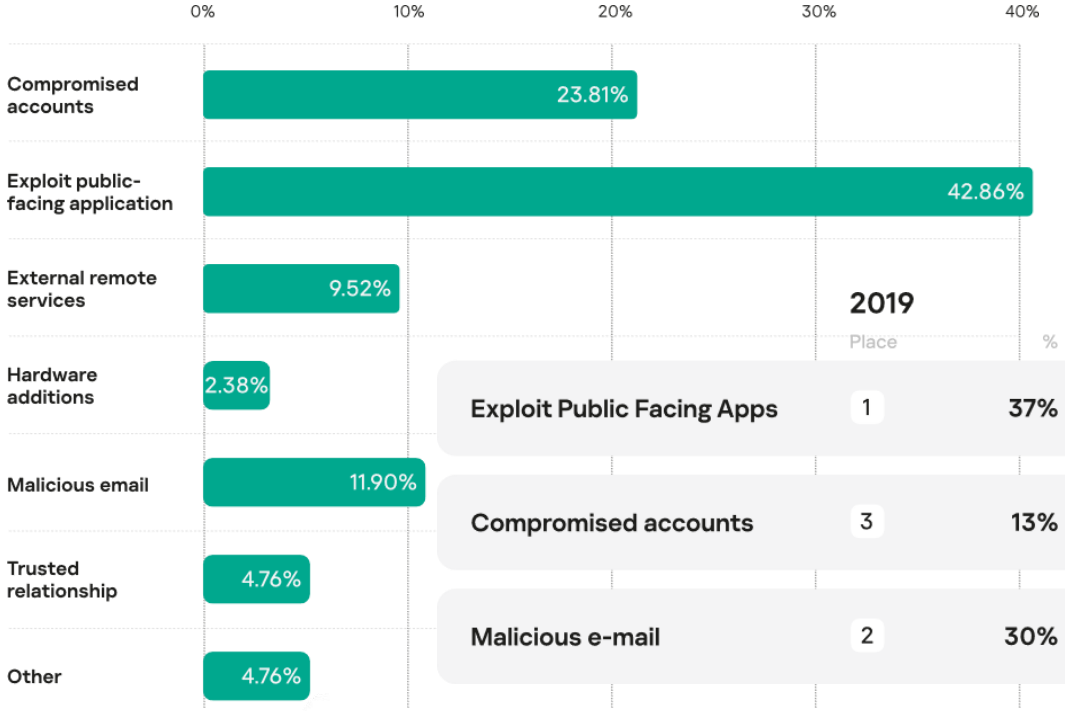
- Develop industrial cybersecurity methodologies, frameworks, and standards -
- Consult industrial organizations on industrial cybersecurity issues -
- Help developers make their products more secure -

Visit ICS CERT website *** Contact us *** Read RFC-2350 document

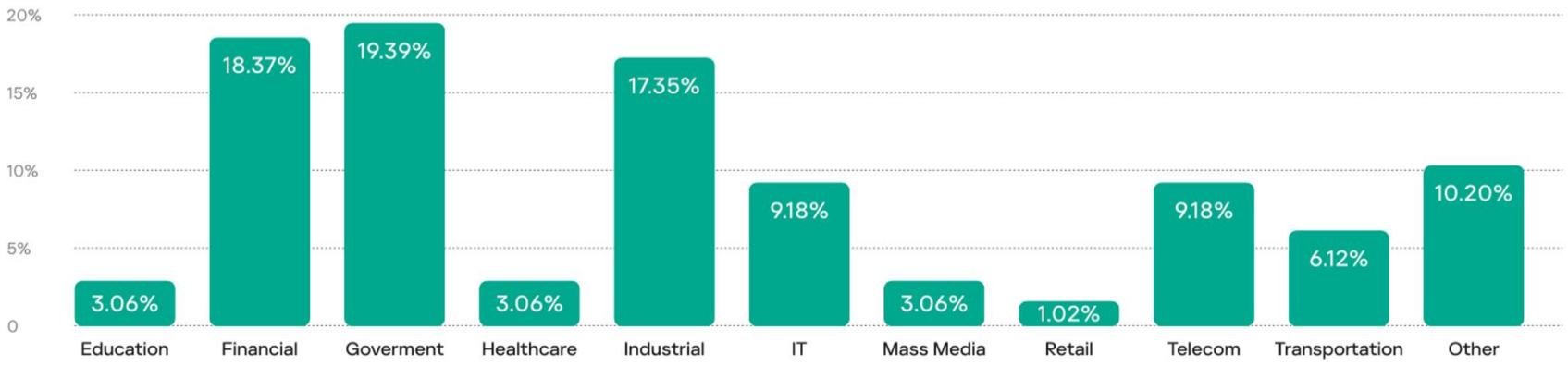
Not If, but when?

kaspersky

Source: Kaspersky GERT



	2019 Place	2019 %	2020 Place	2020 %	2021 Place	2021 %	2022 Place	2022 %
Exploit Public Facing Apps	1	37%	2	31.5%	1	53.6%	1	42.9%
Compromised accounts	3	13%	1	31.6%	2	17.9%	2	23.8%
Malicious e-mail	2	30%	3	23.7%	3	14.3%	3	11.9%

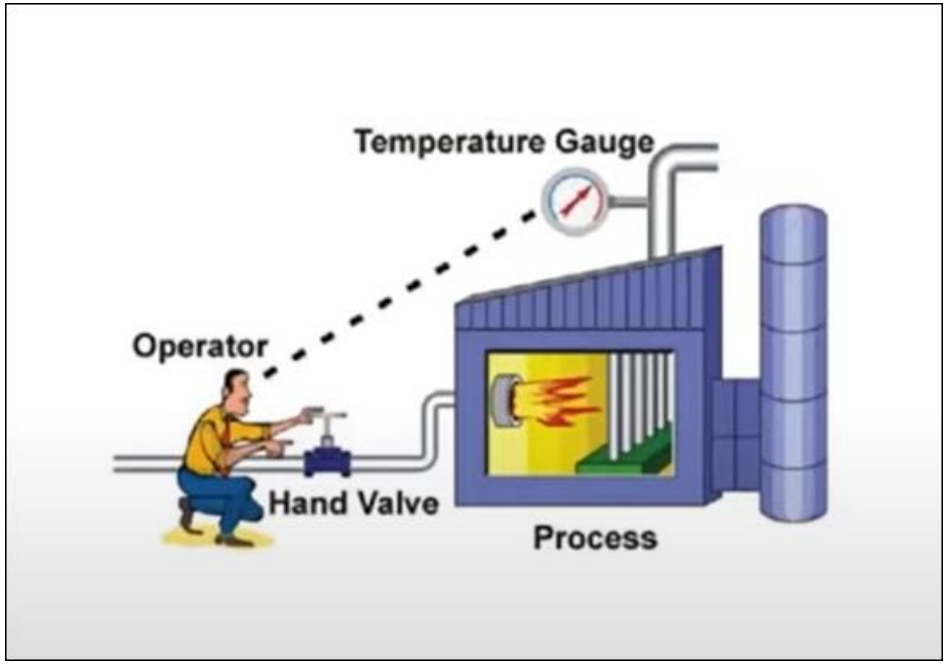


kaspersky

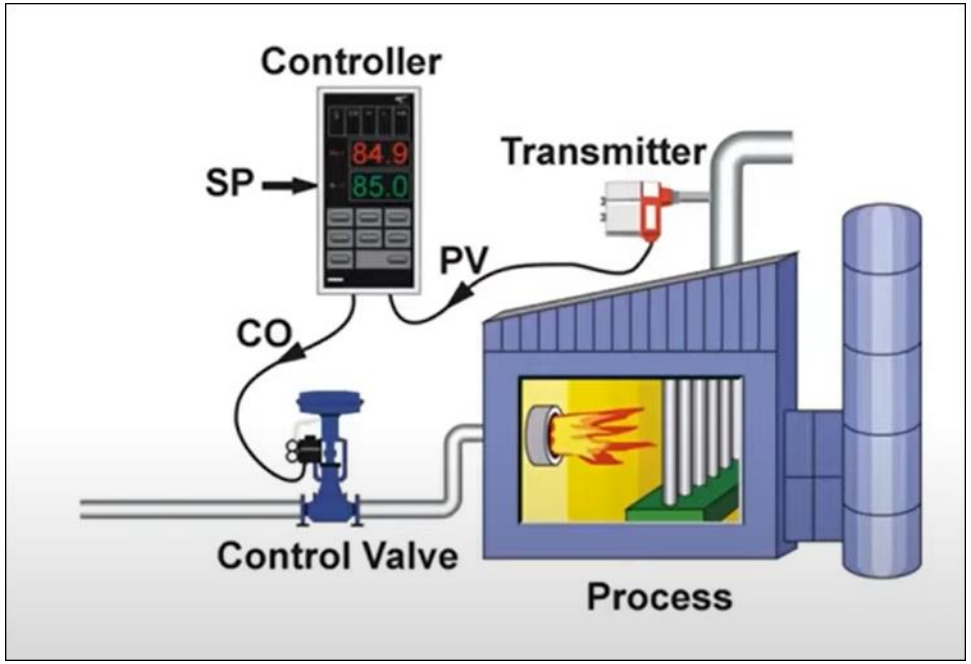
Industrial Cybersecurity

Why is there an increase in attacks on Industrial organization ?

Manual Operations



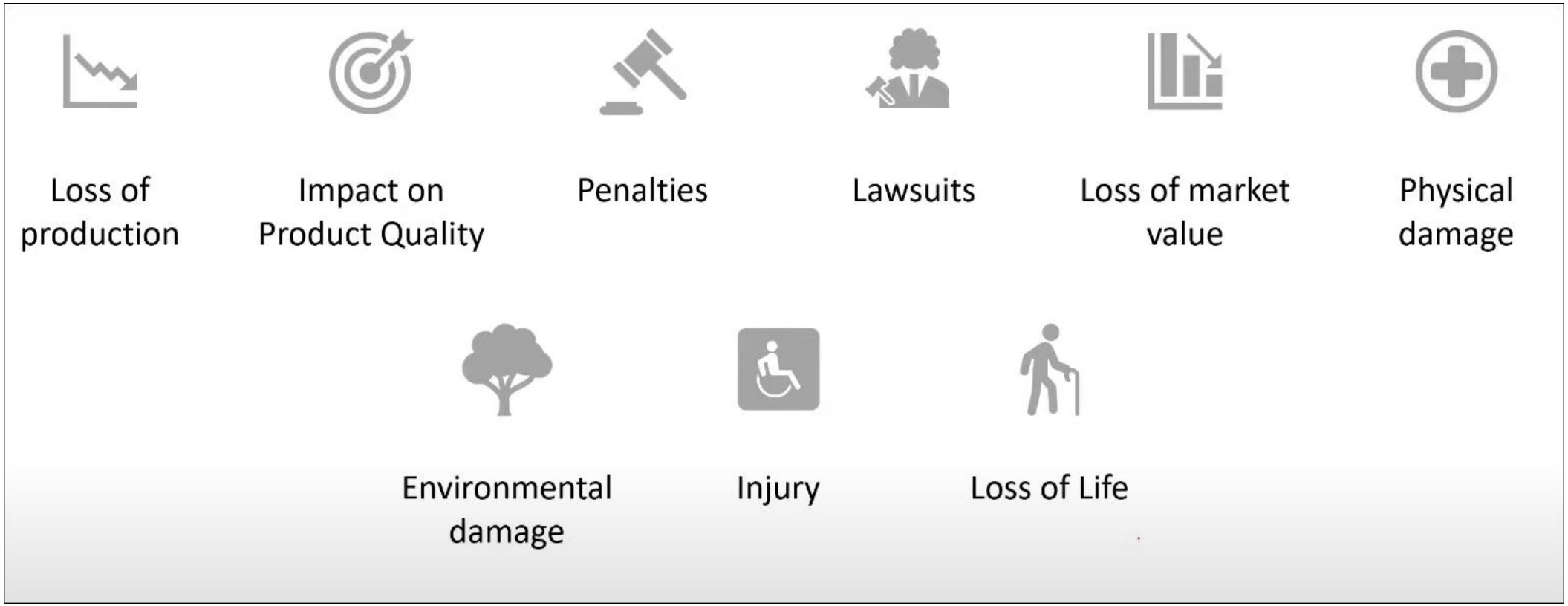
Automation



kaspersky

Industrial Cybersecurity

Why an attack on Industrial Organization is more devastating?



IT vs OT / ICS Cyber Security Differences

kaspersky
Industrial Cybersecurity

Aspect	IT Cybersecurity	OT Cybersecurity
Scope	Information Technology (data, systems, networks)	Operational Technology (industrial devices, control system, physical processes)
Examples of Incidents	Data breaches, malware infections, phishing	Unauthorized access to ICS, Alert on severe vibration of the gas turbine etc
Impact	Affects data integrity, availability, confidentiality	Can lead to operational disruptions, safety hazards, physical damage
Defenses	Firewalls, antivirus, encryption, access controls	Network segmentation, specialized intrusion detection, fail-safe mechanisms
Objective of Attacks	Data theft, unauthorized access	Process disruption, physical damage
Incident Response	Data breach containment, recovery	Operational recovery, safety assurance
Regulations	GDPR, HIPAA, etc.	NIST Cybersecurity Framework, IEC 62443, sector-specific regulations

kaspersky

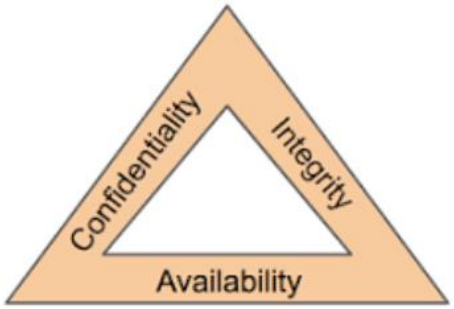
Industrial Cybersecurity

CIA VS SRP TRIAD

Safety

– The most important consideration for ICS
  - The machinery must not hurt people
  - The people can not cause a safety risk

– When an incident happens
  - The system must go to fail-safe

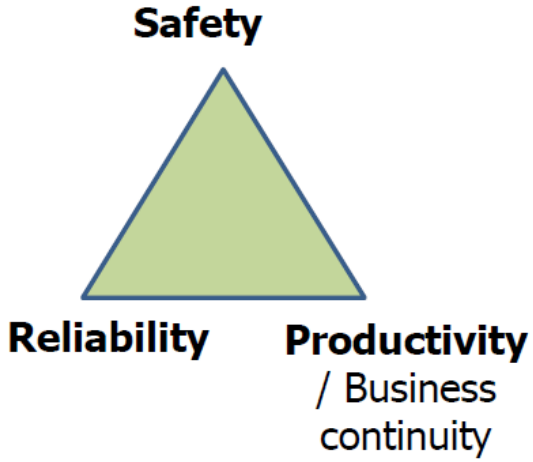


Reliability

– The system operates consistently and reliable
  - Achieved through correct design and redundancy

Productivity

– Business continuity shall be built into the process
  - Achieved through policies, training, and redundancy



kaspersky

Industrial Cybersecurity

ICS : Incident Response (IR) Objectives

- Acquiring forensics data from key ICS assets
- Quickly triaging to understand the threat
- Containing threats while running operations
- Eradicating when its safe for operations
- Ensure physical and environmental safety
- Legacy devices – connectivity and isolation

Incident Response

Traditional vs Modern Incident Response

Traditional Incident Response	Modern Incident Response
Reactive	Proactive
Legacy IR Process	Intelligence-Driven IR Process
Manual	Automated / AI-Driven
Time Consuming	Faster / Rapid
Isolated	Collaborative
Limited Visibility	Comprehensive Visibility
Limited Scalability	Elasticity
On-site / On-Prem	On-Site / Remote / Cloud
Resource Constraints	Resource Optimization

Incident Response Process – A Recap

Where to start (from scratch)….?

- What is the business process and the underlying information system?
- What are the objectives?
- What are the assets?
- What about resources?
- What about roles and responsibilities?
- What about plans, playbooks, checklists?
- What about incident definition, incident categories, prioritization, cyber risk, etc.?

kaspersky

Industrial Cybersecurity

Before incident:

- Collect all devices firmware distributives and updates
- Collect all versions of programs for all devices
- Copy all serial numbers, MAC and IP addresses of all devices
- Hardware configuration of system and network, schematics and diagrams
- Enable logging if devices are support it
- Keep in touch with ICS support teams
- Make trainings for ICS information security emergency cases

TO DO LIST difference with ICS systems

kaspersky

Industrial Cybersecurity

In case of incident:

- First of all check that people are in safe! Because manufacturing can be damaged!
- Keep devices working (if it’s possible and safe)
- Obtain as much information as possible about any open network connections
- Collect data about all running programs and tasks from all devices
- Collect all programs from PLC and RTU
- All points from corporate system checklist
- Cooperation with ICS support team
- More cooperation with IT and security

Challenges in ICS/OT incident response

kaspersky

Industrial Cybersecurity

- If it is a malfunction or an attack?
- if the incident has occurred on IT network or OT network ?
- If the incident has occurred on some asset in IT network, does that asset has connectivity to OT network ?
- Is there a way to contain or isolate an IT asset without any disruption in Physical process ?
- Dealing with Multiple stake holders (e.g. operators, maintenance teams, engineers, cyber analysts)
- Availability Versus Understanding the Incident
- Proprietary protocols
- Lack of understanding of consequences & impact during Incident Response
- Not easy to practice TTX
- Legacy systems would not be able to run advanced tooling required during IR
- Offline Versus Online Digital Forensic

Incident Response Frameworks – A Recap

- Following standards
- Support building teams internal and external facing incident response teams
- There is no need to adopt all steps of one framework
- Tailor them to the organization's need
- Focus on business value or technical value

kaspersky

Industrial Cybersecurity

Incident Response (IR) Management

IR team

- Data collection
- Initial vector identification
- Definition of TTPs (Techniques, Tactics & Procedures)

Everyone has different goals and priorities

An attacker

- To reach the malicious goal

An organization victim

- Continuation of business processes
- Reputation of organization
- Pressure of top management
- Penalties & Fines

Facility Management & OT Specialist

- Ensure Physical Safety
- Ensure the factory is operational all the time.
- Ensure no environment hazards

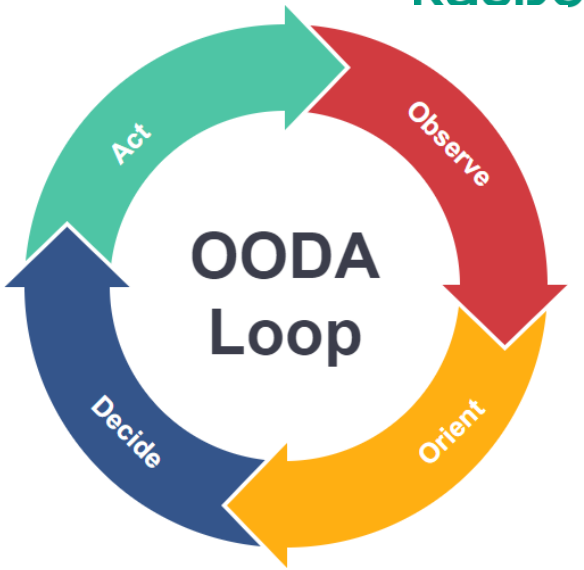
Key People in Cyber Crisis Management

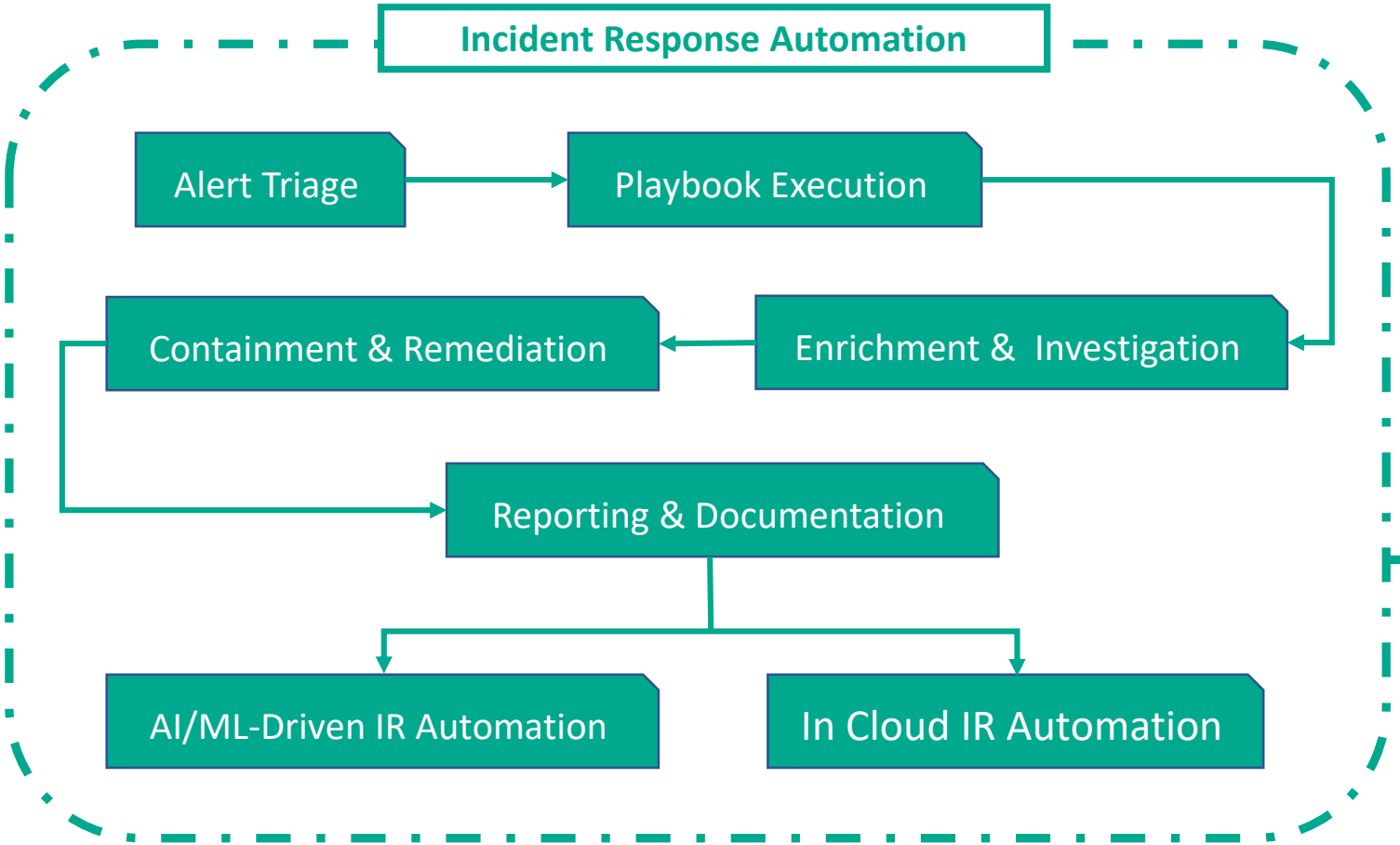
- Incident Response Manager
- Incident Response Analyst
- Threat Intelligence Team
- SOC team
- IT Coordinator
- Risk Management
- PR Manager
- Legal Advisor
- **ICS/OT Security Specialist**
- **OT Engineers**
- **Facility Maintenance team**

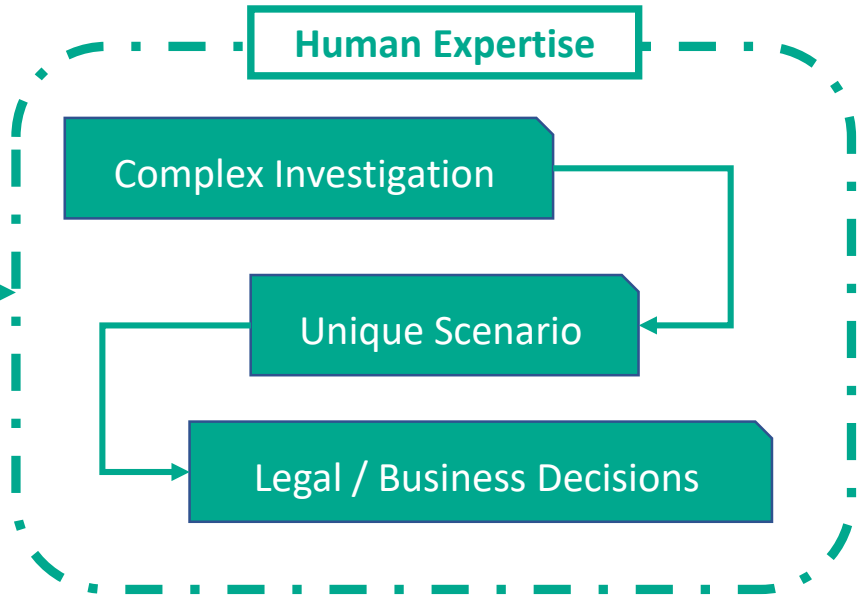
kaspersky

Automation in Incident Response

- SIEM + XDR + SOAR + Case Management
- Sandbox + IOA + IOC + TI + TH + VM for wider coverage







Incident Response for Large Scale Investigations

Challenges in Large-Scale Investigations:

- The sheer volume of data to analyze
- The need for quick response and mitigation
- Coordination access multiple systems, teams, and possibly geographic time zones & locations
- Budget constraints – limited resources for tools for monitoring, detection, hunting & automations

Requirements for an Effective Response

Robustness
Ability to handle vast amount of data and types of incidents

Speed
Rapid Identification, investigations and response to limit damage

Efficiency
Tools should streamline rather than complicate the IR process

Incident Detection

kaspersky

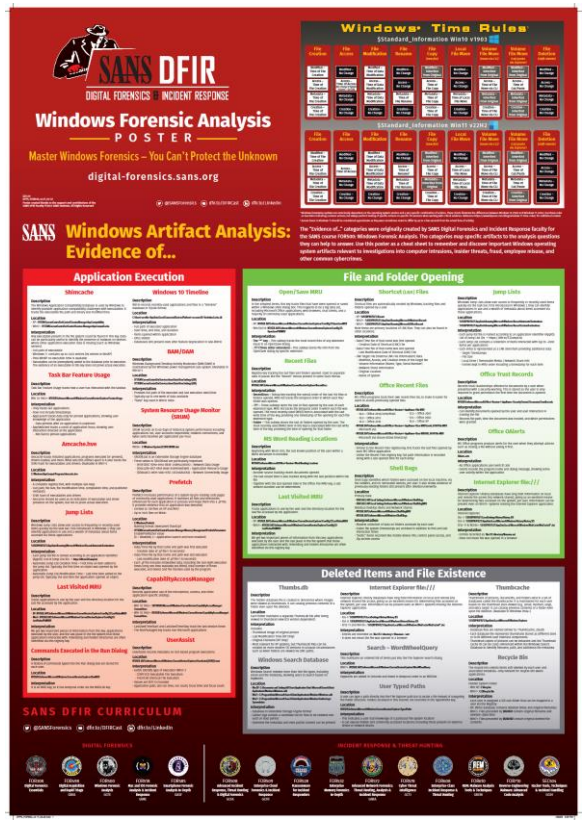
Industrial Cybersecurity

Typical initial alerts in ICS/OT environment

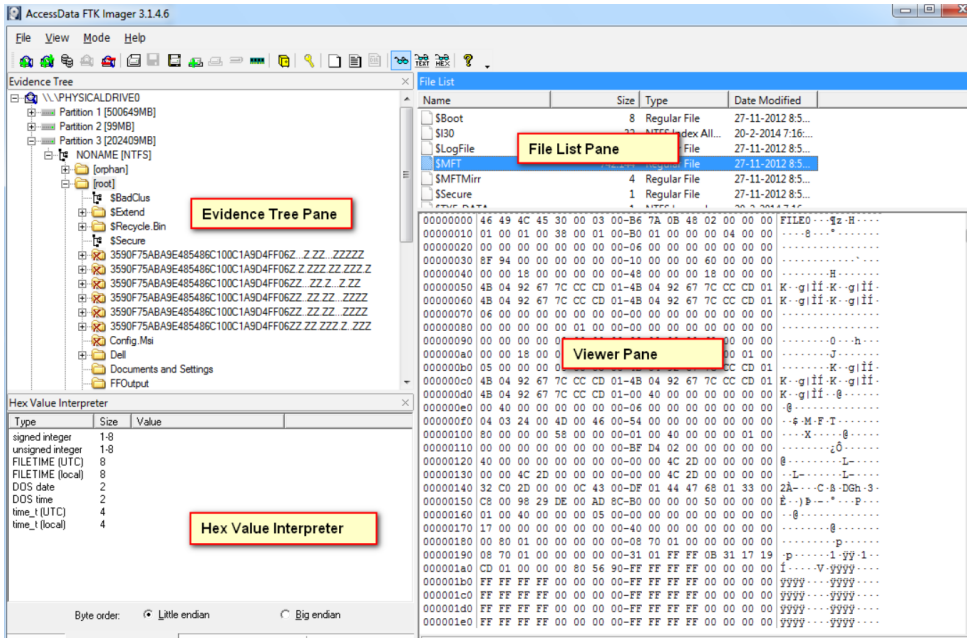
- Scenario 1: The HMI Screen is not getting field updates
- Scenario 2: The Power Plant stopped producing energy
- Scenario 3: Alert on severe vibration of the gas turbine
- Scenario 4: The mouse on the HMI screen is moving
- Scenario 5: The IT stopped receiving ICS data
- Scenario 6: CCTV shows people nearby the generator
- Scenario 7: Alert on sudden activation of the SIS
- Scenario 8: The operator sees high boiler pressure
- Scenario 9: Instruction to shut down the plant
- Scenario 10: The CERT is reporting on attacks worldwide

Incident Detection

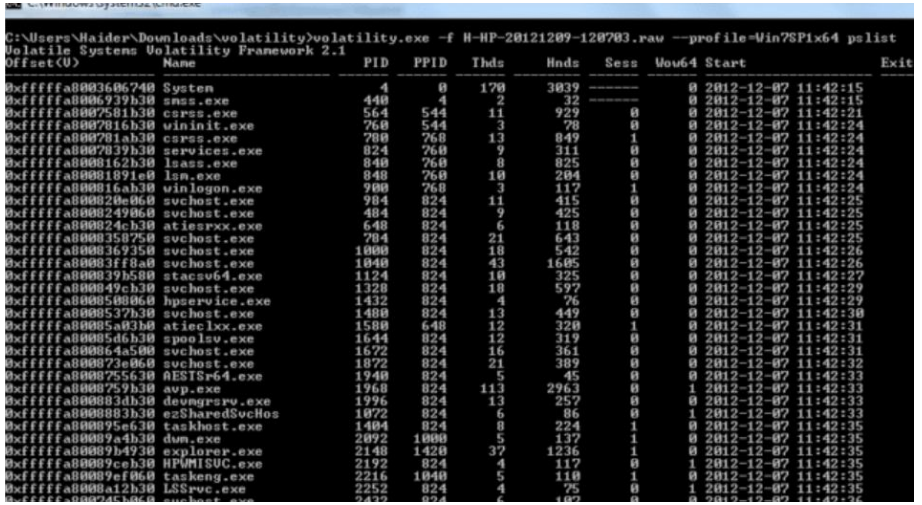
Quick Artefacts



Disk image analysis



Memory image analysis

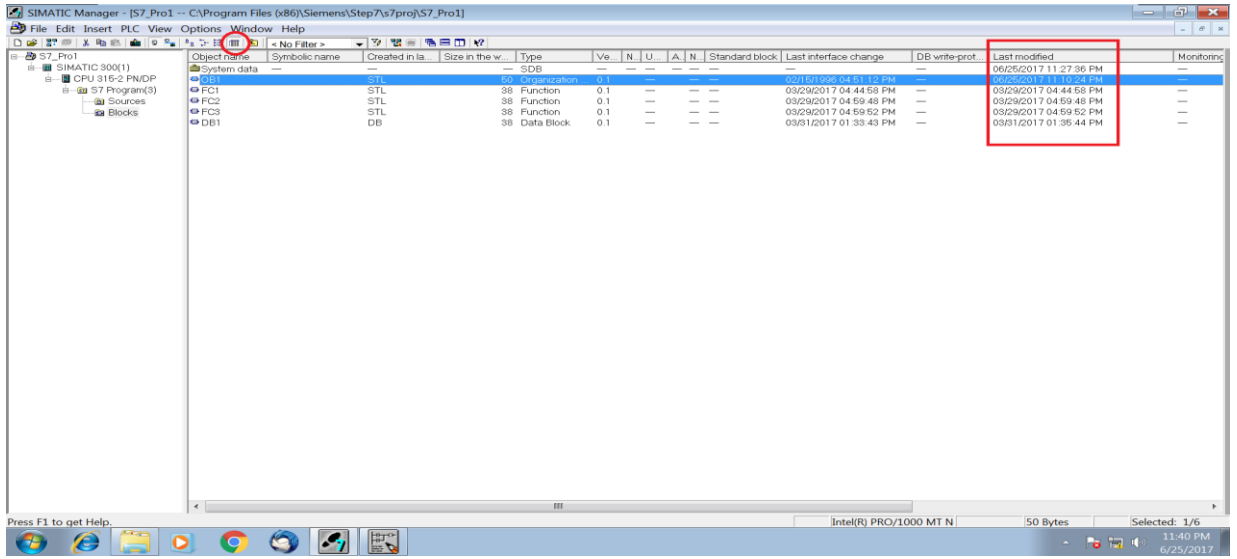


Differences between forensic and ICS forensic

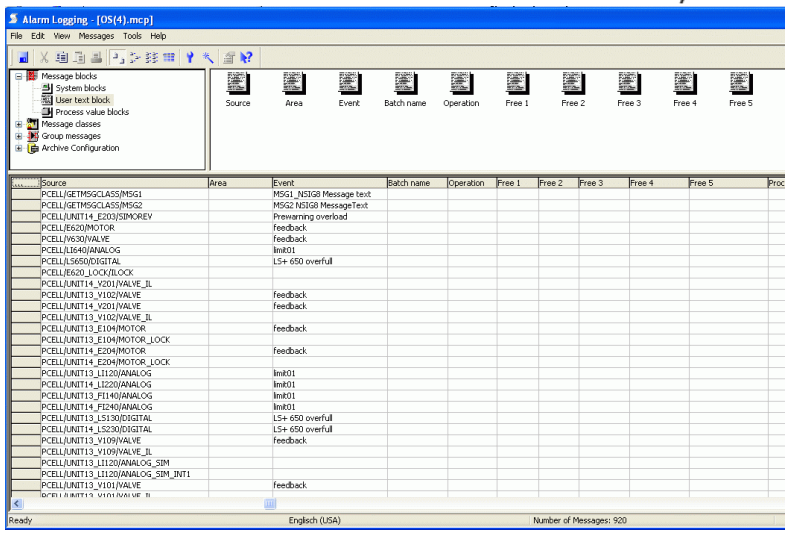
kaspersky

Industrial Cybersecurity

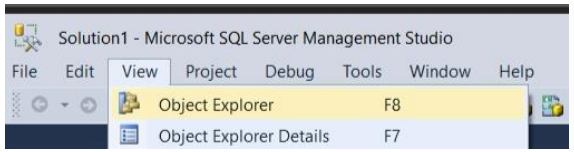
PLC

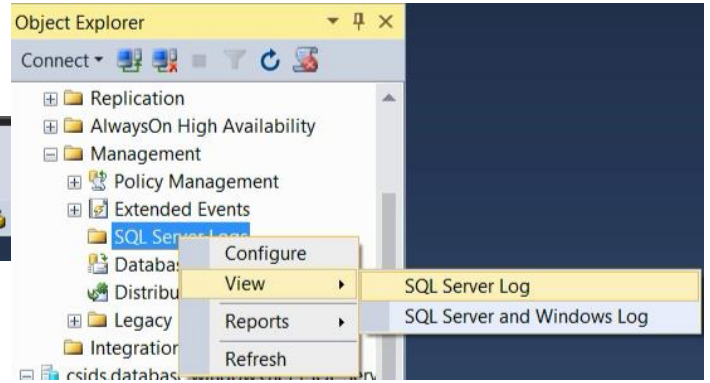


SCADA

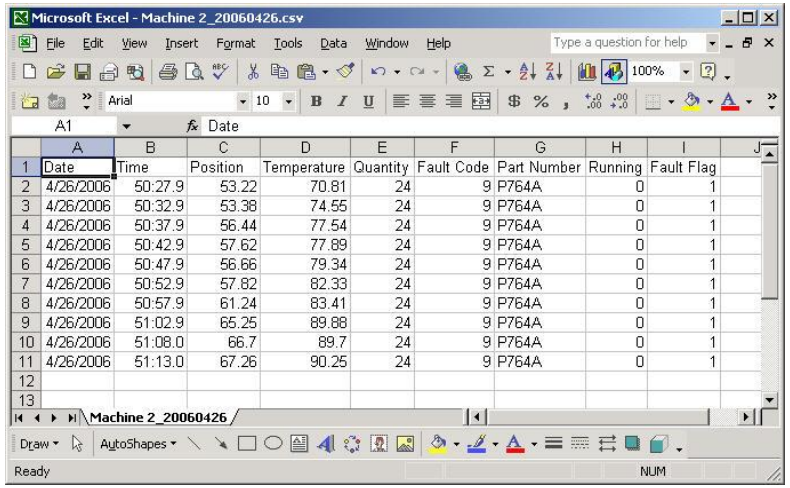


Historian Server





OPC

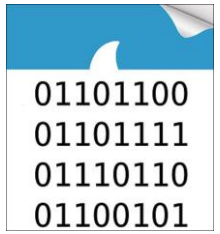


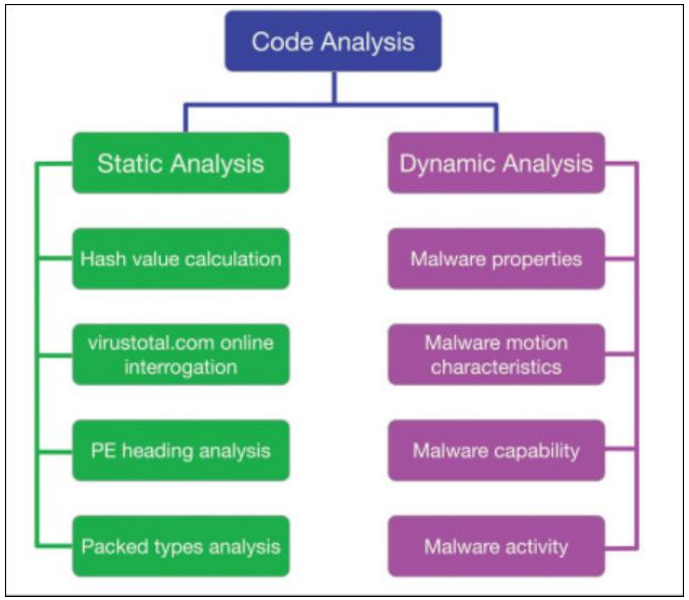
	A	B	C	D	E	F	G	H	I
1	Date	Time	Position	Temperature	Quantity	Fault Code	Part Number	Running	Fault Flag
2	4/26/2006	50:27.9	53.22	70.81	24	9	P764A	0	1
3	4/26/2006	50:32.9	53.38	74.55	24	9	P764A	0	1
4	4/26/2006	50:37.9	56.44	77.54	24	9	P764A	0	1
5	4/26/2006	50:42.9	57.62	77.89	24	9	P764A	0	1
6	4/26/2006	50:47.9	56.66	79.34	24	9	P764A	0	1
7	4/26/2006	50:52.9	57.82	82.33	24	9	P764A	0	1
8	4/26/2006	50:57.9	61.24	83.41	24	9	P764A	0	1
9	4/26/2006	51:02.9	65.25	89.88	24	9	P764A	0	1
10	4/26/2006	51:08.0	66.7	89.7	24	9	P764A	0	1
11	4/26/2006	51:13.0	67.26	90.25	24	9	P764A	0	1
12									
13									

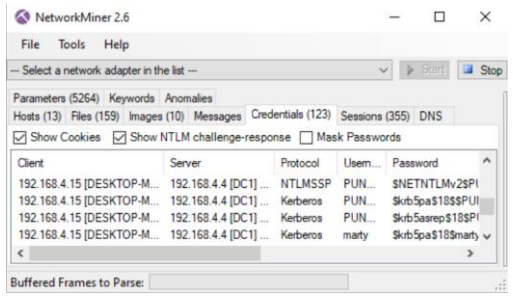
Incident Detection

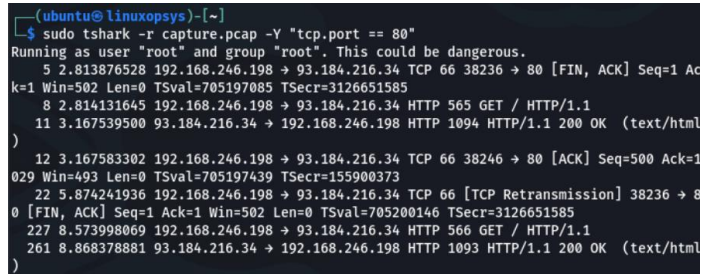
Malicious File

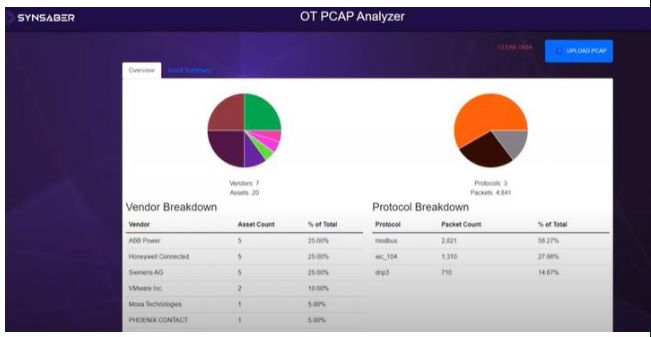
PCAP











Incident Detection

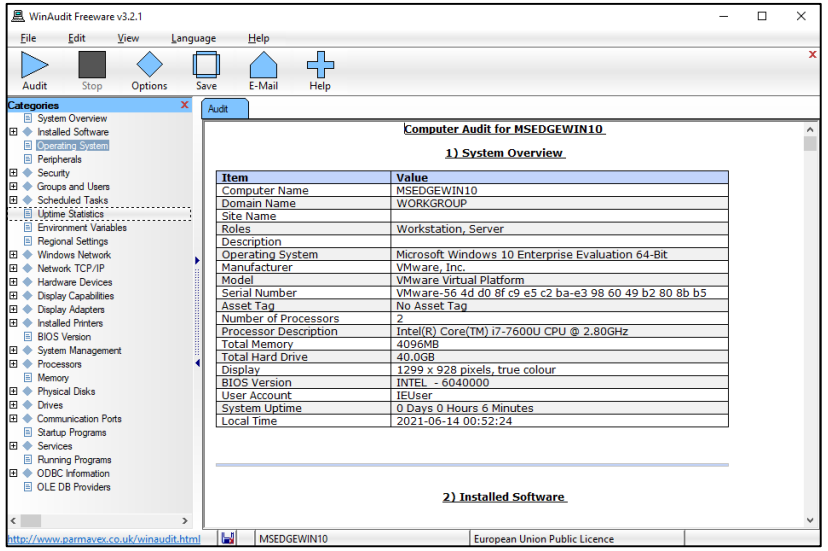
Using the power of both, Windows PowerShell and Windows Management Instrumentation

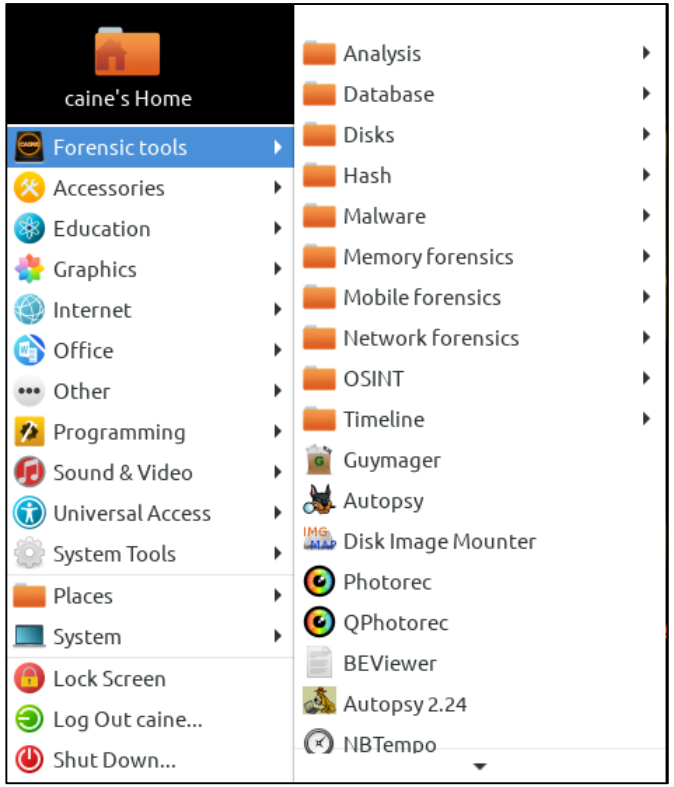
- WMI available starting with Windows ME
- PowerShell available by default since Windows 7
- Used for administrative purposes
- Flexible processing and filtering functions
- Local and remote command and/or script execution
- PowerShell:
  - Integrated scripting environment for script development and debugging
  - Continuous improvements and development

Incident Detection

Computer Aided Investigative Environment (Caine)

- Bootable into a Linux System
- All devices are unmounted by default
- Shipped with portable tools for DFIR
- Live system
  - WinAudit
  - NirLauncher



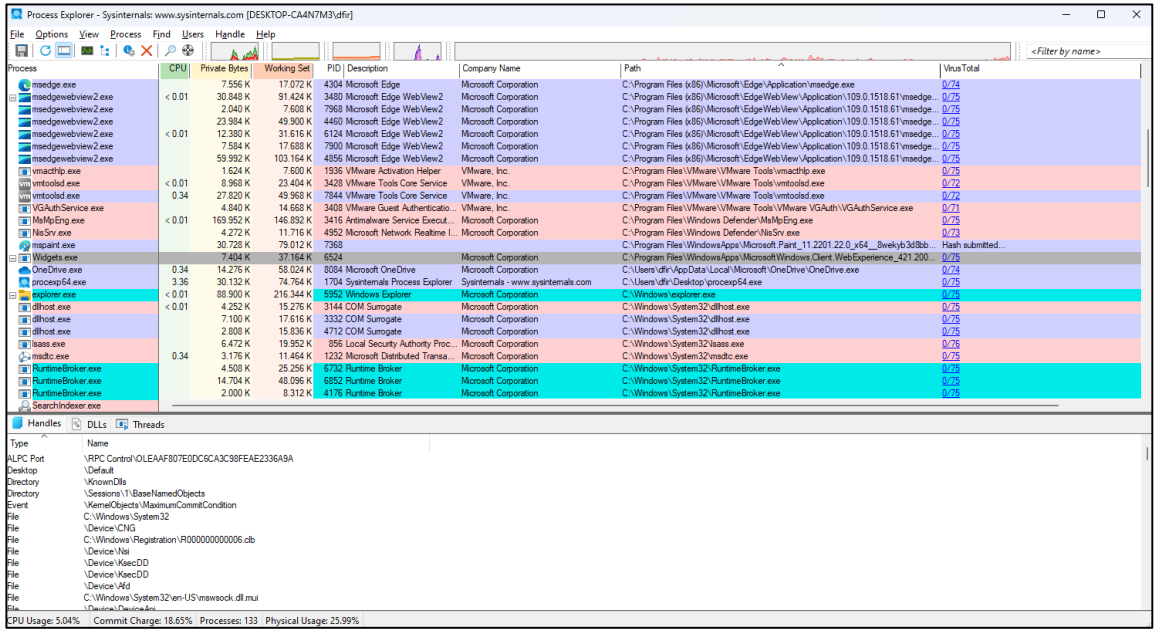


https://www.caine-live.net/

Incident Detection

Sysinternals Process Explorer

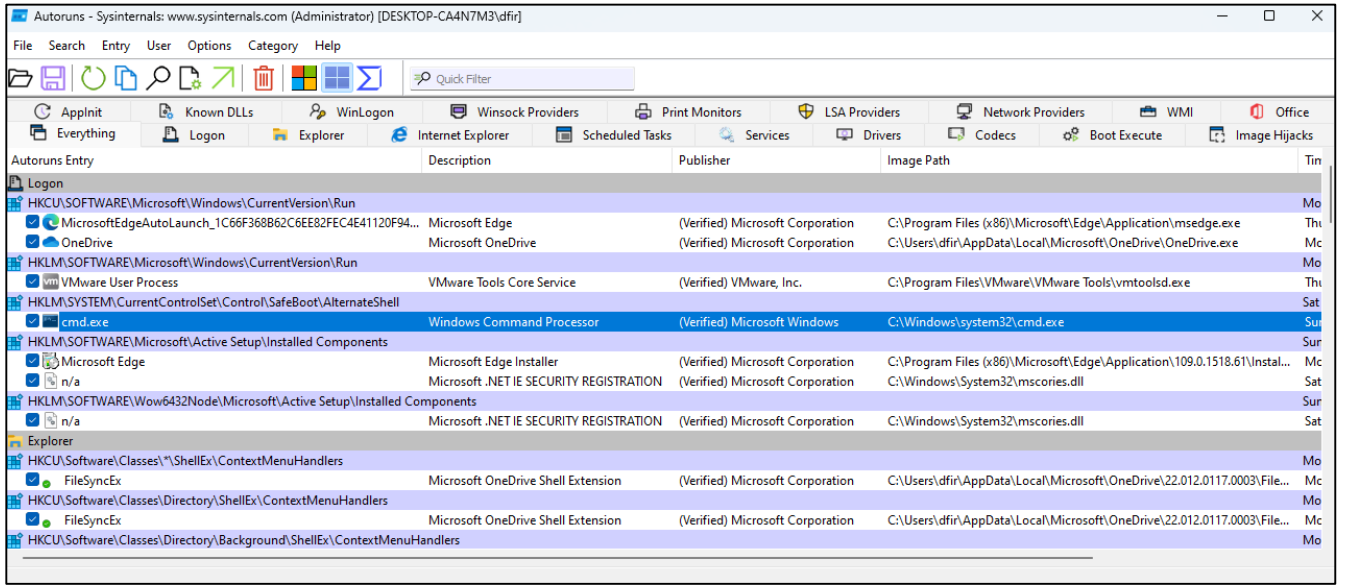
- Displays information about processes and their handles and loaded DLLs
- Color coding
- Detailed information about a process security
- Suspend or dump a process
- Strings of a process
- TCP/IP endpoints
- VT integration
- Etc.



Incident Detection

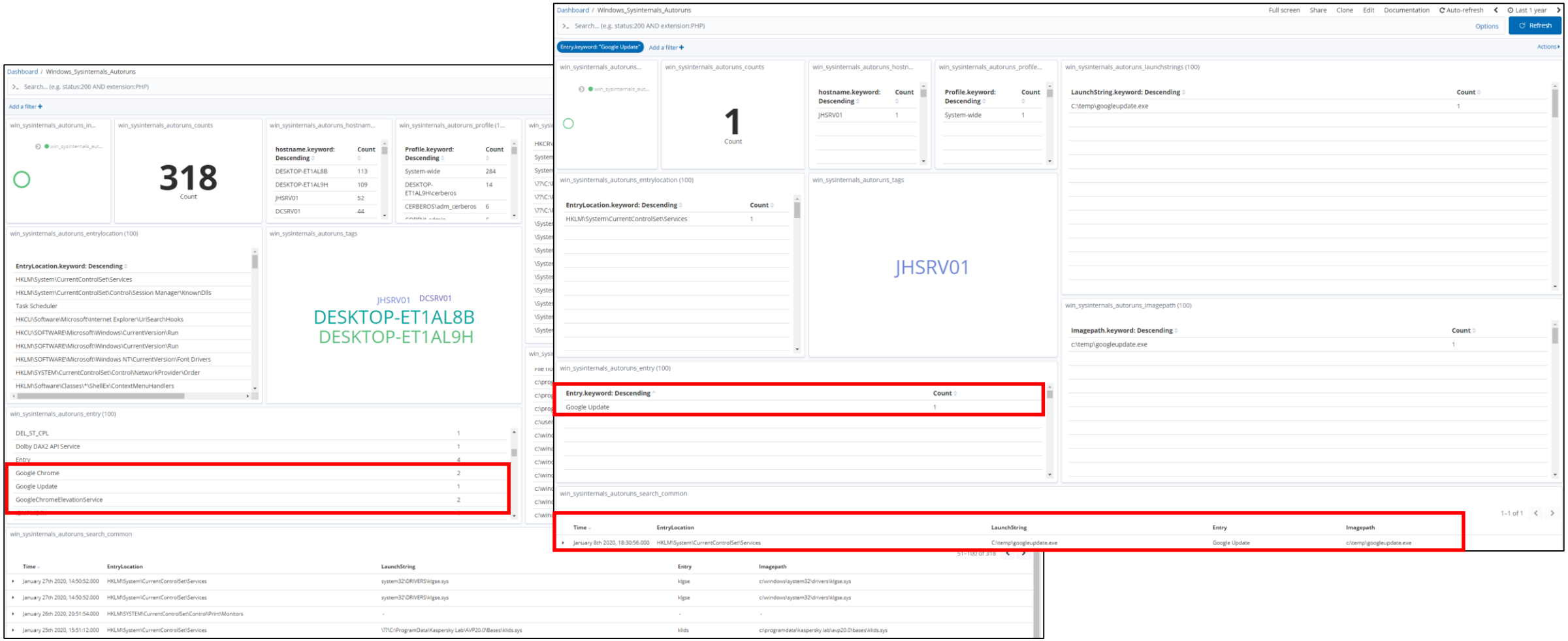
Sysinternals Autoruns

- ASEP manager
- Comprehensive knowledge of autostart locations
- Hiding feature
- Jump to entry
- Jump to image
- Offline scan
- Deleting entries
- VT integration
- Etc.



Incident Detection

Sysinternals Autoruns in enterprise environment (cont)



Incident Detection:

Lateral Movement

Incident Detection

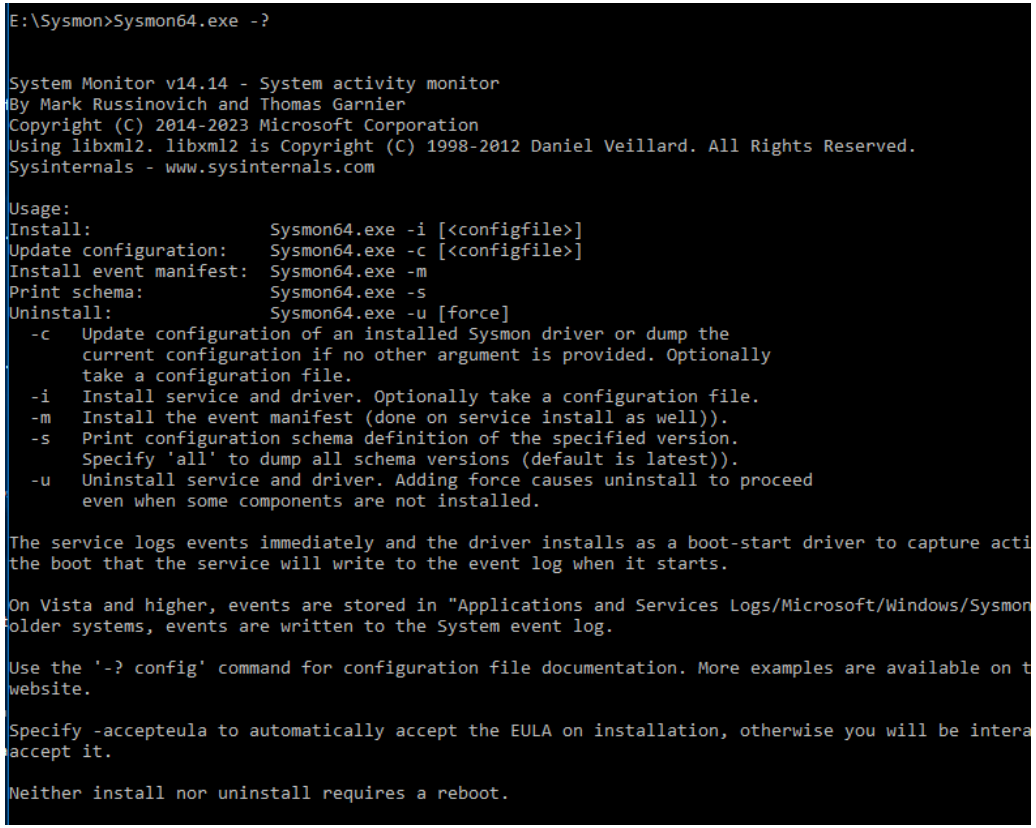
Do we capture all the events we need for investigation?

- Gap between happening and recording of activities
  - Missing process creation information
  - Limited network connection information
  - Process tampering
  - Access of a process
  - File creation events
  - Network pips
  - Registry
  - WMI

Incident Detection

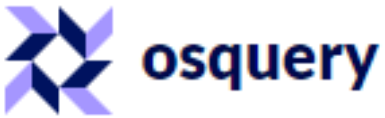
Microsoft System monitor (or Sysmon)

- Windows system service or driver
- Remains resident
- Extends Windows logging capabilities
- Fix the mentioned gaps
- Does NOT provide analysis nor protects you
- Events are stored under Microsoft-Windows-Sysmon%4Operational.evtx
- Using Windows Event Collector etc. for forwarding
- Usage
- https://download.sysinternals.com/files/Sysmon.zip



Incident Response - osquery

- Universal open-source endpoint for operating system instrumentation, monitoring, and analytics framework
- Allows easily ask questions about Linux, MacOS and Windows via standard SQL
- Supports ad-hoc or scheduled queries
- Provides ability to query and log like:
  - Running processes
  - Logged in users
  - Password changes
  - Listening ports
  - File Integrity Monitoring
  - Yara rule hunting
  - And many more…..



Incident Response

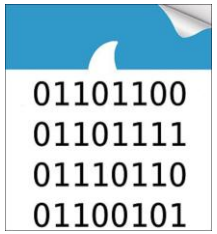
Using different kind of tools for analysis & hunting….

- LogonTracer - https://github.com/JPCERTCC/LogonTracer
- ChainSaw & Sigma Rules - https://github.com/WithSecureLabs/chainsaw
- HayaBusa - https://github.com/Yamato-Security/hayabusa
- APT-Hunter - https://github.com/ahmedkhlief/APT-Hunter
- EVTXHussar - https://github.com/yarox24/EvtxHussar
- Rheagal - https://github.com/AbdulRhmanAlfaifi/Rhaegal
- Persistence Hunter - https://github.com/last-byte/PersistenceSniper

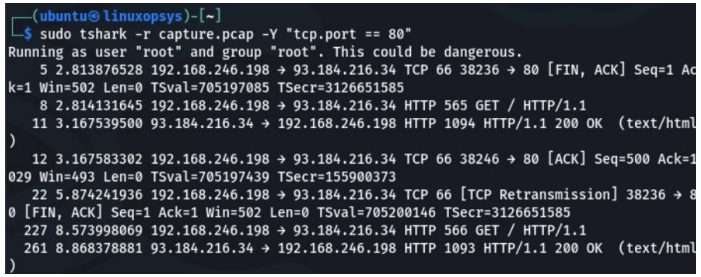
Incident Detection

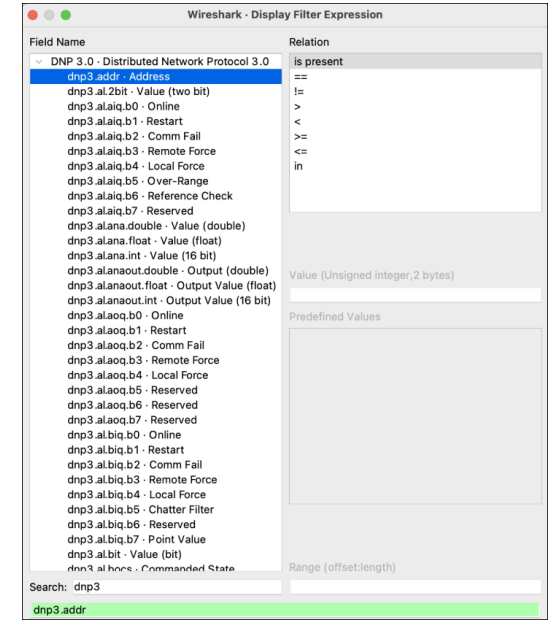
Network Analysis

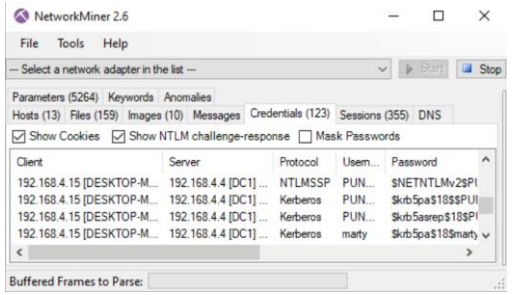
[Practice : https://www.malware-traffic-analysis.net/2023/index.html](https://www.malware-traffic-analysis.net/2023/index.html)

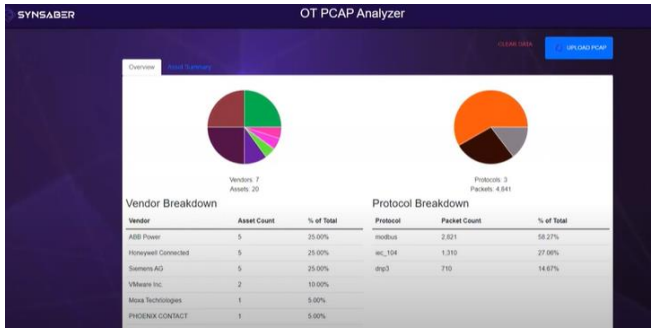


PCAP





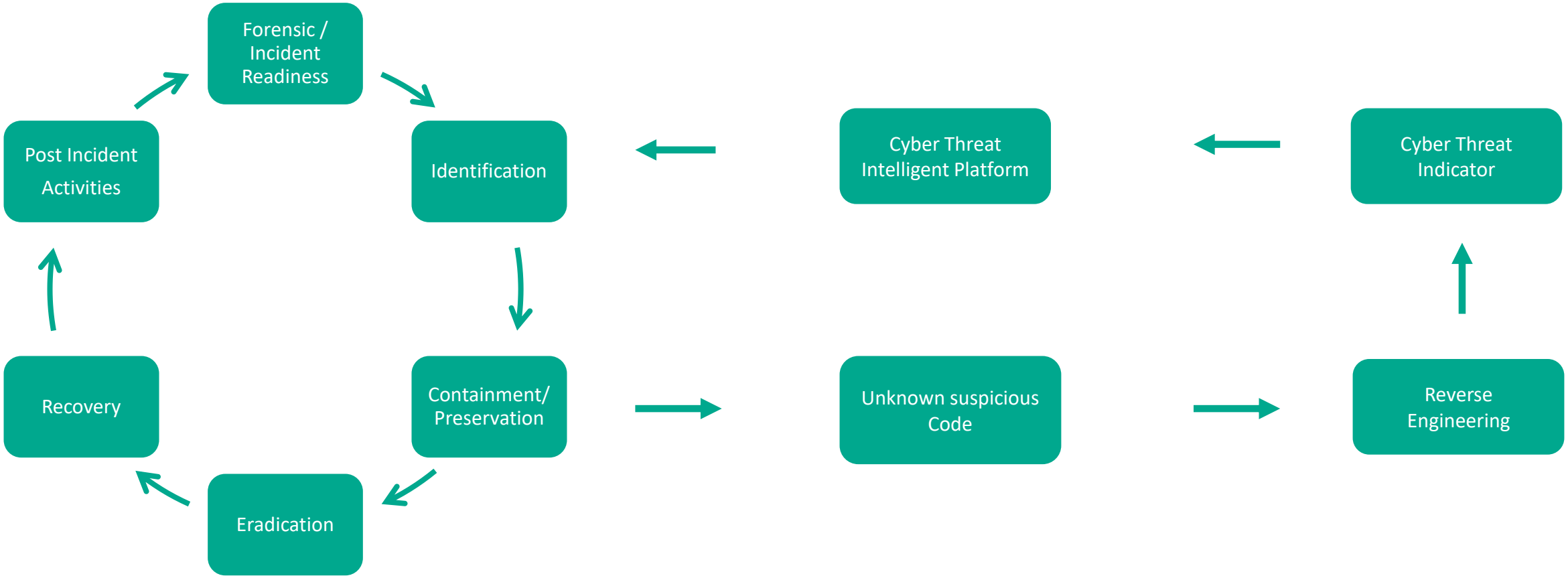




Intelligence-Drive Incident Response

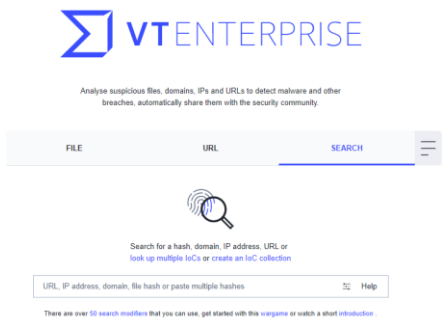
Intelligence-Driven Incident Response

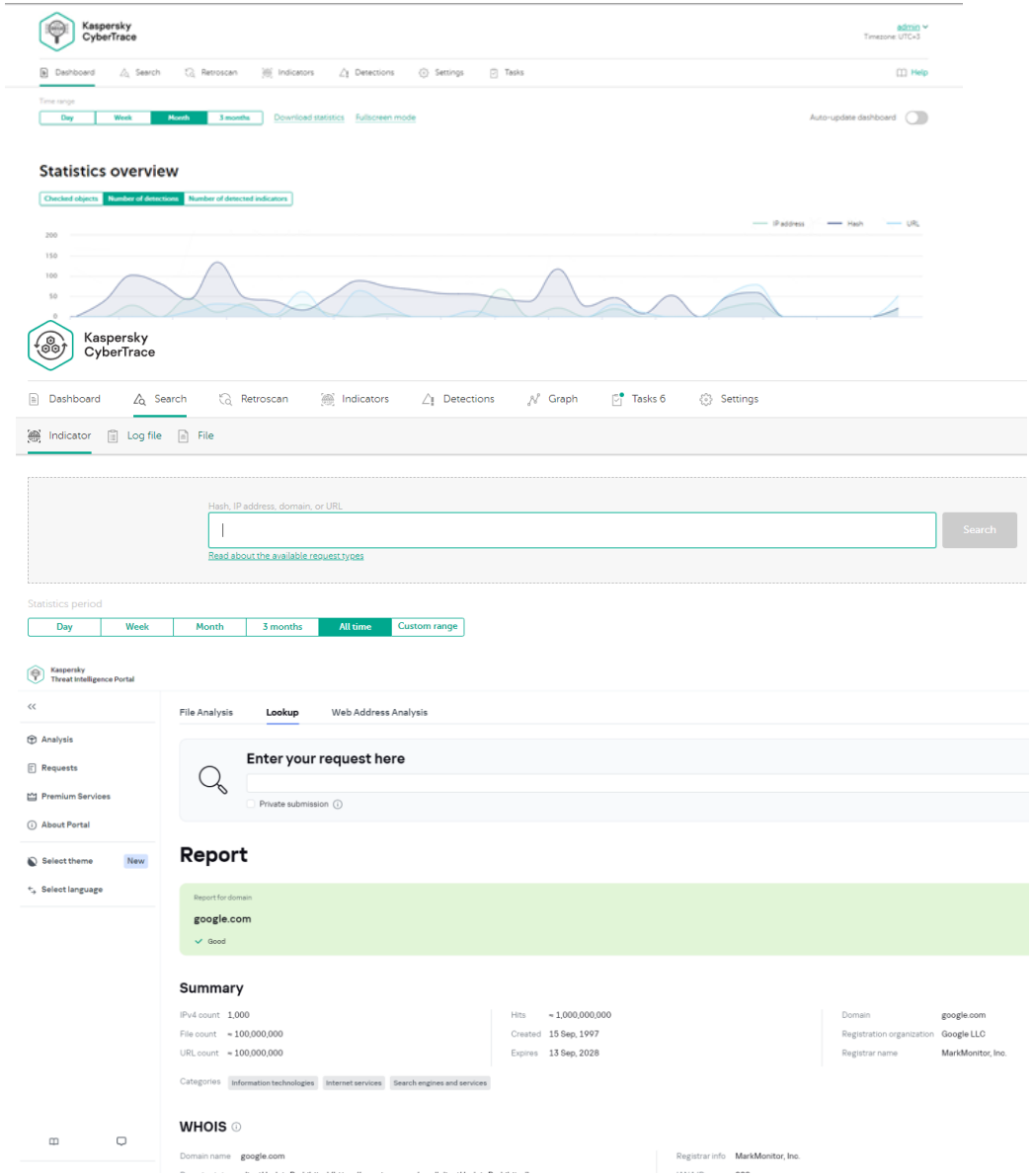
Using Cyber threat intelligence during the incident response



Intelligence-Driven Incident Response

- **Cyber Trace**
  - Aggregates indicators of compromise (IoC) from various sources
  - Multi-Platform SIEM integration & connector supported
  - Commercial, OSINT & custom feed available
  - **Free Community Edition available** with no more than 250 events per second are processed and a maximum of 1,000,000 records can be loaded from all threat intelligence sources.
- **OpenTIP**
  - https://opentip.kaspersky.com/
  - File analysis
  - Lookup-service
- **VirusTotal**
  - https://www.virustotal.com/
  - File analysis
  - Lookup-service
  - File History

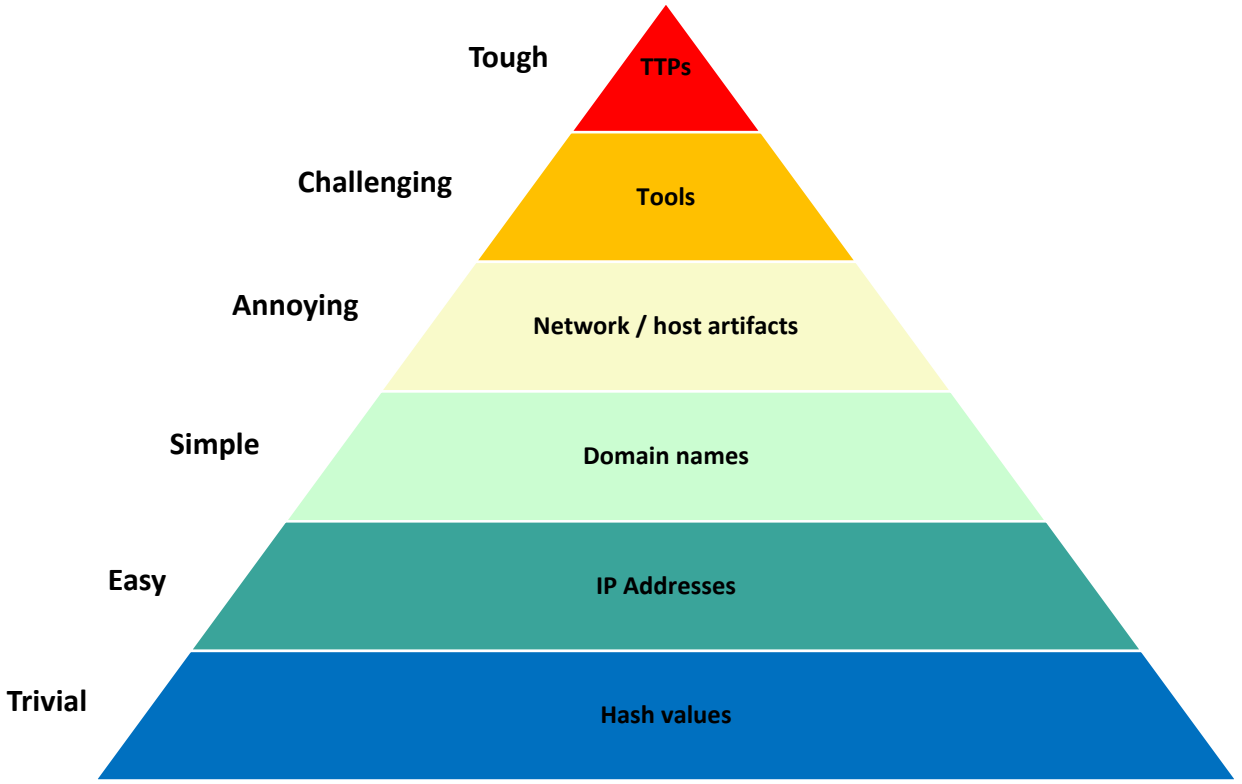




Intelligence-Driven Incident Response

Pyramid of Pain

- Developed by David Bianco 2013
- Description of the construct
  - Between the IoCs and IOA and their leverage effect
  - Ability to modify them during an attack



kaspersky

The MITRE ATT&CK framework

- Knowledge base of Adversarial Tactics, Techniques and Common Knowledge
- MITRE is a non-profit organization
- Comprehensive list of known TTP used by TA used for different cyber domains
- Based on real-world observations
- Each category is divided into subcategory
- Focus on initial and post compromise
- Different frameworks
- https://attack.mitre.org/

ATT&CK®

Incident Response Tools - YARA

- YARA or Yet Another Regex Analyzer or “Swiss Army Knife”
- Identify and classify malware
- Find new malware samples based on family specific features
- Find new exploits and zero days
- Help speeding up incident response
- Increase your defences by deploying custom rules inside your organization
- Classification: identify file formats, archives, packed files, known threats
- Filter network traffic
- Build your own private antivirus.

https://yara.readthedocs.io/en/stable/index.html

https://github.com/VirusTotal/yara/releases

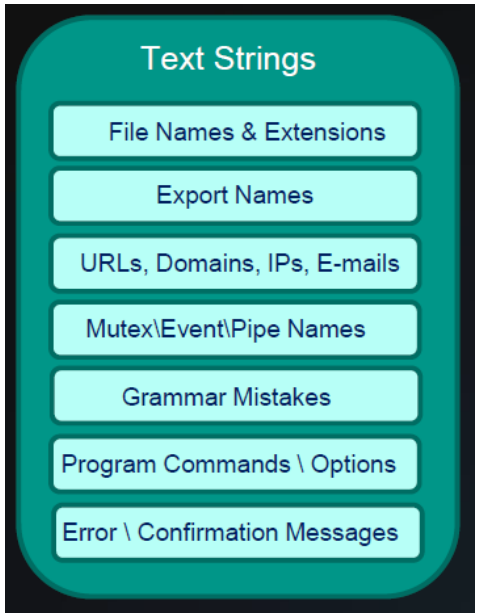
Incident Response Tools - YARA

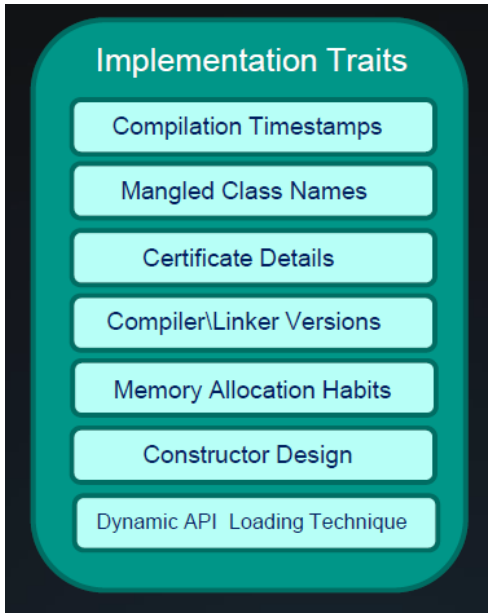
Default usage of yara

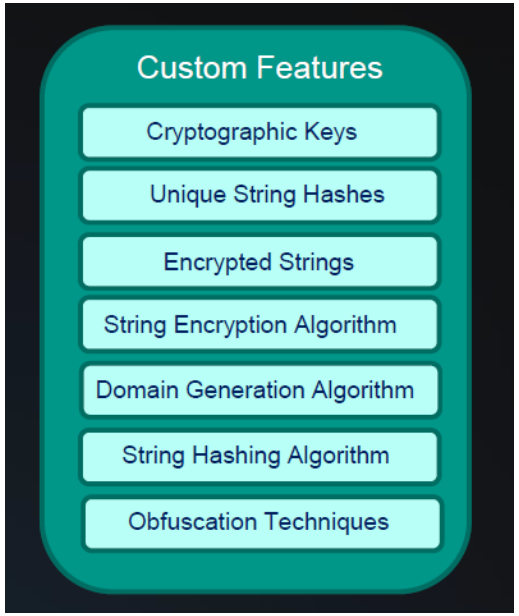
- yara.exe [options] <rule-file>.yar target
- yara.exe –g –m –r <rule-file>.yar <PID>

Options	Description
-r	Folder recursive scan
-s	Print strings
-m	Print meta data
-g	Print tags

Design tips







- Tools for yara: any string analyzer, PE-Studio, CFF explorer, hex-view, any editor

Intelligence-Driven Incident Response

Tools for writing yara rules

- Any string analyzer
  - Common Linux “strings“ tool
  - FLOSS
  - YarGen - https://github.com/Neo23x0/yarGen
  - YaraDbg - https://yaradbg.dev/
- PE file structure viewer
  - PE studio (free and commercial version)
  - CFF explorer
- Hex viewer
  - HxD
  - FAR
- Kaspersky KLARA
  https://github.com/KasperskyLab/klara
- Any editor (which supports yara syntax ☺)

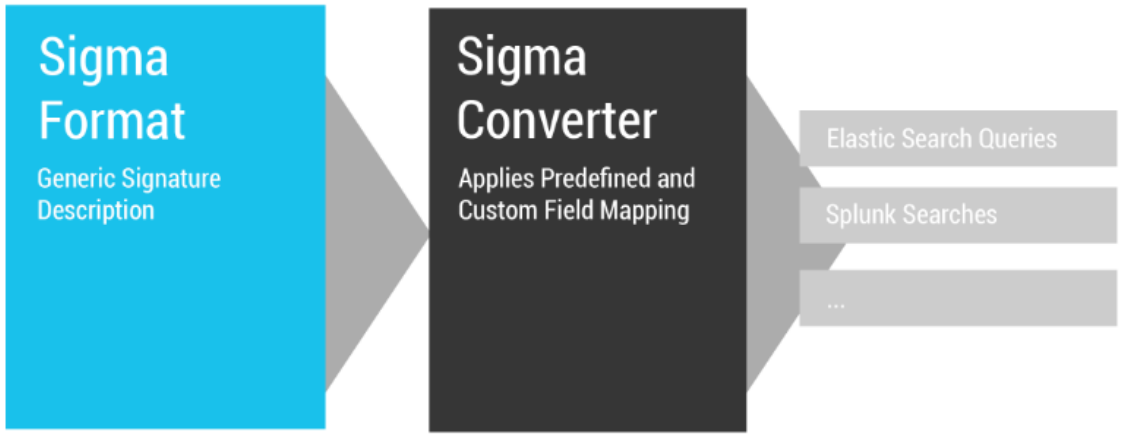
Intelligence-Driven Incident Response

Other useful Yara Scanner

- Yara-Scanner
  https://github.com/iomoath/yara-scanner
- YARAify
  https://yaraify.abuse.ch/
- Loki
  https://github.com/Neo23x0/Loki
- Kraken
  https://github.com/botherder/kraken
- Spyre
  https://github.com/spyre-project/spyre
- Clara
  https://github.com/abhinavbom/clara
- FastFinder
  https://github.com/codeyourweb/fastfinder

Incident Response - Sigma

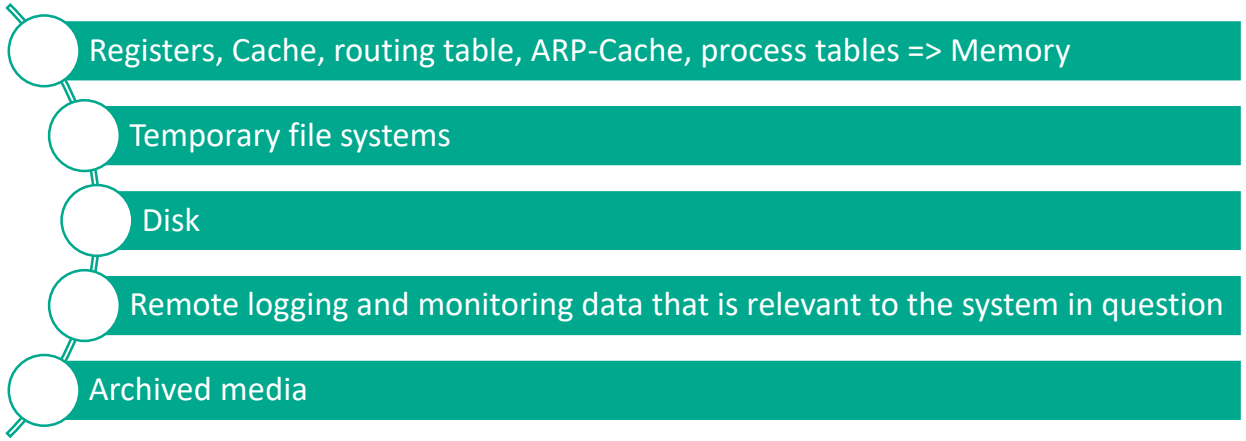
- Open-source project
- Sigma is for log files what snort is for network and YARA for files
- Used to identify pattern in log events based on generic signature formats
- Based on rules written in YAML
- Typical approach
- Avoiding vender-lock
- Sharing signature with TI community
- https://github.com/SigmaHQ/sigma



Evidence Collection

Evidence collection

- After identifying the incident, we have to acquire the digital artifacts
- Full and proper acquisition is a critical step in successful Digital Forensics
- Status of the system is critical
- Considering volatility order when acquiring digital media (RFC3227)



- Can be (host|network)-based or other evidence data

Evidence Collection

List of DON'TS:

- Do not:
  - Power off the system, if running, until you acquire all possible data
  - Power off the system, if shut down, since malicious startup scripts may destroy evidence data
  - Rely on the programs that are installed on the malicious system – always use pre-verified software
  - Contents are irreversibly deleted when the system is turned off

Evidence collection

Memory acquisition

- The one-click memory acquisition tool “Dumpit”
- Two acquisition variants:
  - Interactive
  - Non-interactive

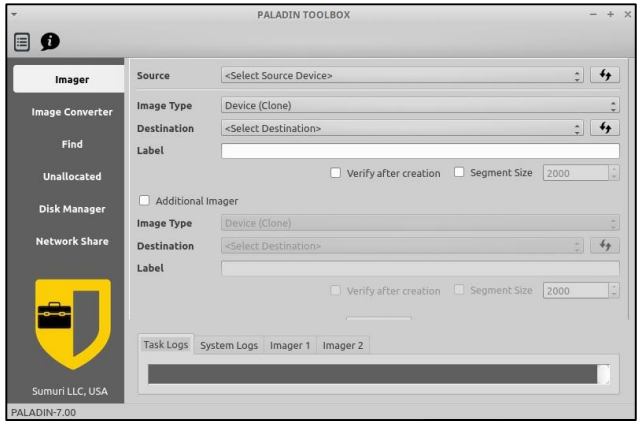
- Dumpit.exe /OUTPUT <output-path> / quiet

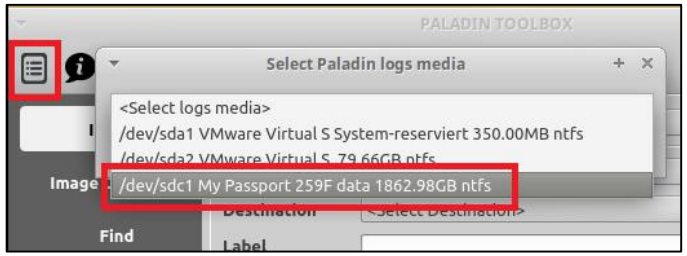
```
E:\Comae-Toolkit-v20221206\x64>DumpIt.exe /O

  DumpIt 3.6.20221203 (X64) (Dec  3 2022)
  Copyright (C) 2007 - 2021, Matt Suiche (msuiche)
  Copyright (C) 2016 - 2021, Comae Technologies DMCC <https://www.comae.com>
  Copyright (c) 2022, Magnet Forensics, Inc. <https://www.magnetforensics.com/>
  All rights reserved.

  Thanks for using DumpIt! Always use Microsoft crash dumps!

    Destination path:           \??\E:\Comae-Toolkit-v20221206\x64\DESKTOP-6T3M3B1-20230113-073303.dmp

    Computer name:              DESKTOP-6T3M3B1


    --> Proceed with the acquisition ? [y/n] y

    [+] Information:
    Dump Type:                   Microsoft Crash Dump


    [+] Machine Information:
    Windows version:             10.0.19044
    MachineId:                   02894D56-A217-1C8D-E917-33B1D0956395
    TimeStamp:                   133180687862556517
    Cr3:                         0x1ad002
    KdCopyDataBlock:             0xfffff8017930de58
    KdDebuggerData:              0xfffff80179a00b20
    KdpDataBlockEncoded:         0xfffff80179a50b00

    Current date/time:           [2023-01-13 (YYYY-MM-DD) 7:33:06 (UTC)]
    + Processing... Done.

    Acquisition finished at:     [2023-01-13 (YYYY-MM-DD) 7:34:23 (UTC)]
    Time elapsed:                1:16 minutes:seconds (76 secs)

    Created file size:           8588750848 bytes (8190 Mb)
    Total physical memory size:  8190 Mb

    NtStatus (troubleshooting):   0x00000000
    Total of written pages:       2096861
    Total of inacessible pages:          0
    Total of accessible pages:    2096861

    SHA-256: F6AD246743ED1C3942138F45093CD329EFEDD3FA21B402F16E2E2F3DB5F019F8

    JSON path:                   E:\Comae-Toolkit-v20221206\x64\DESKTOP-6T3M3B1-20230113-073303.json
```

Evidence collection

Disk acquisition using the Linux forensic live CD “Paladin”

- Live Linux distribution (https://sumuri.com/product/paladin-edge-64-bit/)
- Toolbox with:
  - Imager (over the network or second image)
  - Converting images
  - Triage collection via MIME-type
  - Disk Manager





Evidence Collection

Triage Data

Evidence collection

The **triage** data collection

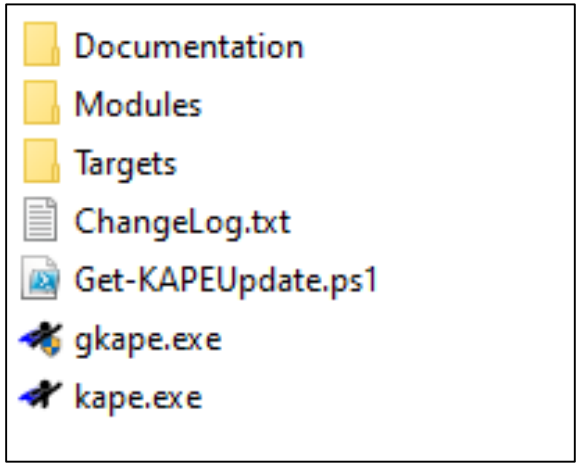
- Origin from military medicine
  - Method for prioritizing medical assistance
  - With insufficient resources
- Using in term of information technology
  - Triage evidence collection
  - Triage evidence analysis
  - Used to answer the initial question
  - Conducted on a live system
  - Conducted over an image

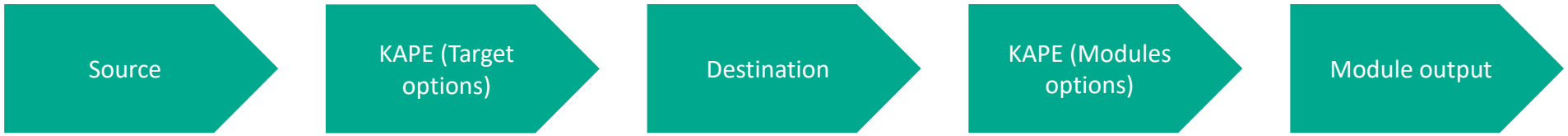
Which artifacts would you collect?

Evidence collection

Triage collection with KAPE

- Kroll Artefact Parser and Extractor (KAPE)
- Triage collection and timeline analysis tool
- Based on targets and modules files
- GUI, command line, portable
- Provides detailed copy log
- Transfer evidence data to another location
- The approach:





https://www.kroll.com/en/services/cyber-risk/investigate-and-respond

Evidence collection

Triage collection with Velociraptor

- Command line:

```
PS C:\Forensics_Tools> .\velociraptor-v0.6.7-4-windows-amd64.exe artifacts collect -v Windows.KapeFiles.Targets --output Output_Triage_Files.zip   --args _BasicCollection=Y --args VSSAnalysis=Y --args KapeTriage
=Y --args WebBrowsers=Y
[INFO] 2023-02-06T13:13:54Z
[INFO] 2023-02-06T13:13:54Z
[INFO] 2023-02-06T13:13:54Z
[INFO] 2023-02-06T13:13:54Z
[INFO] 2023-02-06T13:13:54Z
[INFO] 2023-02-06T13:13:54Z
[INFO] 2023-02-06T13:13:54Z Digging deeper!                https://www.velocidex.com
[INFO] 2023-02-06T13:13:54Z This is Velociraptor 0.6.7-4 built on 2022-12-06T13:31:56Z (c6f11a7)
[INFO] 2023-02-06T13:13:54Z No embedded config - you can pack one with the `config repack` command
[INFO] 2023-02-06T13:13:54Z Env var VELOCIRAPTOR_CONFIG is not set
[INFO] 2023-02-06T13:13:54Z Setting empty config
[INFO] 2023-02-06T13:13:54Z Starting Org Manager service.
[INFO] 2023-02-06T13:13:54Z Starting services for Root Org
[INFO] 2023-02-06T13:13:54Z Starting Journal service for Root Org.
[INFO] 2023-02-06T13:13:54Z Starting the notification service for Root Org.
[INFO] 2023-02-06T13:13:54Z Starting repository manager for Root Org
[INFO] 2023-02-06T13:13:54Z Loaded 347 built in artifacts in 153.8474ms
[INFO] 2023-02-06T13:13:54Z Installing Dummy inventory_service. Will download tools to temp directory.
[INFO] 2023-02-06T13:13:54Z Setting compression level to 5
[INFO] 2023-02-06T13:13:54Z Will create container at Output_Triage_Files.zip
[INFO] 2023-02-06T13:13:54Z Selecting _BasicCollection
[INFO] 2023-02-06T13:13:54Z Selecting KapeTriage
[INFO] 2023-02-06T13:13:55Z Selecting WebBrowsers
[INFO] 2023-02-06T13:13:55Z ntfs: Selecting glob Program Files*\Bitdefender*\**10\regex:*.+\.(db|db-wal|db-shm)
[INFO] 2023-02-06T13:13:55Z ntfs: Selecting glob $Boot
[INFO] 2023-02-06T13:13:55Z ntfs: Selecting glob $Extend\$UsnJrnl:$J
[INFO] 2023-02-06T13:13:55Z ntfs: Selecting glob $Extend\$UsnJrnl:$Max
[INFO] 2023-02-06T13:13:55Z ntfs: Selecting glob $Extend\$J
[INFO] 2023-02-06T13:13:55Z ntfs: Selecting glob $Extend\$Max
[INFO] 2023-02-06T13:13:55Z ntfs: Selecting glob $LogFile
```

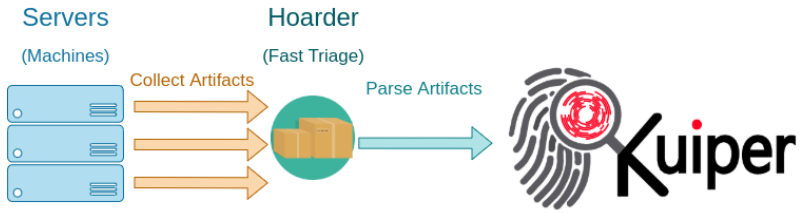
- Parameter
  - **artifacts collect** : collects artifacts data interactively
  - **--output**: name of the resulted data
  - **--args :** tells which data to be collected

Evidence collection

Other useful artifacts collection & parsers tools

- EricZimmerman Tools
  https://ericzimmerman.github.io/

- Hoarder & Kuiper
  https://github.com/muteb/Hoarder
  https://github.com/DFIRKuiper/Kuiper



- TAP-iR
  https://tap-ir.github.io/#/

- Fennec (Linux / OSX)
  https://github.com/AbdulRhmanAlfaifi/Fennec

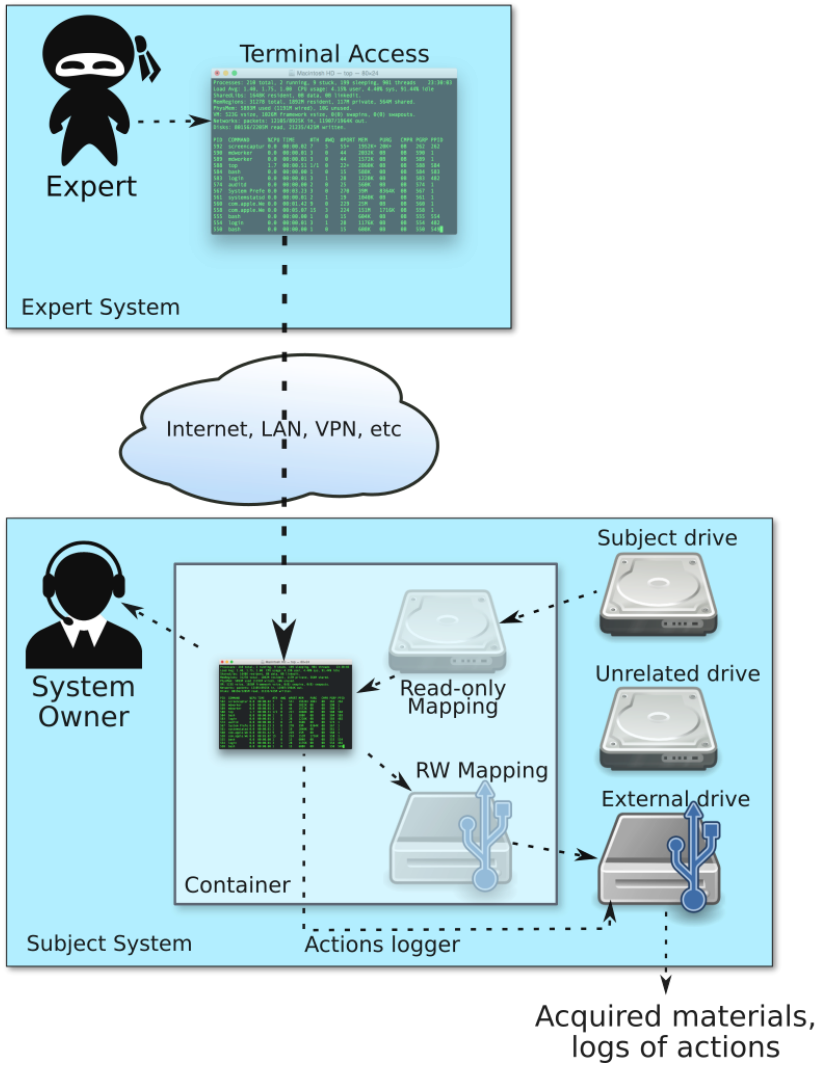
- TimeSketch
  https://github.com/google/timesketch

Remote Evidence Collection

Biscout

- A swiss-army knife for the remote forensic investigation of live systems and has been made freely available for all to use.
- Can remotely collect key forensic materials, acquire full disk images via the network or locally attached storage, or simply remotely assist in malware incident handling.

https://github.com/KasperskyLab/bitscout



https://bitscout-forensics.info/

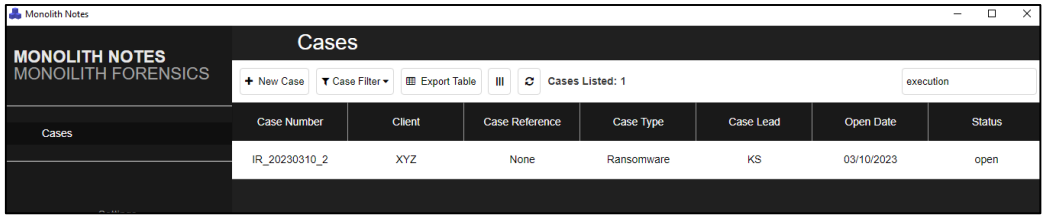
Documentation & Case Management

Documentation is to incident response as navigation with tools

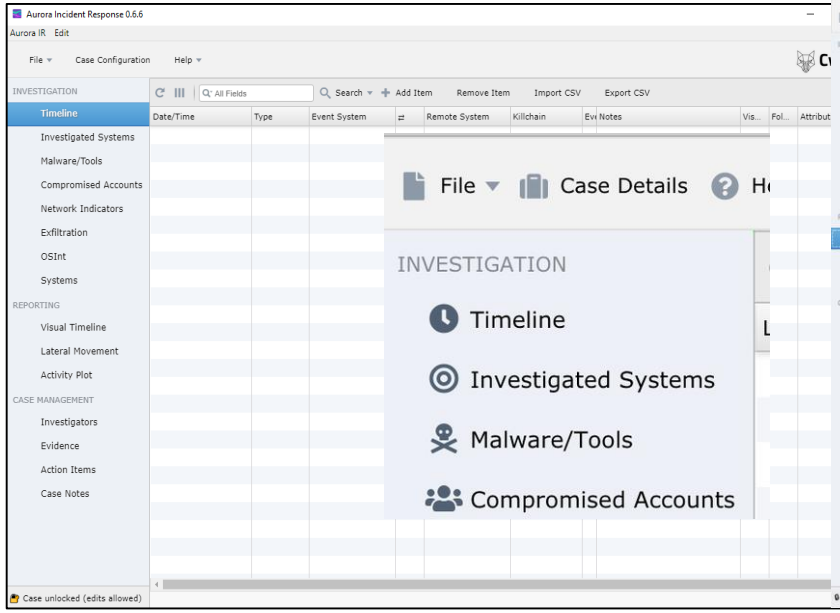
- During IR you will be flooded with information
- Would you remember all of the information and your work activities?
  - Which system was already investigated by whom?
  - What malicious artifacts have been found?
  - What was the IP of this server again?
  - Where is the hard drive of the system x again?
  - Etc.
- Handover of team activities
- Audience
- Etc.

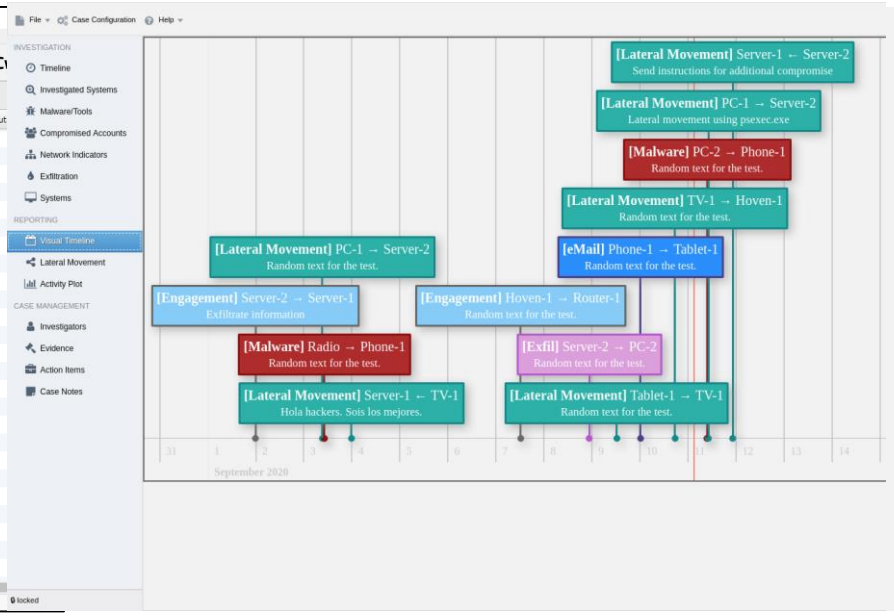
Documentation – supporting tools

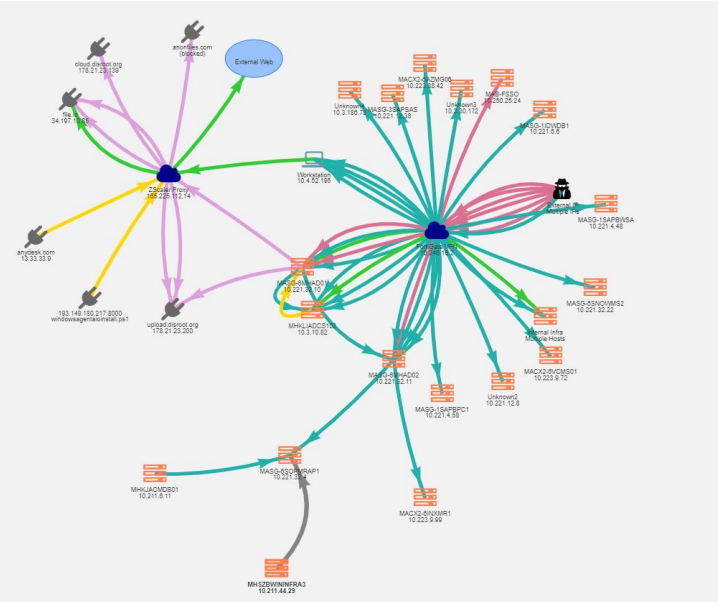
- Just notes (https://monolithforensics.com/free-tools)



- Aurora Incident Response (https://github.com/cyb3rfox/Aurora-Incident-Response)

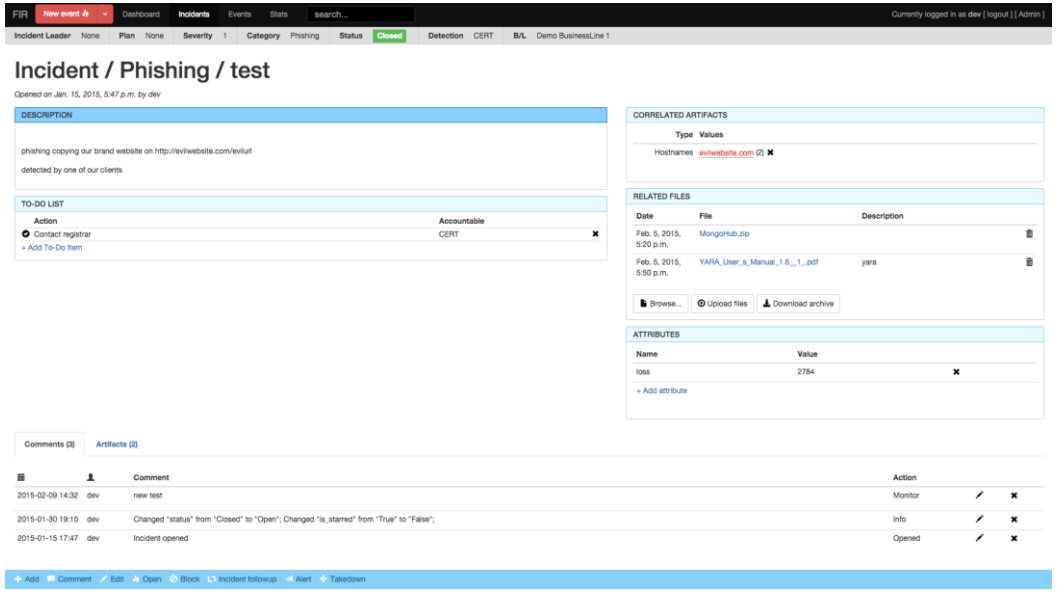


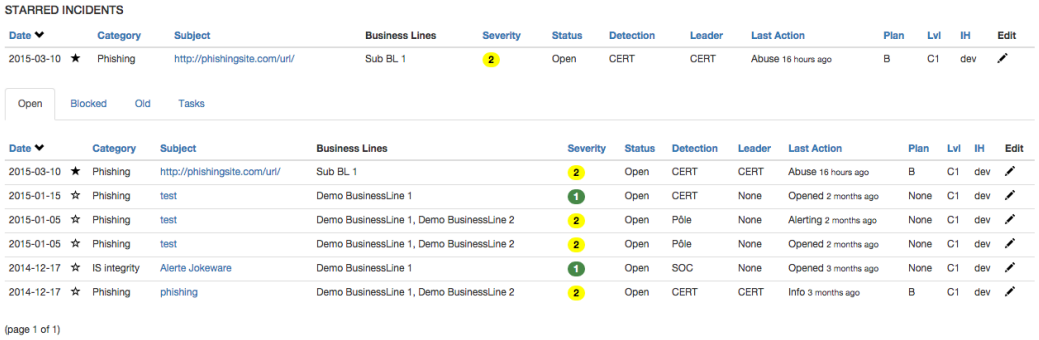




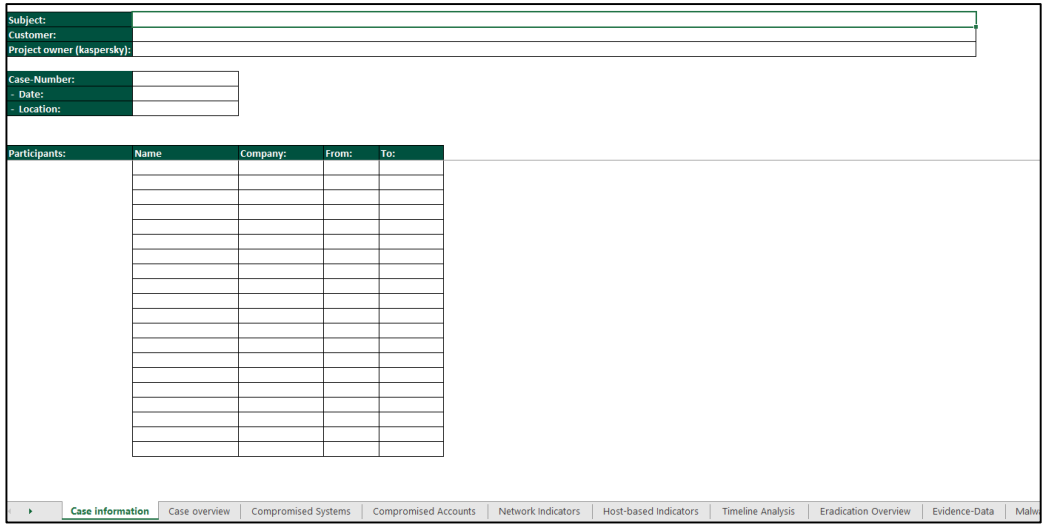
Documentation – supporting tools

- FIR - Fast Incident Response (https://github.com/certsocietegenerale/FIR/)





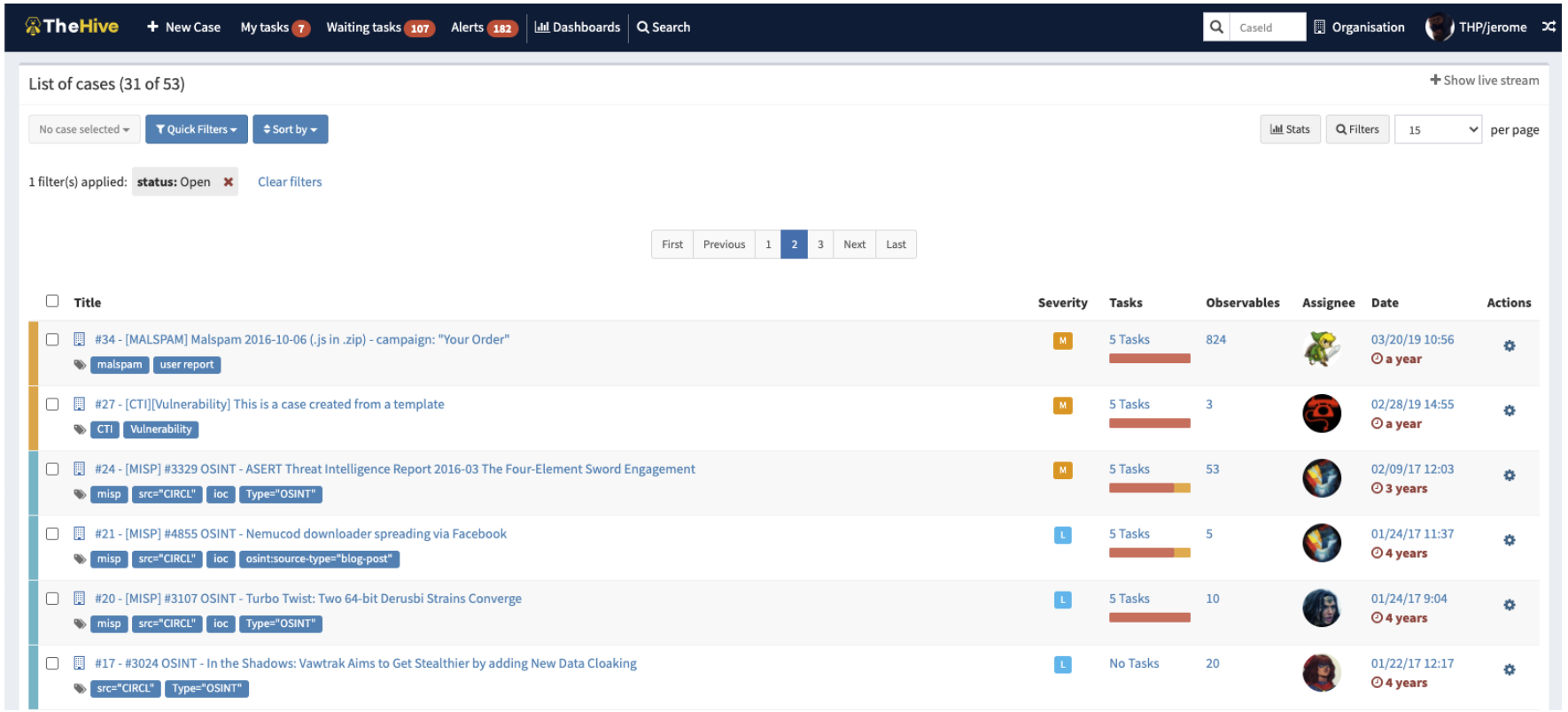
- Or the good old one…



Documentation – Case Management

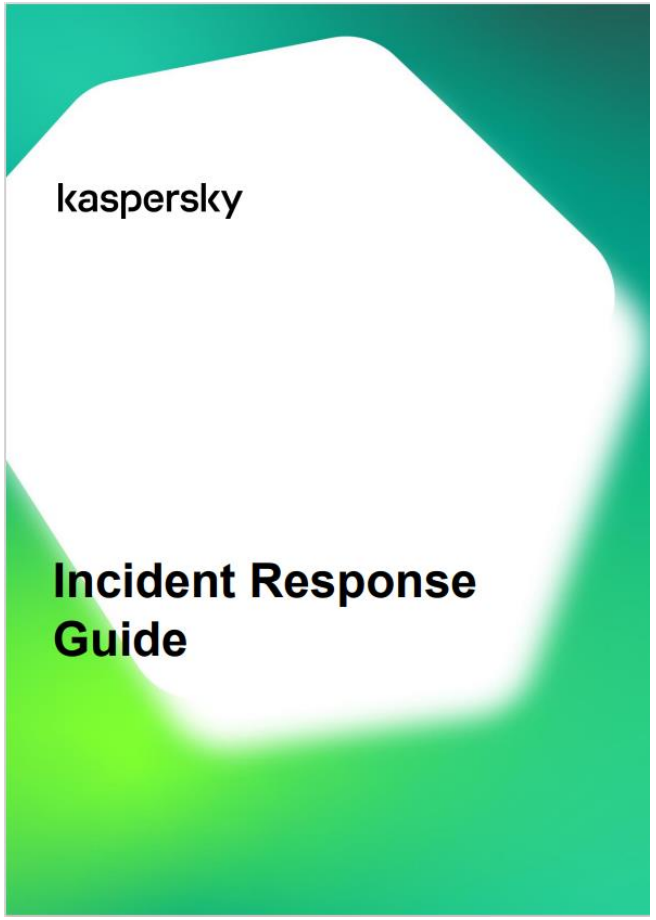
The Hive Project (TheHive + Cortex) + MISP

- Scalable 3-in-1 open source and free Security Incident Response Platform designed for SOCs, CSIRTs, CERTs



https://github.com/TheHive-Project

Kaspersky Incident Response Guide



This guide provides basic explanations and recommendations for responding to information security incidents.

This guide aims to do the following:

- Systematize information about the attack lifecycle and actions involved in the incident response (IR)
- process.
- Provide a recommended sequence of actions for IR.
- Describe a range of tools and utilities that can be used at every phase of the IR process.
- Provide information about IR best practices.

Download:

https://securelist.com/neutralization-reaction/81620/

Q & A

Salman Shaikh
Senior Security Researcher -
Kaspersky Labs ICS CERT

Ahmad Zaidi Said
Incident Response Specialist (DFIR), Kaspersky GERT

Want to know more about Kaspersky Expert Services?
services@kaspersky.com