

Effective DFIR Investigation With Limited Resources For IT/OT

Ahmad Zaidi & Salman Shaikh

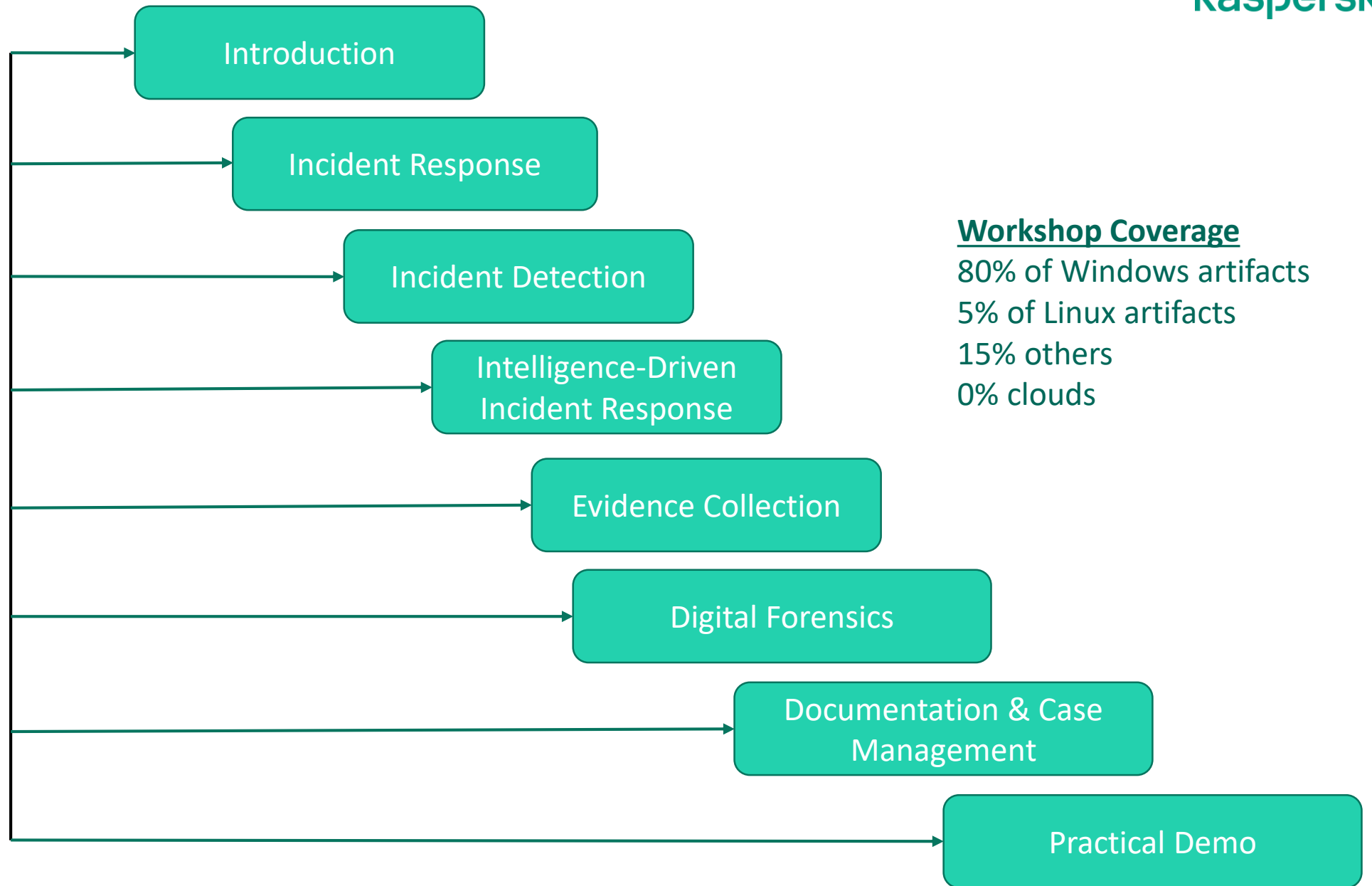
21/09/2023

Port Vila, Vanuatu



AGENDA

EFFECTIVE DFIR INVESTIGATION



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)

EUROPE

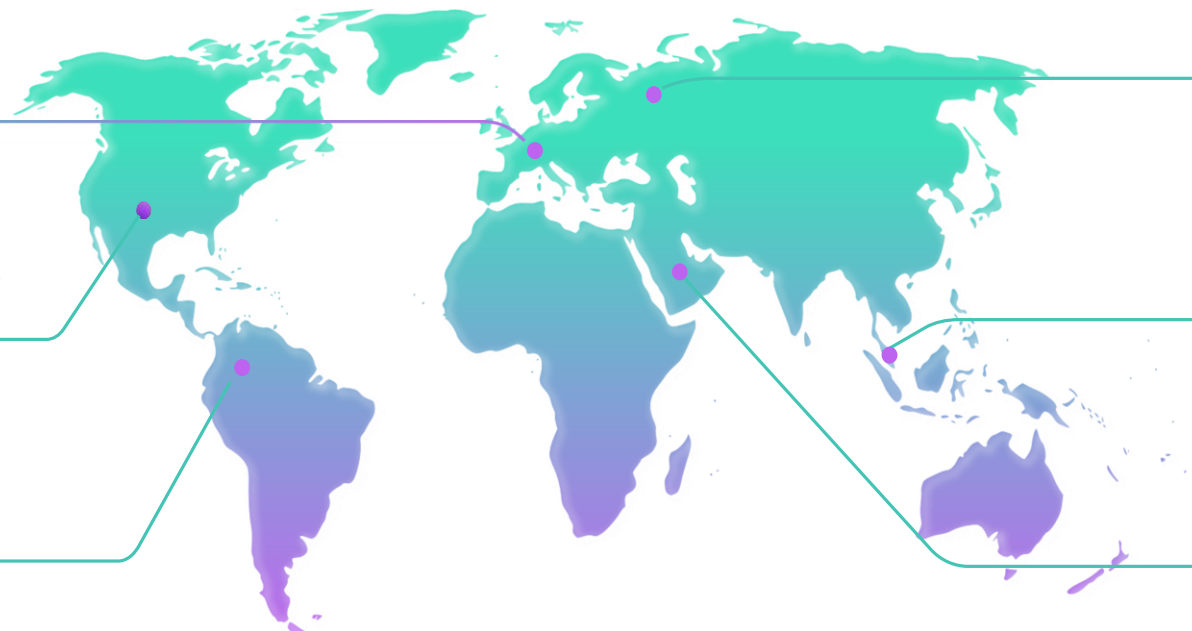
Germany
France
Italy

NORTH AMERICA

USA

LATAM

Columbia
Brazil
Mexico



Head
Quarter

APAC
Malaysia

META
KSA
UAE
Egypt

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



PECB ISO/IEC 27035
SERVING LEGAL INCIDENT MANAGERS

CCSK

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

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



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





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:

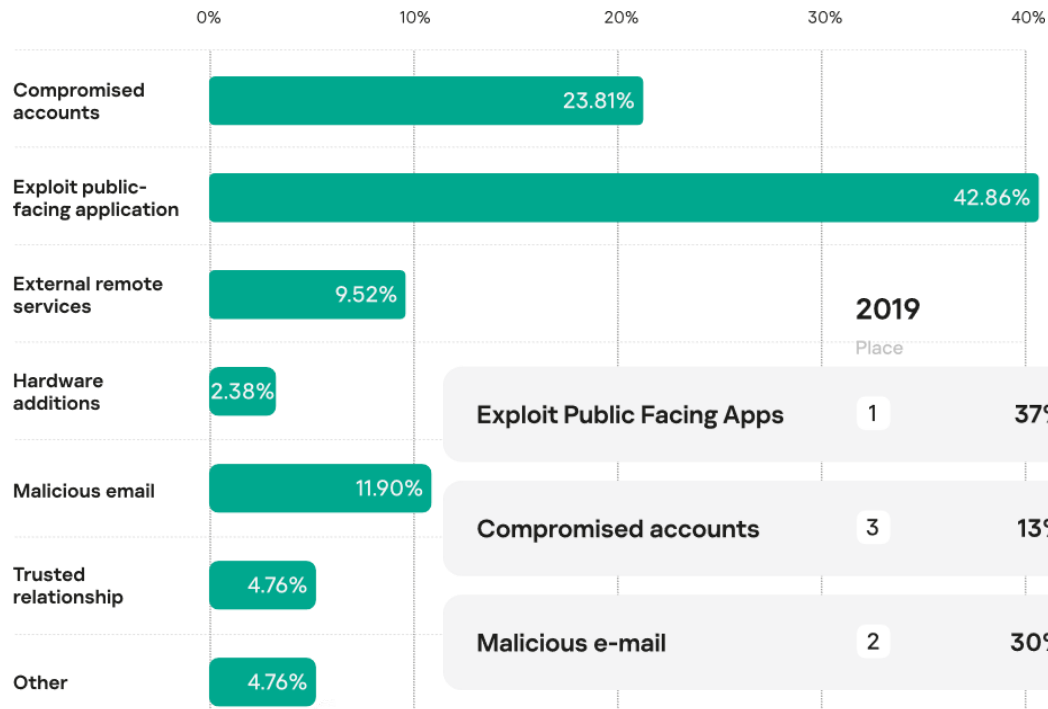
- Develop industrial cybersecurity methodologies, frameworks, and standards -
- Consult industrial organizations on industrial cybersecurity issues -
- Help developers make their products more secure -

[Visit ICS CERT website](#)

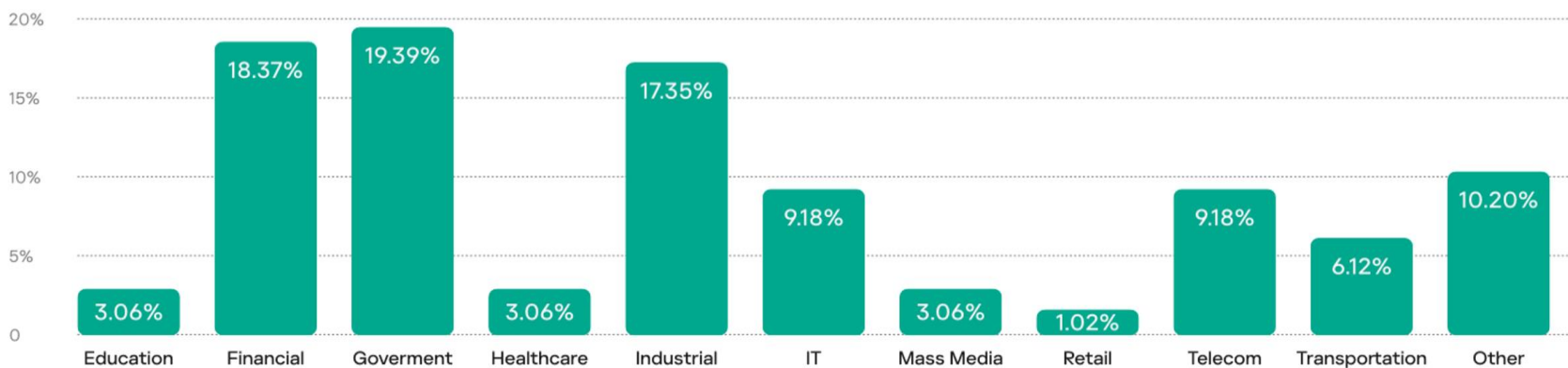
[Contact us](#)

[Read RFC-2350 document](#)

Not If, but when?



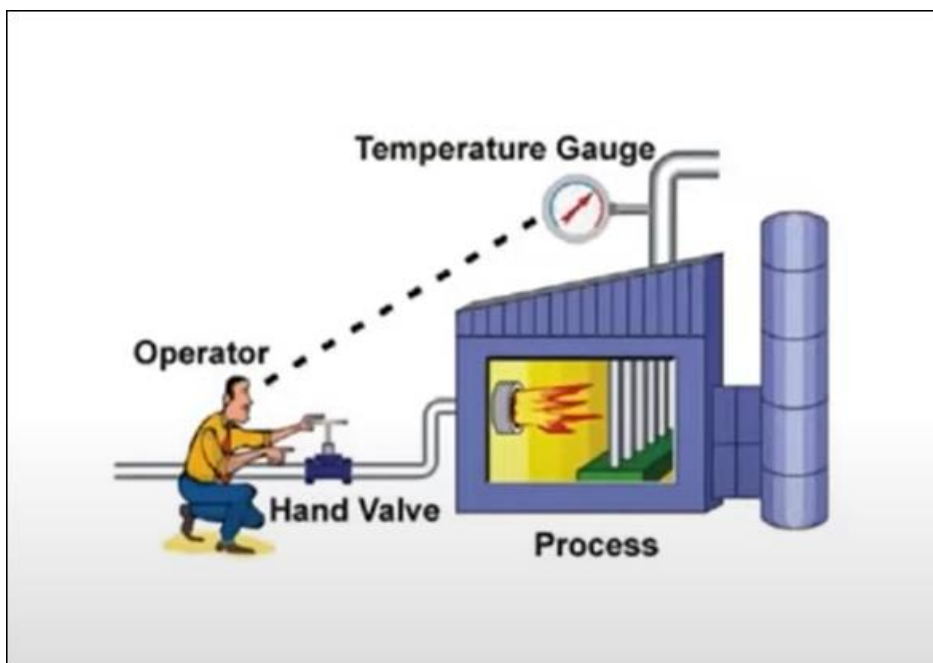
	2019		2020		2021		2022	
	Place	%	Place	%	Place	%	Place	%
Exploit Public Facing Apps	1	37%	2	31.5%	1	53.6%	1	42.9%
Compromised accounts	3	13%	1	31.6%	2	17.9%	2	23.8%
Malicious e-mail	2	30%	3	23.7%	3	14.3%	3	11.9%



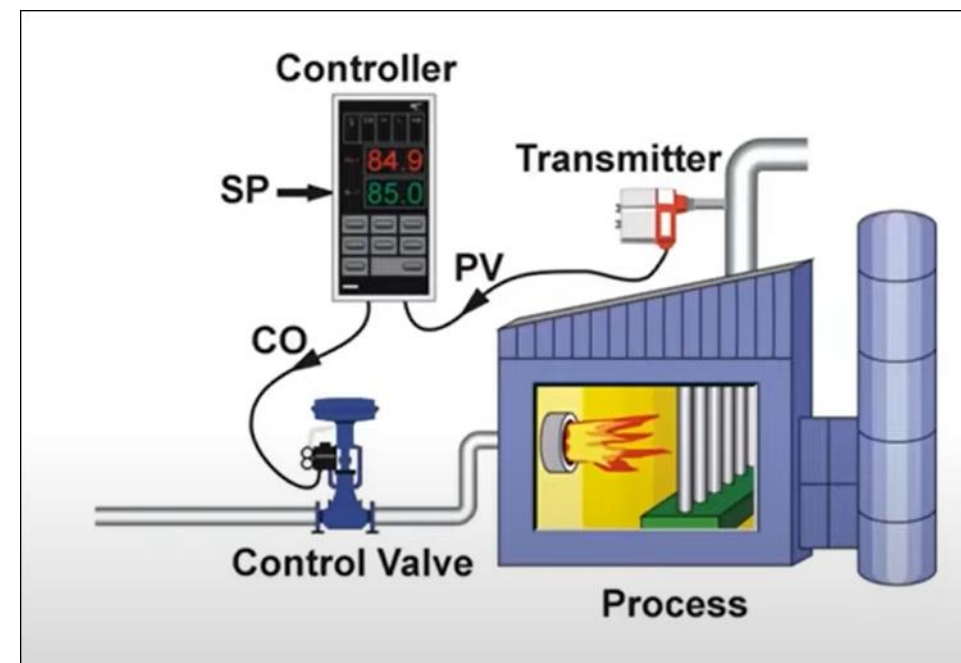


Why is there an increase in attacks on Industrial organization ?

Manual Operations



Automation





Why an attack on Industrial Organization is more devastating?





IT vs OT / ICS Cyber Security Differences

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



CIA VS SRP TRIAD

Safety

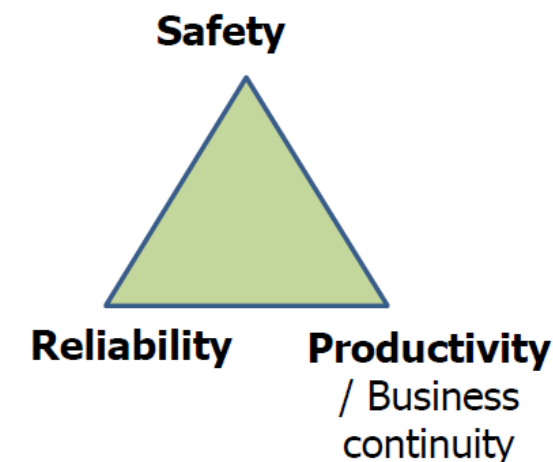
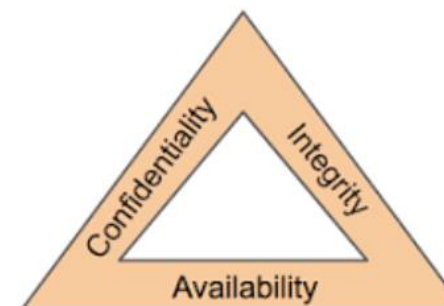
- The most important consideration for ICS
 - The machinery must not hurt people
 - The people can not cause a safety risk
- When an incident happens
 - The system must go to fail-safe

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





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.?





TO DO LIST difference with ICS systems

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

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

- 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





Incident Response (IR) Management

IR team



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

An attacker



- To reach the malicious goal

An organization victim



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

Everyone has different goals and priorities

Facility Management & OT Specialist



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



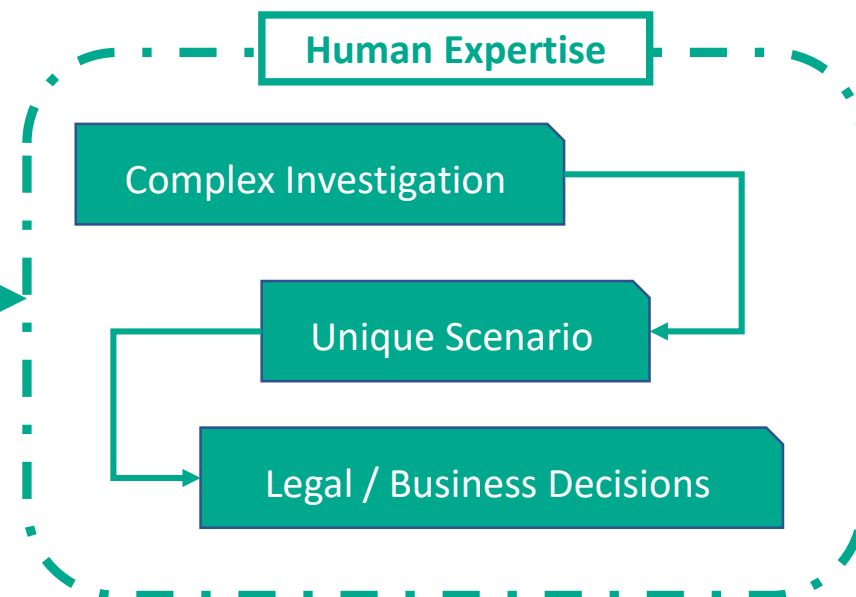
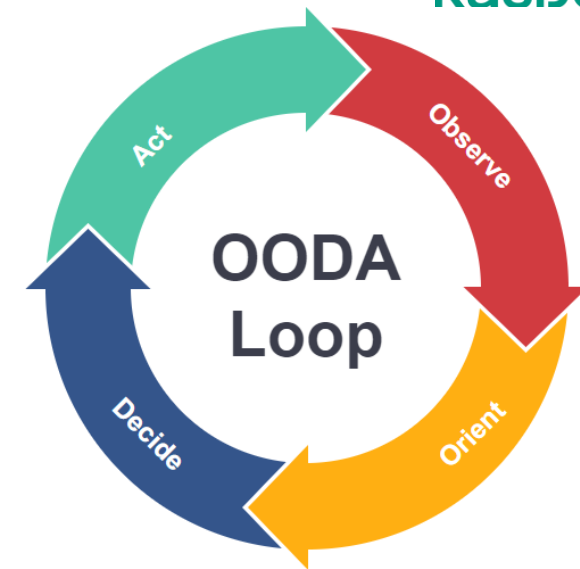
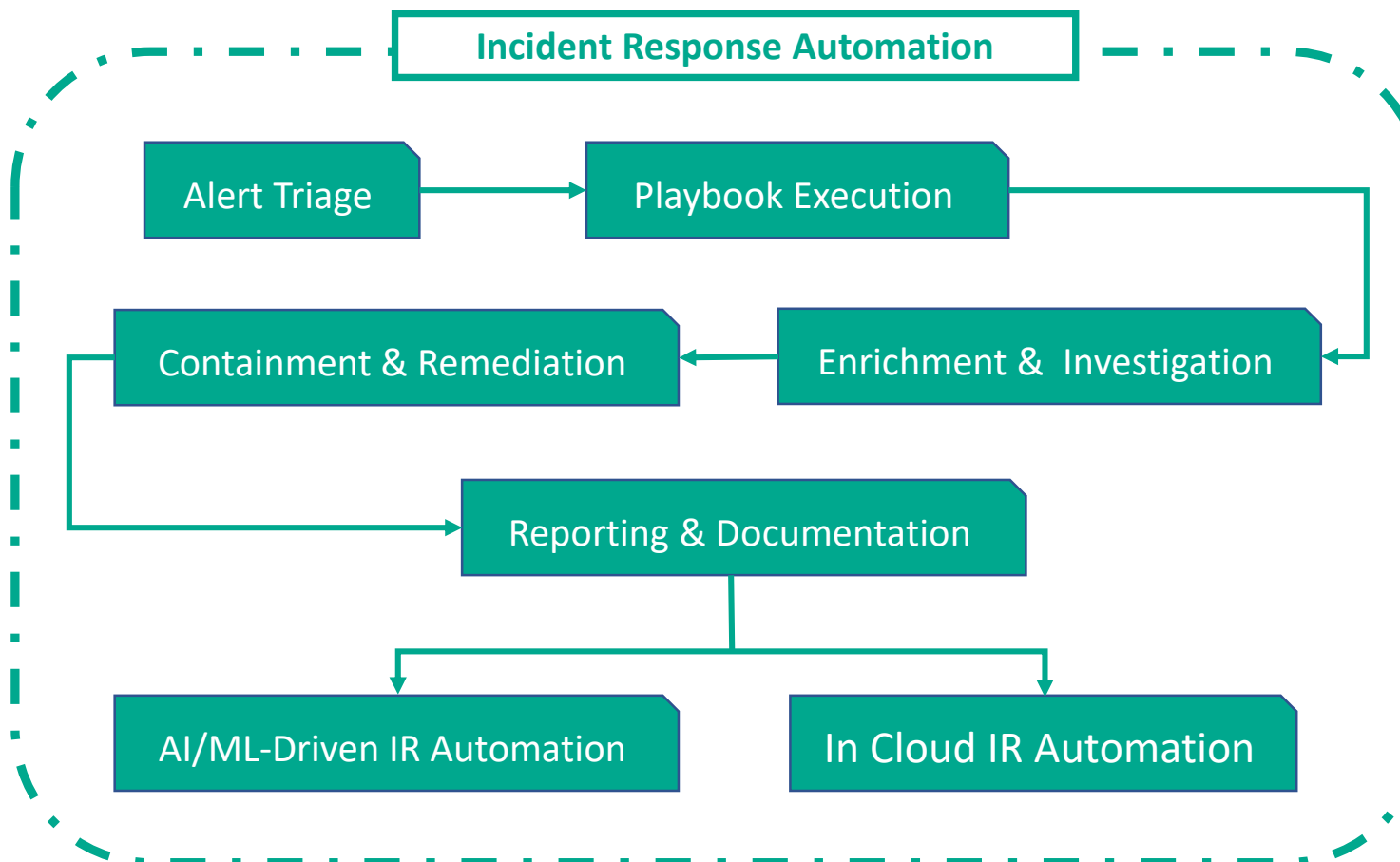
Key People in Cyber Crisis Management

- 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**



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 across 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





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

SANS DFIR
DIGITAL FORENSICS INCIDENT RESPONSE
Windows Forensic Analysis POSTER
Master Windows Forensics - You Can't Protect the Unknown
digital-forensics.sans.org

SANS Windows Artifact Analysis: Evidence of...

Application Execution

File and Folder Opening

Deleted Items and File Existence

SANS DFIR CURRICULUM

Disk image analysis

AccessData FTK Imager 3.14.6

Evidence Tree Pane

File List Pane

Viewer Pane

Hex Value Interpreter

Memory image analysis

```
C:\Users\haider\Downloads\volatility>volatility.exe -f H-HP-20121209-120703.raw --profile=Win7SP1x64 pslist
Volatility Systems Volatility Framework 2.1
Offset(K) Name PID PPID Thds Hnds Sess Wou64 Start Exit
0xfffffa8003606740 System 4 0 170 3839 0 0 2012-12-07 11:42:15
0xfffffa8006939b30 smss.exe 440 4 2 32 0 0 2012-12-07 11:42:15
0xfffffa8007581b30 csrss.exe 564 544 11 929 0 0 2012-12-07 11:42:21
0xfffffa8007816b30 wininit.exe 760 544 3 76 0 0 2012-12-07 11:42:24
0xfffffa800781ab30 csrss.exe 780 760 13 849 1 0 2012-12-07 11:42:24
0xfffffa8007839b30 services.exe 824 760 9 311 0 0 2012-12-07 11:42:24
0xfffffa8008162b30 lsass.exe 840 760 8 825 0 0 2012-12-07 11:42:24
0xfffffa80081891e0 lsass.exe 848 760 10 204 0 0 2012-12-07 11:42:24
0xfffffa800816ab30 winlogon.exe 900 760 3 117 1 0 2012-12-07 11:42:24
0xfffffa800820e060 smss.exe 984 824 11 415 0 0 2012-12-07 11:42:25
0xfffffa8008249860 svchost.exe 484 824 9 425 0 0 2012-12-07 11:42:25
0xfffffa800824c30 atiesxxx.exe 648 824 6 118 0 0 2012-12-07 11:42:25
0xfffffa8008358750 svchost.exe 784 824 21 643 0 0 2012-12-07 11:42:25
0xfffffa80083f9350 svchost.exe 1000 824 10 542 0 0 2012-12-07 11:42:26
0xfffffa80083ff8a0 svchost.exe 1040 824 43 1695 0 0 2012-12-07 11:42:26
0xfffffa800839b580 stacsv64.exe 1124 824 10 325 0 0 2012-12-07 11:42:27
0xfffffa800849c30 svchost.exe 1320 824 10 597 0 0 2012-12-07 11:42:27
0xfffffa8008500860 hpservice.exe 1432 824 4 76 0 0 2012-12-07 11:42:29
0xfffffa8008537b30 svchost.exe 1480 824 13 449 0 0 2012-12-07 11:42:30
0xfffffa80085a03b0 atieclxx.exe 1580 640 12 320 1 0 2012-12-07 11:42:31
0xfffffa80085d6b30 spoolsv.exe 1644 824 12 319 0 0 2012-12-07 11:42:31
0xfffffa800864a500 svchost.exe 1672 824 16 361 0 0 2012-12-07 11:42:31
0xfffffa800872e060 svchost.exe 1872 824 21 389 0 0 2012-12-07 11:42:32
0xfffffa8008755630 AESTS64.exe 1940 824 5 45 0 0 2012-12-07 11:42:33
0xfffffa8008759b30 ahp.exe 1968 824 113 2963 0 1 2012-12-07 11:42:33
0xfffffa800883db30 devmgmt.exe 1996 824 13 257 0 0 2012-12-07 11:42:33
0xfffffa800883b30 esSharedSvcHost 1072 824 6 86 0 1 2012-12-07 11:42:33
0xfffffa800891e630 svchost.exe 1404 824 8 224 1 0 2012-12-07 11:42:35
0xfffffa80089a4b30 dm.exe 2092 1000 5 137 1 0 2012-12-07 11:42:35
0xfffffa80089b4930 explorer.exe 2148 1420 37 1236 1 0 2012-12-07 11:42:35
0xfffffa80089ceb30 HPUMISUC.exe 2192 824 4 117 0 1 2012-12-07 11:42:35
0xfffffa80089f0660 taskeng.exe 2216 1940 5 110 1 0 2012-12-07 11:42:35
0xfffffa8008a12b30 LSASvc.exe 2252 824 5 75 0 1 2012-12-07 11:42:35
0xfffffa8008a1b060 svchost.exe 2432 824 7 107 0 0 2012-12-07 11:42:36
```



Differences between forensic and ICS forensic

PLC

Object Name	Symbolic Name	Created in	Size in the w	Type	Last interface change	DB write-prot	Last modified	Monitoring
System data				SDB			06/26/2017 11:27:36 PM	
FC1	STL	03/29/2017 04:44:58 PM	38	Function	0.1		03/29/2017 11:27:36 PM	
FC2	STL	03/29/2017 04:44:58 PM	38	Function	0.1		03/29/2017 04:44:58 PM	
FC3	STL	03/29/2017 04:59:48 PM	38	Function	0.1		03/29/2017 04:59:48 PM	
DB1	DB	03/31/2017 01:33:43 PM	38	Data Block	0.1		03/31/2017 01:35:44 PM	

SCADA

Source	Area	Event	Batch name	Operation	Free 1	Free 2	Free 3	Free 4	Free 5	Proc
PCCELLGETMSGCLASSMSG1		MSG1 MSG8 Message text								
PCCELLGETMSGCLASSMSG2		MSG2 MSG8 MessageText								
PCCELLUNIT14_E003SIMOREV		Prewarning overload								
PCCELL620/MOTOR		feedback								
PCCELL1630/VALVE		feedback								
PCCELL1640/ANALOG		lim01								
PCCELL1660/DIGITAL		L5+ 650 overful								
PCCELL620_LOCK/LOCK										
PCCELLUNIT14_V001/VALVE_IL		feedback								
PCCELLUNIT13_V102/VALVE		feedback								
PCCELLUNIT14_V201/VALVE		feedback								
PCCELLUNIT13_V102/VALVE_IL		feedback								
PCCELLUNIT13_E104/MOTOR		feedback								
PCCELLUNIT13_E104/MOTOR_LOCK		feedback								
PCCELLUNIT14_E004/MOTOR		feedback								
PCCELLUNIT14_E004/MOTOR_LOCK		feedback								
PCCELLUNIT13_L1120/ANALOG		lim01								
PCCELLUNIT14_L1220/ANALOG		lim01								
PCCELLUNIT13_F1140/ANALOG		lim01								
PCCELLUNIT14_F1240/ANALOG		lim01								
PCCELLUNIT13_L1300/DIGITAL		L5+ 650 overful								
PCCELLUNIT14_L1230/DIGITAL		L5+ 650 overful								
PCCELLUNIT13_V109/VALVE		feedback								
PCCELLUNIT13_V109/VALVE_IL		feedback								
PCCELLUNIT13_L1120/ANALOG_SIM										
PCCELLUNIT13_L1120/ANALOG_SIM_INT1										
PCCELLUNIT13_V101/VALVE		feedback								

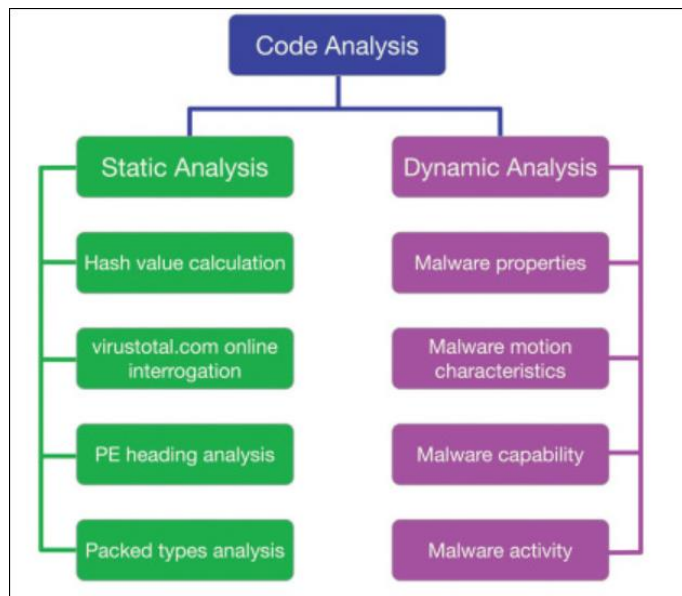
Historian Server

OPC

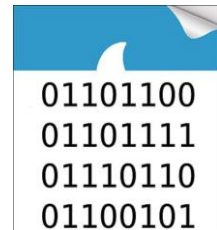
Date	Time	Position	Temperature	Quantity	Fault Code	Part Number	Running	Fault Flag
4/26/2006	50:27.9	53.22	70.81	24	9	P764A	0	1
4/26/2006	50:32.9	53.38	74.55	24	9	P764A	0	1
4/26/2006	50:37.9	56.44	77.54	24	9	P764A	0	1
4/26/2006	50:42.9	57.62	77.89	24	9	P764A	0	1
4/26/2006	50:47.9	56.66	79.34	24	9	P764A	0	1
4/26/2006	50:52.9	57.82	82.33	24	9	P764A	0	1
4/26/2006	50:57.9	61.24	83.41	24	9	P764A	0	1
4/26/2006	51:02.9	65.25	89.88	24	9	P764A	0	1
4/26/2006	51:08.0	66.7	89.7	24	9	P764A	0	1
4/26/2006	51:13.0	67.26	90.25	24	9	P764A	0	1

Incident Detection

Malicious File 

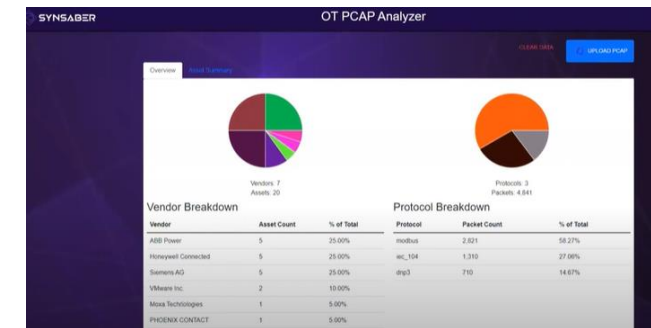
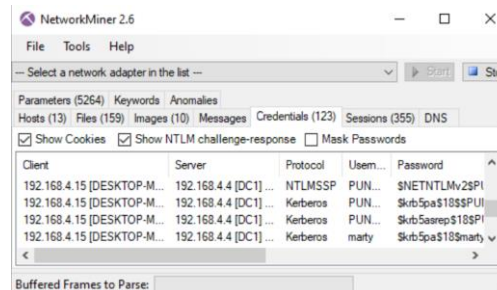


PCAP



```

(ubuntu@linuxopsys)-[~]
└─$ sudo tshark -r capture.pcap -Y "tcp.port == 80"
Running as user "root" and group "root". This could be dangerous.
 5 2.813876528 192.168.246.198 → 93.184.216.34 TCP 66 38236 → 80 [FIN, ACK] Seq=1 Ac
k=1 Win=502 Len=0 TSval=705197085 TSecr=3126651585
 8 2.814131645 192.168.246.198 → 93.184.216.34 HTTP 565 GET / HTTP/1.1
11 3.167539500 93.184.216.34 → 192.168.246.198 HTTP 1094 HTTP/1.1 200 OK (text/html
)
12 3.167583302 192.168.246.198 → 93.184.216.34 TCP 66 38246 → 80 [ACK] Seq=500 Ack=1
029 Win=493 Len=0 TSval=705197439 TSecr=155900373
22 5.874241936 192.168.246.198 → 93.184.216.34 TCP 66 [TCP Retransmission] 38236 → 8
0 [FIN, ACK] Seq=1 Ack=1 Win=502 Len=0 TSval=705200146 TSecr=3126651585
227 8.573998069 192.168.246.198 → 93.184.216.34 HTTP 566 GET / HTTP/1.1
261 8.868378881 93.184.216.34 → 192.168.246.198 HTTP 1093 HTTP/1.1 200 OK (text/html
)
  
```



Incident Detection

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

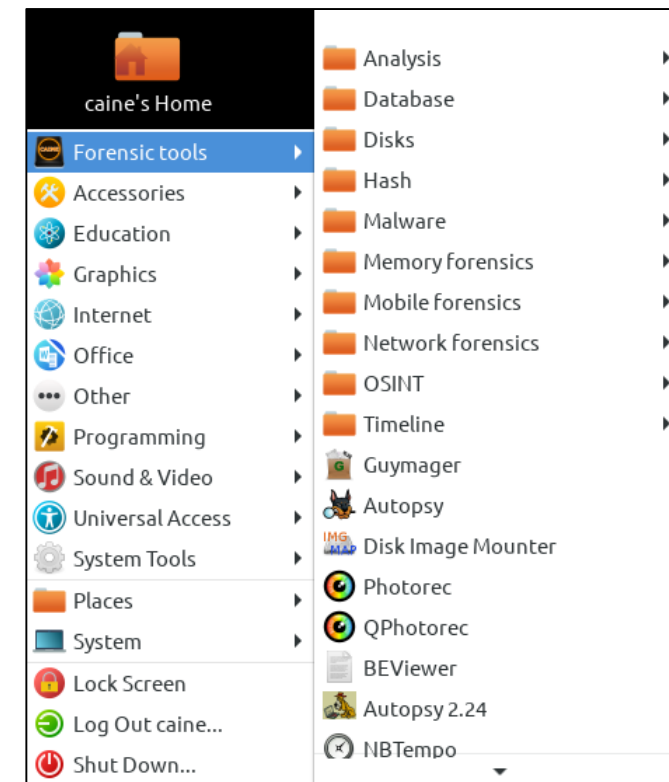
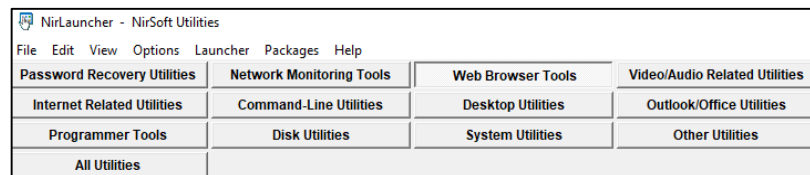
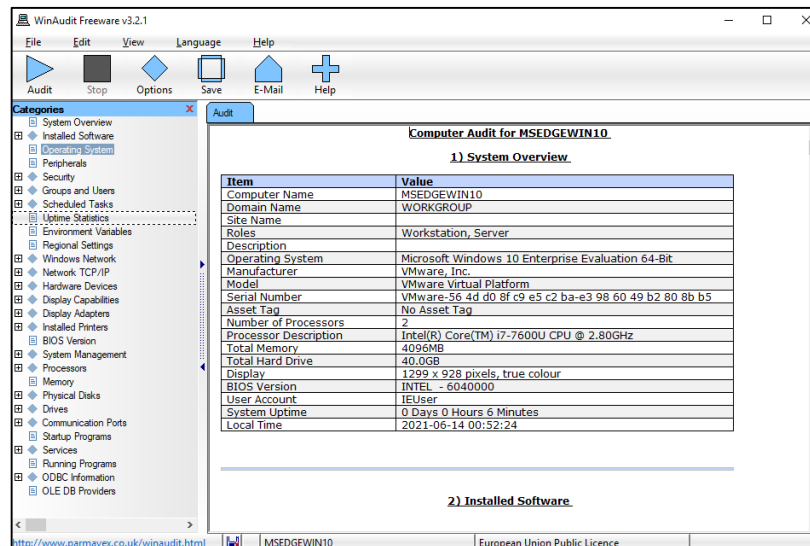
- WMI available starting with Windows ME
- PowerShell available by default since Windows 7
- Used for administrative purposes
- Flexible processing and filtering functions
- Local and remote command and/or script execution
- PowerShell:
 - Integrated scripting environment for script development and debugging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

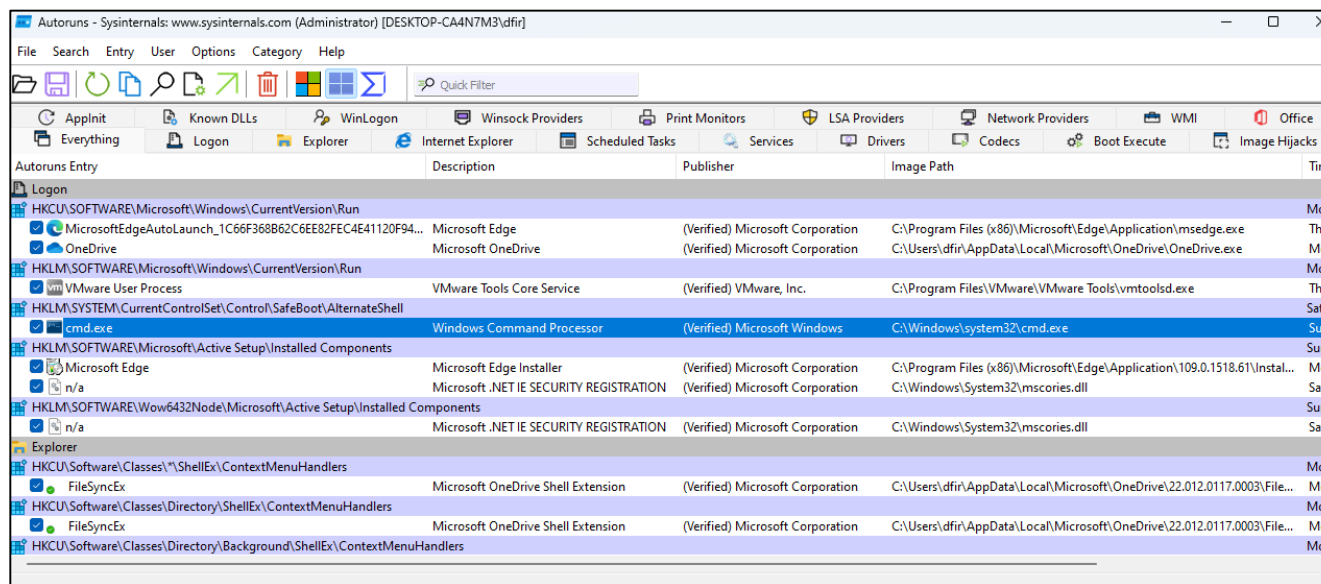
- Displays information about processes and their handles and loaded DLLs
- Color coding
- Detailed information about a process security
- Suspend or dump a process
- Strings of a process
- TCP/IP endpoints
- VT integration
- Etc.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Path	VmsTotal
msedge.exe		7,556 K	17,072 K	4304	Microsoft Edge	Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	0/74
msedgewebview2.exe	< 0.01	30,848 K	91,424 K	3480	Microsoft Edge WebView2	Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\109.0.1518.61\msedge...	0/75
msedgewebview2.exe		2,040 K	7,608 K	7968	Microsoft Edge WebView2	Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\109.0.1518.61\msedge...	0/75
msedgewebview2.exe		23,584 K	49,920 K	4460	Microsoft Edge WebView2	Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\109.0.1518.61\msedge...	0/75
msedgewebview2.exe	< 0.01	12,380 K	31,616 K	6124	Microsoft Edge WebView2	Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\109.0.1518.61\msedge...	0/75
msedgewebview2.exe		7,584 K	17,688 K	7900	Microsoft Edge WebView2	Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\109.0.1518.61\msedge...	0/75
msedgewebview2.exe		59,992 K	103,164 K	4856	Microsoft Edge WebView2	Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\109.0.1518.61\msedge...	0/75
vmacthlp.exe		1,624 K	7,600 K	1936	VMware Activation Helper	VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmacthlp.exe	0/75
vmtoolsd.exe	< 0.01	9,968 K	23,404 K	3428	VMware Tools Core Service	VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	0/72
vmtoolsd.exe	0.34	27,820 K	49,968 K	7844	VMware Tools Core Service	VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	0/72
VGAuthService.exe		4,840 K	14,668 K	3408	VMware Guest Authentication	VMware, Inc.	C:\Program Files\VMware\VMware Tools\VMware VGAuthService.exe	0/71
MsMpEng.exe	< 0.01	169,952 K	146,892 K	3416	Antimalware Service Execut...	Microsoft Corporation	C:\Program Files\Windows Defender\MsMpEng.exe	0/75
NisSrv.exe		4,272 K	11,716 K	4562	Microsoft Network Realtime I...	Microsoft Corporation	C:\Program Files\Windows Defender\NisSrv.exe	0/73
mspaint.exe		30,728 K	79,012 K	7368			C:\Program Files\WindowsApps\Microsoft.Windows.Client.WebExperience_421.200...	0/75
Widgets.exe		7,404 K	37,164 K	6524		Microsoft Corporation	C:\Program Files\WindowsApps\Microsoft.Windows.Client.WebExperience_421.200...	0/75
OneDrive.exe	0.34	14,276 K	58,024 K	8084	Microsoft OneDrive	Microsoft Corporation	C:\Users\dfir\AppData\Local\Microsoft\OneDrive\OneDrive.exe	0/74
process64.exe	3.36	30,132 K	74,764 K	1704	Sysinternals Process Explorer	Sysinternals - www.sysinternals.com	C:\Users\dfir\Desktop\process64.exe	0/75
explorer.exe	< 0.01	88,500 K	216,344 K	6852	Windows Explorer	Microsoft Corporation	C:\Windows\explorer.exe	0/74
dlhost.exe	< 0.01	4,252 K	15,276 K	3144	COM Surrogate	Microsoft Corporation	C:\Windows\System32\dlhost.exe	0/75
dlhost.exe		7,100 K	17,616 K	3332	COM Surrogate	Microsoft Corporation	C:\Windows\System32\dlhost.exe	0/75
dlhost.exe		2,808 K	15,836 K	4712	COM Surrogate	Microsoft Corporation	C:\Windows\System32\dlhost.exe	0/75
lsass.exe		6,472 K	19,952 K	856	Local Security Authority Proc...	Microsoft Corporation	C:\Windows\System32\lsass.exe	0/75
msactx.exe	0.34	3,176 K	11,464 K	1232	Microsoft Distributed Transa...	Microsoft Corporation	C:\Windows\System32\msactx.exe	0/75
RuntimeBroker.exe		4,508 K	25,256 K	6732	Runtime Broker	Microsoft Corporation	C:\Windows\System32\RuntimeBroker.exe	0/75
RuntimeBroker.exe		14,704 K	48,096 K	6852	Runtime Broker	Microsoft Corporation	C:\Windows\System32\RuntimeBroker.exe	0/75
RuntimeBroker.exe		2,000 K	8,312 K	4176	Runtime Broker	Microsoft Corporation	C:\Windows\System32\RuntimeBroker.exe	0/75

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)

Dashboard / Windows_Sysinternals_Autoruns

Search... (e.g. status:200 AND extension:PHP)

Add a filter +

win_sysinternals_autoruns_in... **318** Count

win_sysinternals_autoruns_counts

win_sysinternals_autoruns_hostname...

hostname.keyword: Descending	Count
DESKTOP-ET1AL8B	113
DESKTOP-ET1AL9H	109
JHSRV01	52
DCSRV01	44

win_sysinternals_autoruns_profile (100)

Profile.keyword: Descending	Count
System-wide	284
DESKTOP-ET1AL9H\cerberos	14
CERBEROS\adm_cerberos	6

win_sysinternals_autoruns_entrylocation (100)

EntryLocation.keyword: Descending

- HKLM\System\CurrentControlSet\Services
- HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
- Task Scheduler
- HKCU\Software\Microsoft\Internet Explorer\LowSearch\Hooks
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Font Drivers
- HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order
- HKLM\Software\Classes*\ShellEx\ContextMenuHandlers

win_sysinternals_autoruns_entry (100)

Entry	Count
DEI_ST_CPL	1
Dolby DAX2 API Service	1
Entry	4
Google Chrome	2
Google Update	1
GoogleChromeElevationService	2

win_sysinternals_autoruns_search_common

Time	EntryLocation	LaunchString	Entry	ImagePath
January 27th 2020, 14:50:52.000	HKLM\System\CurrentControlSet\Services	system32\DRIVERS\kigse.sys	kigse	c:\windows\system32\drivers\kigse.sys
January 27th 2020, 14:50:52.000	HKLM\System\CurrentControlSet\Services	system32\DRIVERS\kigse.sys	kigse	c:\windows\system32\drivers\kigse.sys
January 26th 2020, 20:51:54.000	HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors	-	-	-
January 25th 2020, 15:51:12.000	HKLM\System\CurrentControlSet\Services	\77C:\ProgramData\Kaspersky Lab\AVP20.0\Bases\klds.sys	klds	c:\programdata\kaspersky lab\avp20.0\bases\klds.sys

Dashboard / Windows_Sysinternals_Autoruns

Search... (e.g. status:200 AND extension:PHP)

Entry keyword: "Google Update" Add a filter +

win_sysinternals_autoruns_in... **1** Count

win_sysinternals_autoruns_counts

win_sysinternals_autoruns_hostname...

hostname.keyword: Descending	Count
JHSRV01	1

win_sysinternals_autoruns_profile...

Profile.keyword: Descending	Count
System-wide	1

win_sysinternals_autoruns_launchstrings (100)

LaunchString.keyword: Descending

LaunchString	Count
C:\temp\googleupdate.exe	1

win_sysinternals_autoruns_entrylocation (100)

EntryLocation.keyword: Descending

EntryLocation	Count
HKLM\System\CurrentControlSet\Services	1

win_sysinternals_autoruns_tags

JHSRV01

win_sysinternals_autoruns_imagepath (100)

ImagePath.keyword: Descending

ImagePath	Count
c:\temp\googleupdate.exe	1

win_sysinternals_autoruns_entry (100)

Entry.keyword: Descending

Entry	Count
Google Update	1

win_sysinternals_autoruns_search_common

Time	EntryLocation	LaunchString	Entry	ImagePath
January 8th 2020, 18:30:56.000	HKLM\System\CurrentControlSet\Services	C:\temp\googleupdate.exe	Google Update	c:\temp\googleupdate.exe

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>

```
E:\Sysmon>Sysmon64.exe -?

System Monitor v14.14 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2023 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Usage:
Install:          Sysmon64.exe -i [<configfile>]
Update configuration: Sysmon64.exe -c [<configfile>]
Install event manifest: Sysmon64.exe -m
Print schema:     Sysmon64.exe -s
Uninstall:       Sysmon64.exe -u [force]
  -c Update configuration of an installed Sysmon driver or dump the
      current configuration if no other argument is provided. Optionally
      take a configuration file.
  -i Install service and driver. Optionally take a configuration file.
  -m Install the event manifest (done on service install as well).
  -s Print configuration schema definition of the specified version.
      Specify 'all' to dump all schema versions (default is latest).
  -u Uninstall service and driver. Adding force causes uninstall to proceed
      even when some components are not installed.

The service logs events immediately and the driver installs as a boot-start driver to capture acti
the boot that the service will write to the event log when it starts.

On Vista and higher, events are stored in "Applications and Services Logs/Microsoft/Windows/Sysmon
older systems, events are written to the System event log.

Use the '-? config' command for configuration file documentation. More examples are available on t
website.

Specify -accepteula to automatically accept the EULA on installation, otherwise you will be intera
accept it.

Neither install nor uninstall requires a reboot.
```

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.....



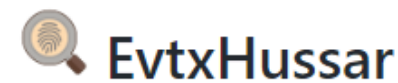
Incident Response

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/ahmedkhelif/APT-Hunter>
- EvtXHussar - <https://github.com/yarox24/EvtxHussar>
- Rheagal - <https://github.com/AbdulRhmanAlfaifi/Rhaegal>
- Persistence Hunter - <https://github.com/last-byte/PersistenceSniper>



LOGONTRACER



PersistenceSniper



RHAEGAL
LOG ANALYZER



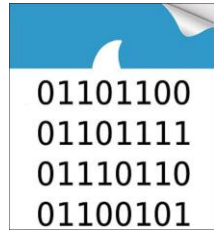
HAYABUSA



Incident Detection

Network Analysis

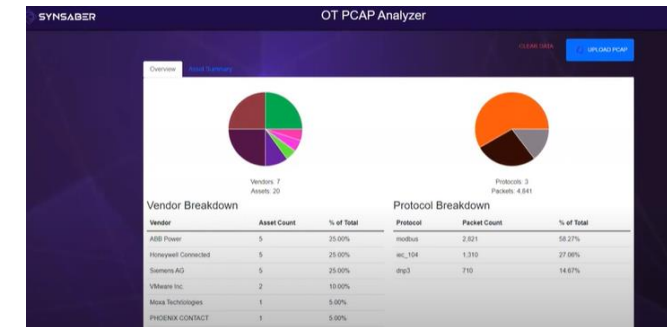
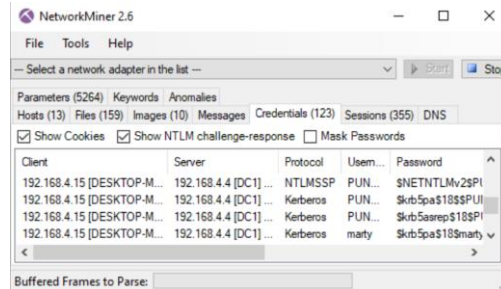
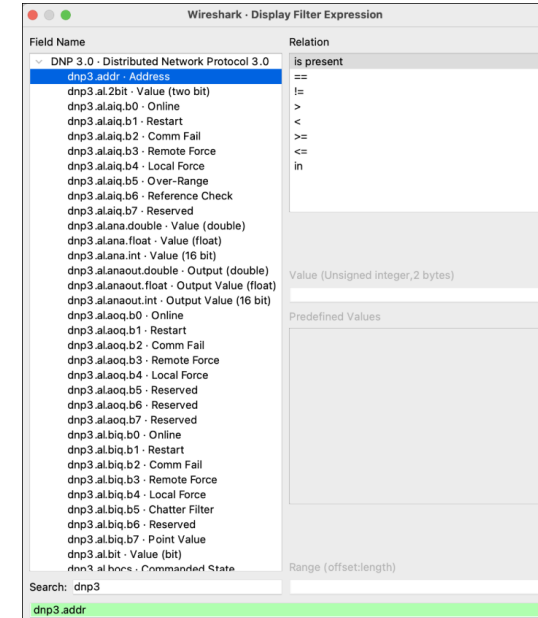
Practice : <https://www.malware-traffic-analysis.net/2023/index.html>



PCAP



```
(ubuntu@linuxopsys)-[~]
└─$ sudo tshark -r capture.pcap -Y "tcp.port == 80"
Running as user "root" and group "root". This could be dangerous.
  5 2.813876528 192.168.246.198 → 93.184.216.34 TCP 66 38236 → 80 [FIN, ACK] Seq=1 A
k=1 Win=502 Len=0 TSval=705197085 TSecr=3126651585
  8 2.814131645 192.168.246.198 → 93.184.216.34 HTTP 565 GET / HTTP/1.1
 11 3.167539500 93.184.216.34 → 192.168.246.198 HTTP 1094 HTTP/1.1 200 OK (text/html)
)
 12 3.167583302 192.168.246.198 → 93.184.216.34 TCP 66 38246 → 80 [ACK] Seq=500 Ack=1
029 Win=493 Len=0 TSval=705197439 TSecr=155900373
 22 5.874241936 192.168.246.198 → 93.184.216.34 TCP 66 [TCP Retransmission] 38236 → 8
0 [FIN, ACK] Seq=1 Ack=1 Win=502 Len=0 TSval=705200146 TSecr=3126651585
 227 8.573998069 192.168.246.198 → 93.184.216.34 HTTP 566 GET / HTTP/1.1
 261 8.868378881 93.184.216.34 → 192.168.246.198 HTTP 1093 HTTP/1.1 200 OK (text/html)
)
```

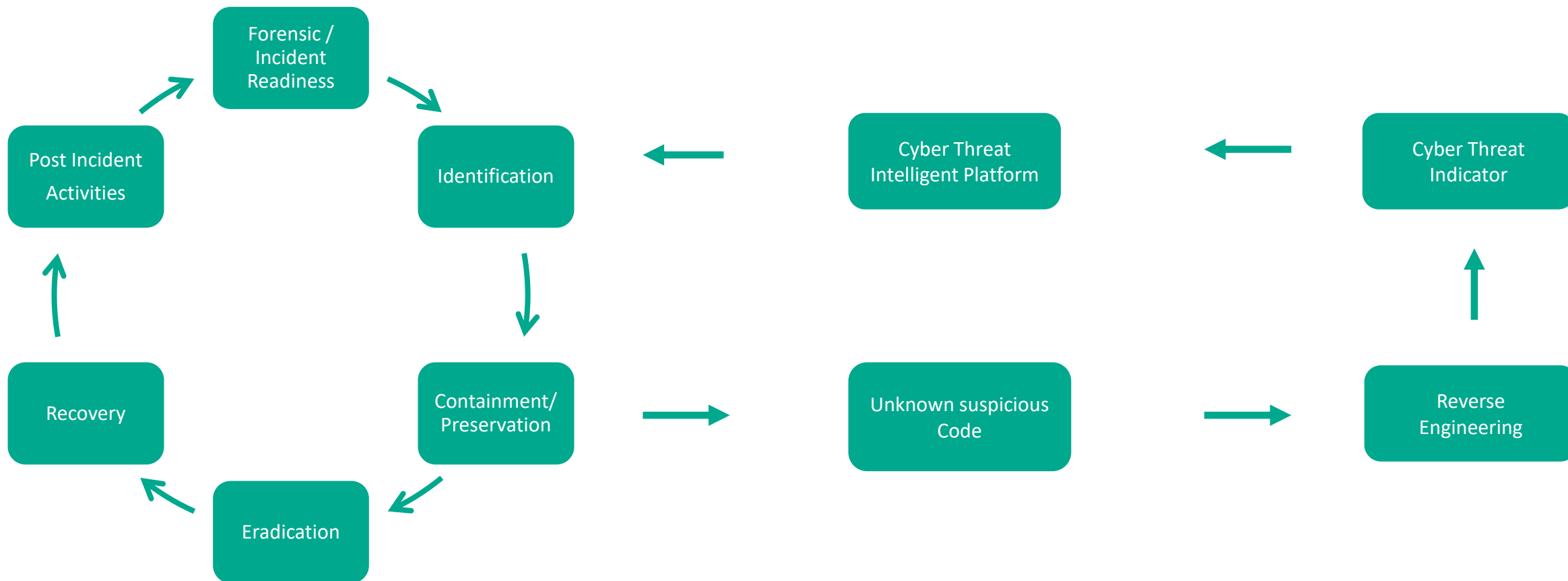


Intelligence-Drive Incident Response



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

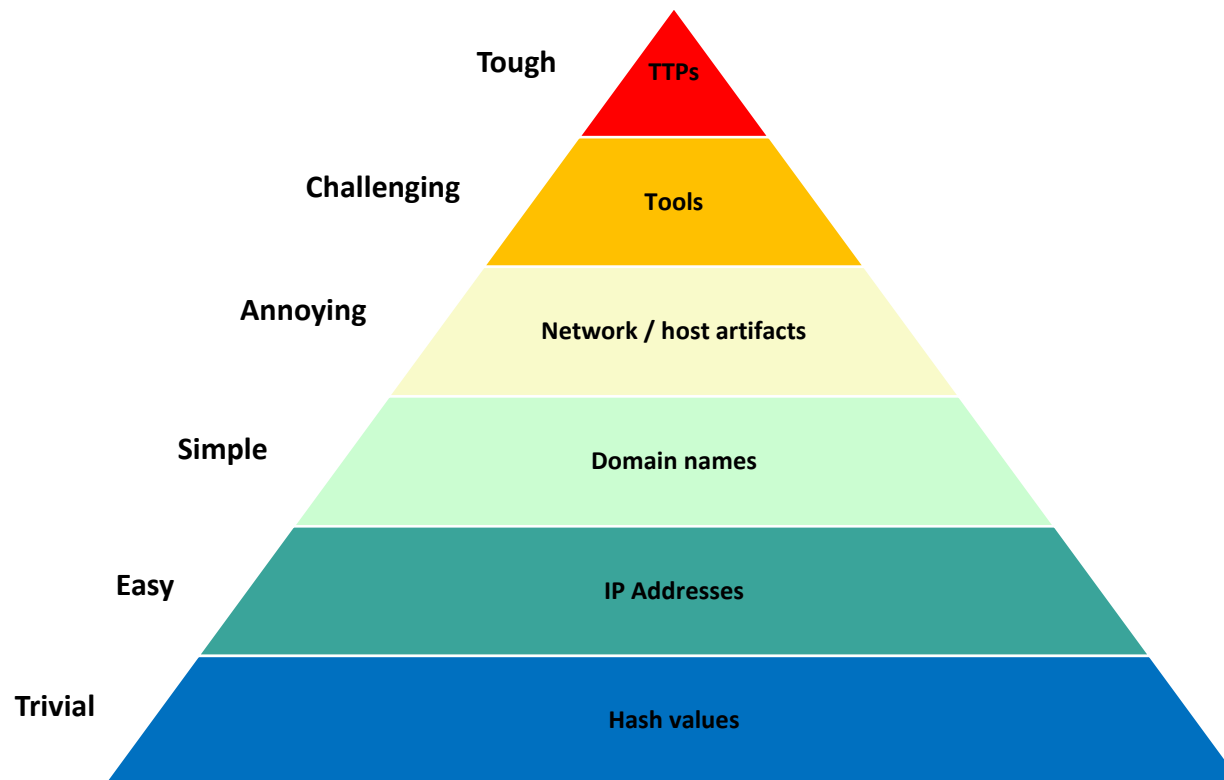
The image shows two screenshots of the Kaspersky CyberTrace interface. The top screenshot displays the 'Statistics overview' section with a line graph showing 'Number of detections' and 'Number of detected indicators' over time, categorized by IP address, Hash, and URL. The bottom screenshot shows the 'Indicator' search page with a search bar and a 'Statistics period' selector set to 'All time'.

The image shows the VirusTotal Enterprise search interface. It features a search bar with a magnifying glass icon and a 'SEARCH' button. Below the search bar, there is a text input field for entering a hash, domain, IP address, or URL. The interface also includes a 'VT ENTERPRISE' logo and a brief description of the service.

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



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>

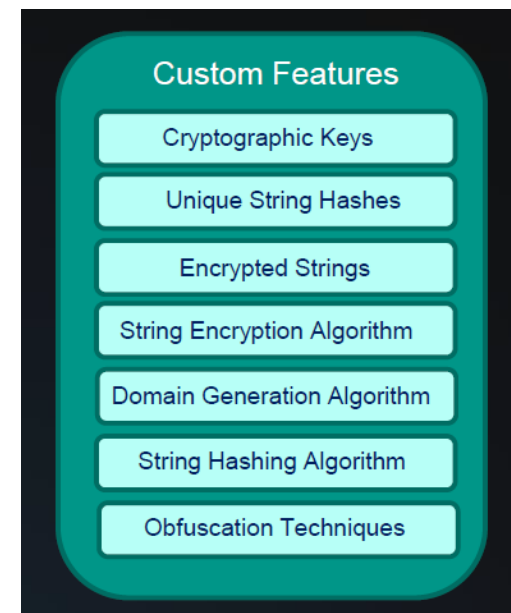
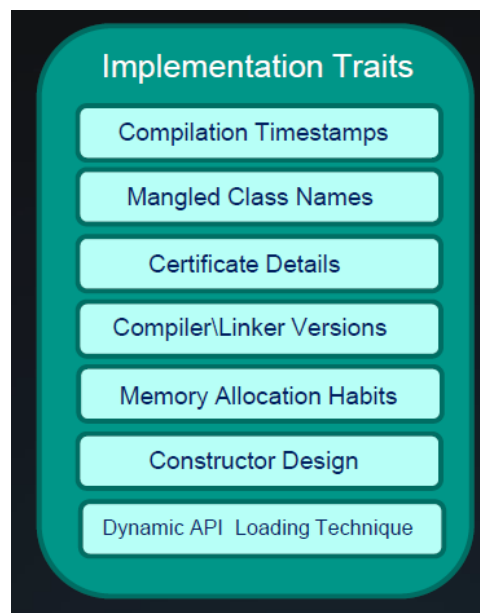
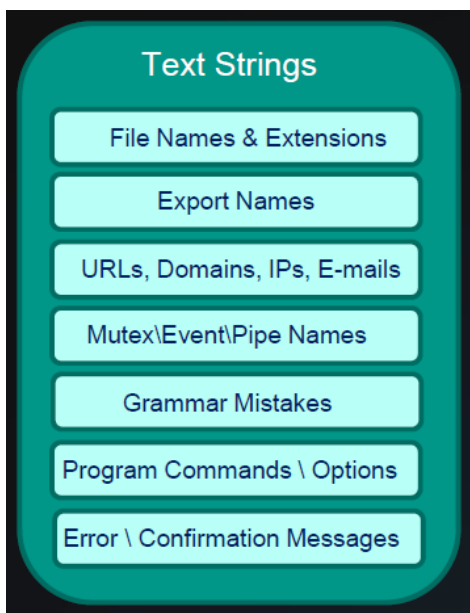


Incident Response Tools - YARA

Default usage of yara

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

Design tips



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

- 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://yaradb.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

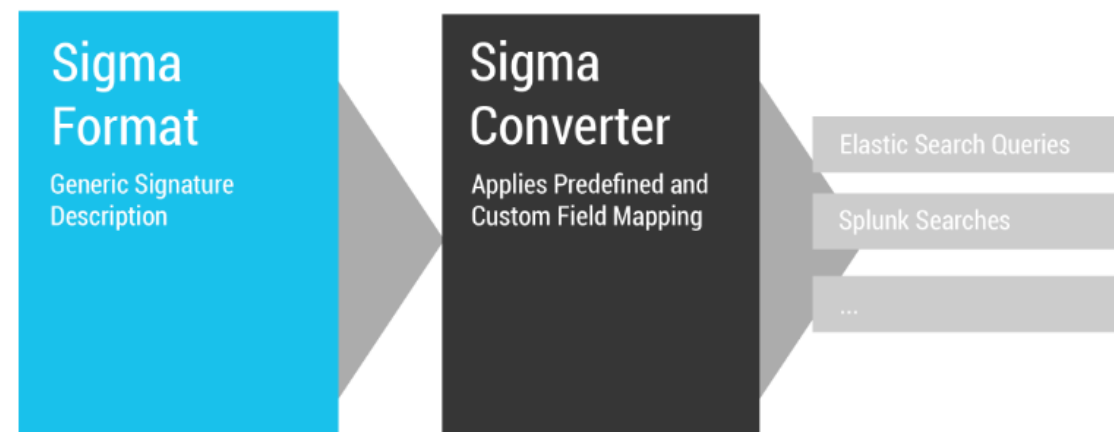
Other useful Yara Scanner

- 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>

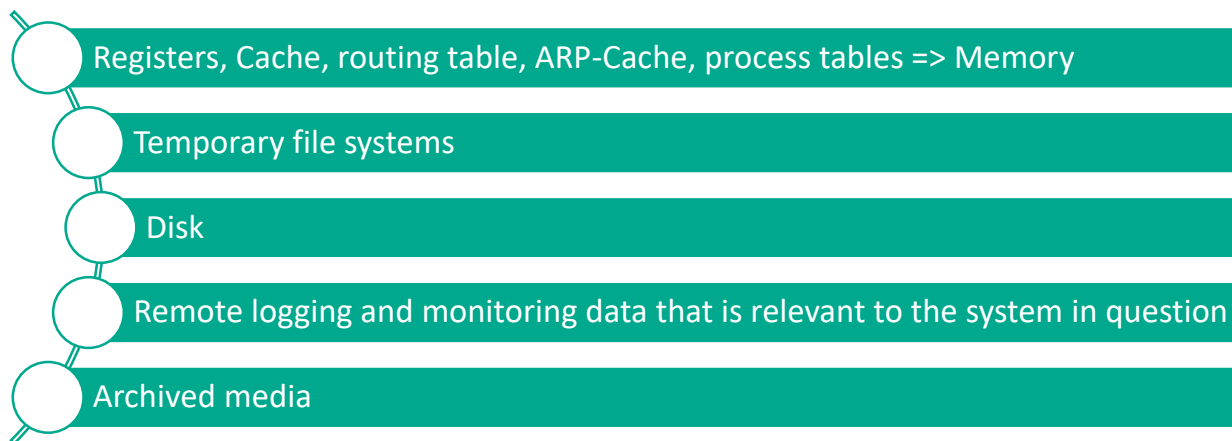


Evidence Collection



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:         0xffffffff8017930de58
KdDebuggerData:          0xffffffff80179a00b20
KdpDataBlockEncoded:     0xffffffff80179a50b00

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 inaccessible pages: 0
Total of accessible pages: 2096861

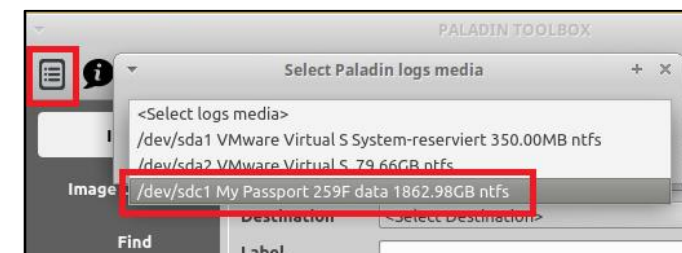
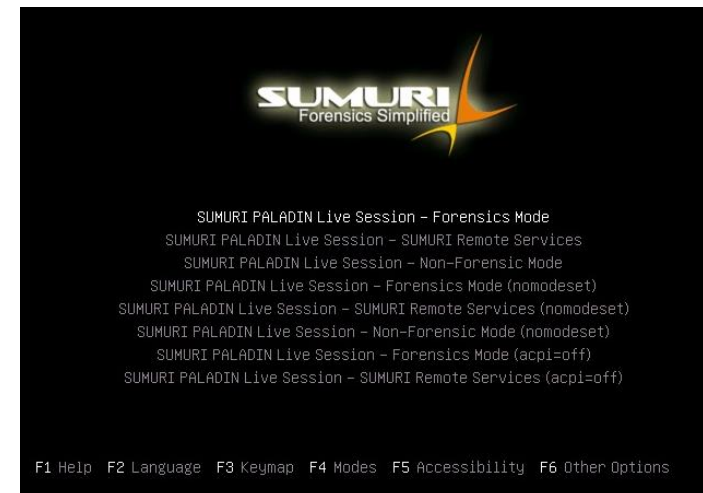
SHA-256: F6AD246743ED1C3942138F45093CD329EFEDD3FA21B402F16E2E2F3DB5F019F8

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

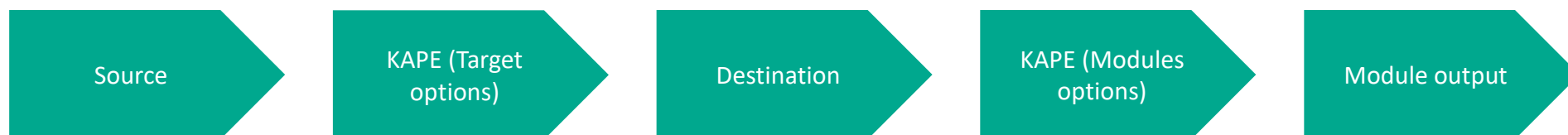
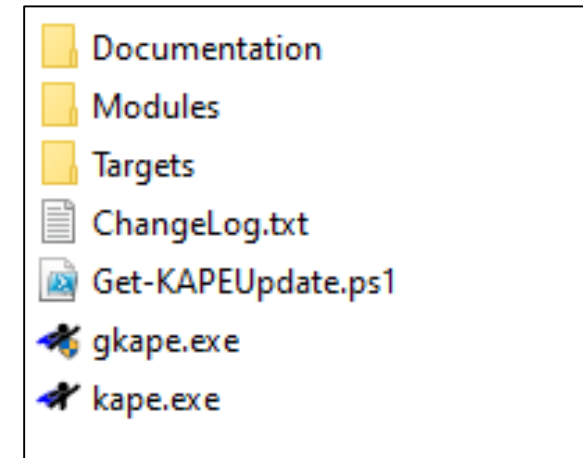


Which artifacts would you collect?

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] 2023-02-06T13:13:54Z 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 $Extend\${UsnJrnl:$}
[INFO] 2023-02-06T13:13:55Z ntfs: Selecting glob $Extend\${UsnJrnl:$}Max
[INFO] 2023-02-06T13:13:55Z ntfs: Selecting glob $Extend\${}
[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

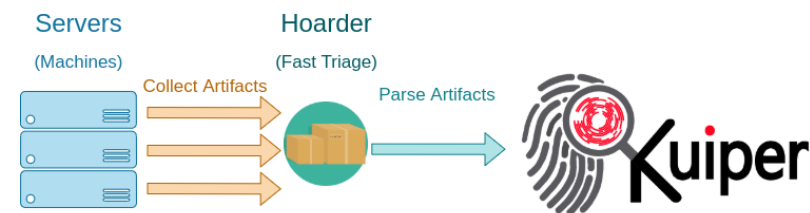
<https://tap-ir.github.io/#/>

- Fennec (Linux / OSX)

<https://github.com/AbdulRhmanAlfaifi/Fennec>

- TimeSketch

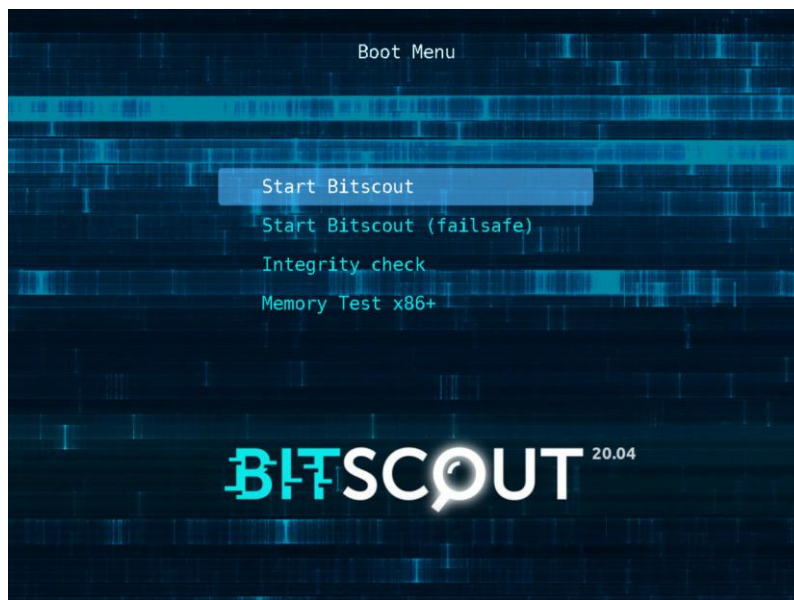
<https://github.com/google/timesketch>



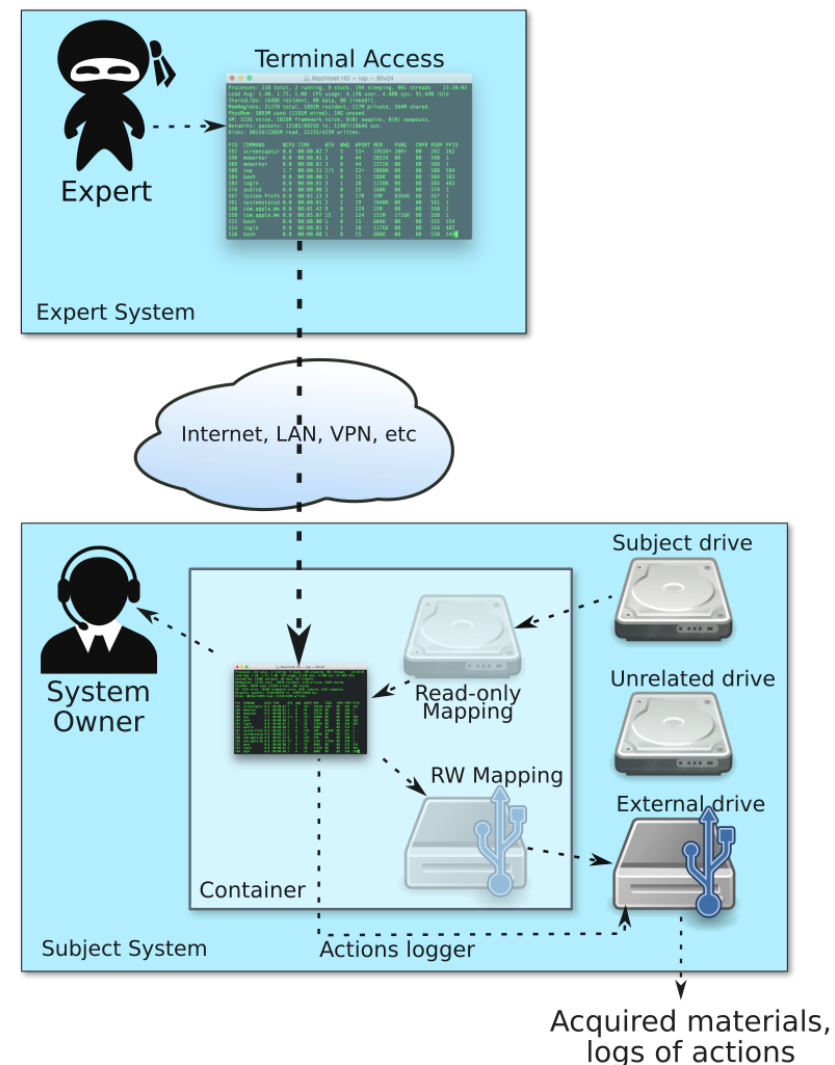
Remote Evidence Collection

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>)

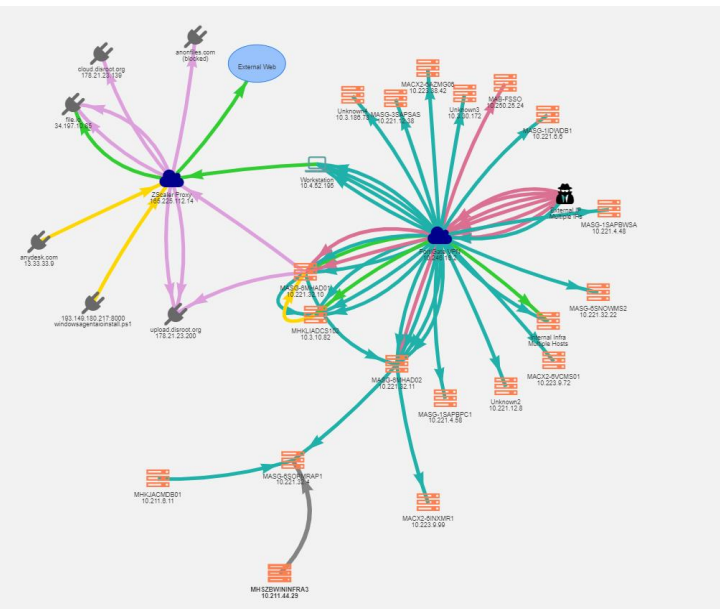
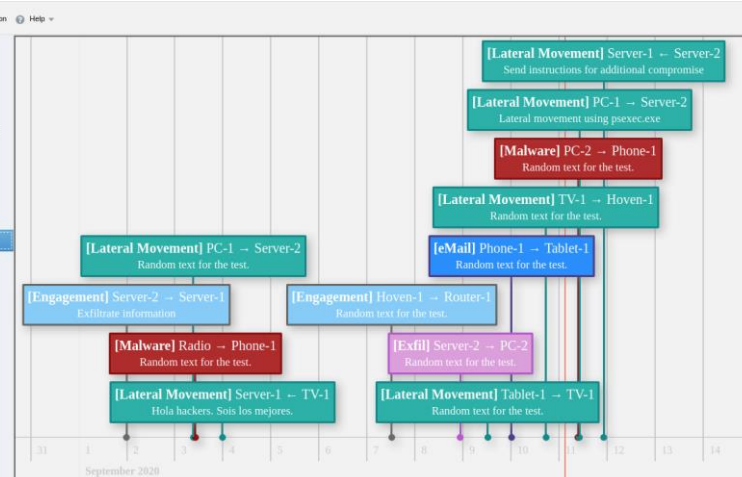
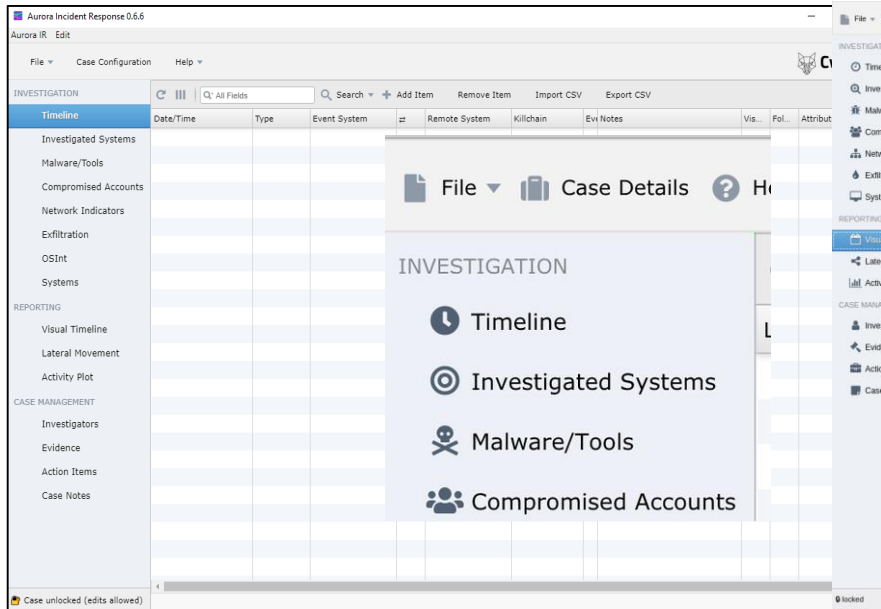
Monolith Notes

MONOLITH NOTES
MONOLITH FORENSICS

Cases

+ New Case Case Filter Export Table Cases Listed: 1 execution

Cases	Case Number	Client	Case Reference	Case Type	Case Lead	Open Date	Status
	IR_20230310_2	XYZ	None	Ransomware	KS	03/10/2023	open



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

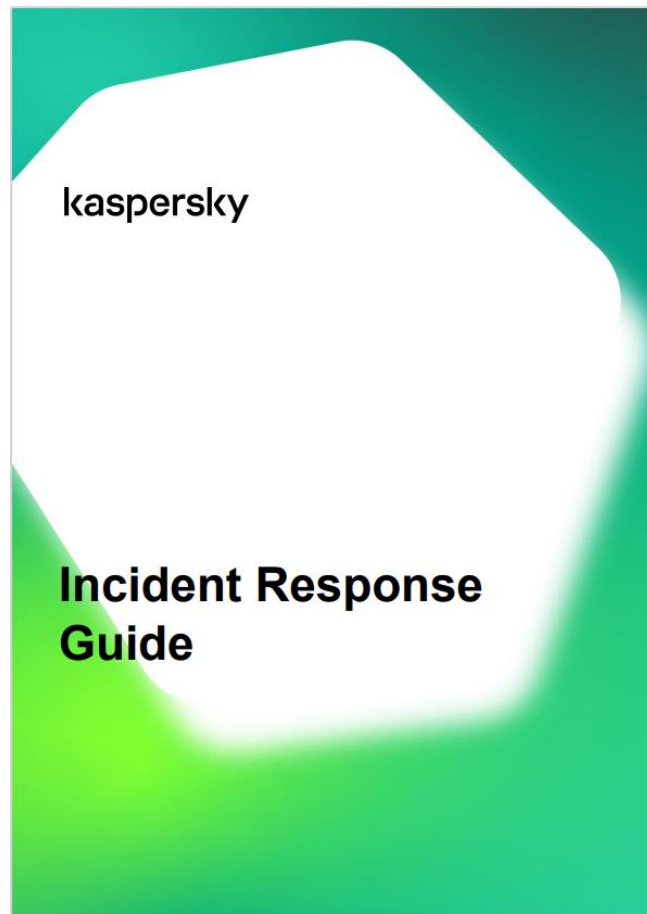
The screenshot shows the TheHive web interface. At the top, there's a navigation bar with 'TheHive' logo, '+ New Case', 'My tasks 7', 'Waiting tasks 107', 'Alerts 182', 'Dashboards', and a search bar. Below this, the main content area is titled 'List of cases (31 of 53)'. It includes filter controls like 'Quick Filters' and 'Sort by', and a filter applied: 'status: Open'. A pagination bar shows 'First', 'Previous', '1', '2', '3', 'Next', 'Last'. The main table lists cases with columns: Title, Severity, Tasks, Observables, Assignee, Date, and Actions. The first case is '#34 - [MALSPAM] Malspam 2016-10-06 (.js in .zip) - campaign: "Your Order"' with severity 'M', 5 tasks, 824 observables, and a date of 03/20/19 10:56. Other cases include vulnerabilities and OSINT reports.

Title	Severity	Tasks	Observables	Assignee	Date	Actions
#34 - [MALSPAM] Malspam 2016-10-06 (.js in .zip) - campaign: "Your Order"	M	5 Tasks	824	[Avatar]	03/20/19 10:56 a year	[Gear]
#27 - [CTI][Vulnerability] This is a case created from a template	M	5 Tasks	3	[Avatar]	02/28/19 14:55 a year	[Gear]
#24 - [MISP] #3329 OSINT - ASERT Threat Intelligence Report 2016-03 The Four-Element Sword Engagement	M	5 Tasks	53	[Avatar]	02/09/17 12:03 3 years	[Gear]
#21 - [MISP] #4855 OSINT - Nemucod downloader spreading via Facebook	L	5 Tasks	5	[Avatar]	01/24/17 11:37 4 years	[Gear]
#20 - [MISP] #3107 OSINT - Turbo Twist: Two 64-bit Derusbi Strains Converge	L	5 Tasks	10	[Avatar]	01/24/17 9:04 4 years	[Gear]
#17 - #3024 OSINT - In the Shadows: Vawtrak Aims to Get Stealthier by adding New Data Cloaking	L	No Tasks	20	[Avatar]	01/22/17 12:17 4 years	[Gear]

<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