GUIDANCE SOFTWARE™

OCTOBER 2016

DEFEATING THREATS WITH DIGITAL FORENSIC INCIDENT RESPONSE

Yasser Anter
Solutions Consultant - MEA
Guidance Software

Fact:

IF 99% OF FLIGHTS DIDN’T CRASH - *YOU WOULDN’T FLY!*

1% failure is enormous…
= 300,000 crashes a year

JUST BECAUSE IT’S QUIET

DOESN’T MEAN YOU’RE SAFE

SENSITIVE DATA IS LUCRATIVE

MORE ATTACKS

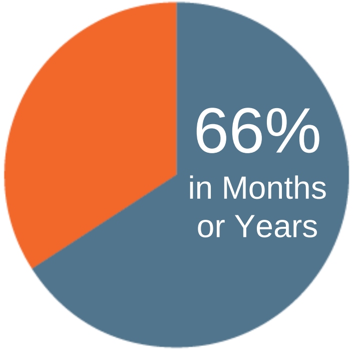
DETECTION AND RESPONSE TIMES ARE UNTENABLE

60% of organizations breached in **minutes or less**[1]

66% of breaches take **months or years** to discover[2]

70-90% of malware samples are uni**que to an organization**[1]

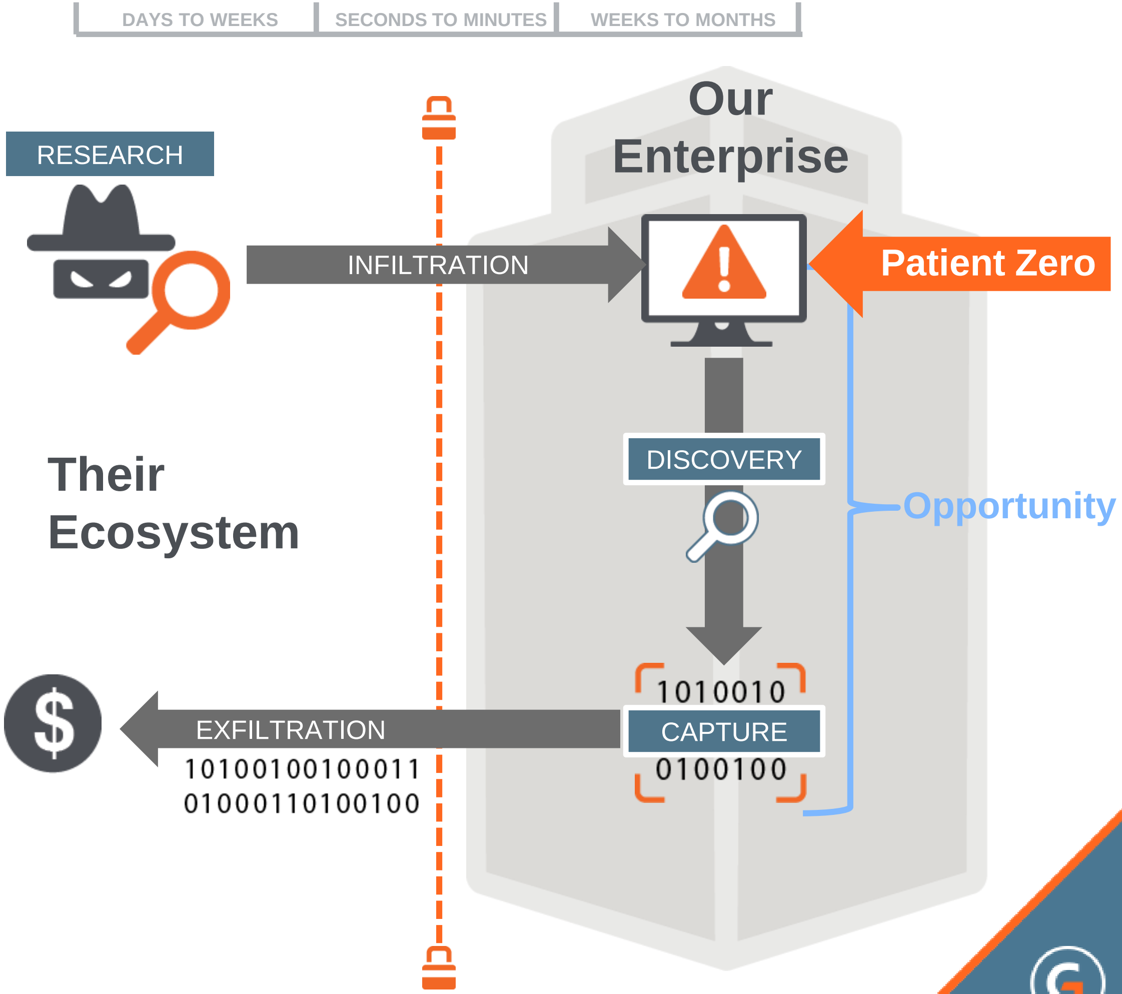
32 days to **respond to an incident**[2]



Time to Resolution

[1] Verizon 2015 Data Breach Investigation Report
[2] Verizon 2013 Data Breach Investigation Report

METHODOLOGY OF AN ATTACK



VISIBILITY is Key

PASSPORT

FINGER PRINT

EYE SCAN

LUGGAGE SCAN

IS IT ENOUGH?

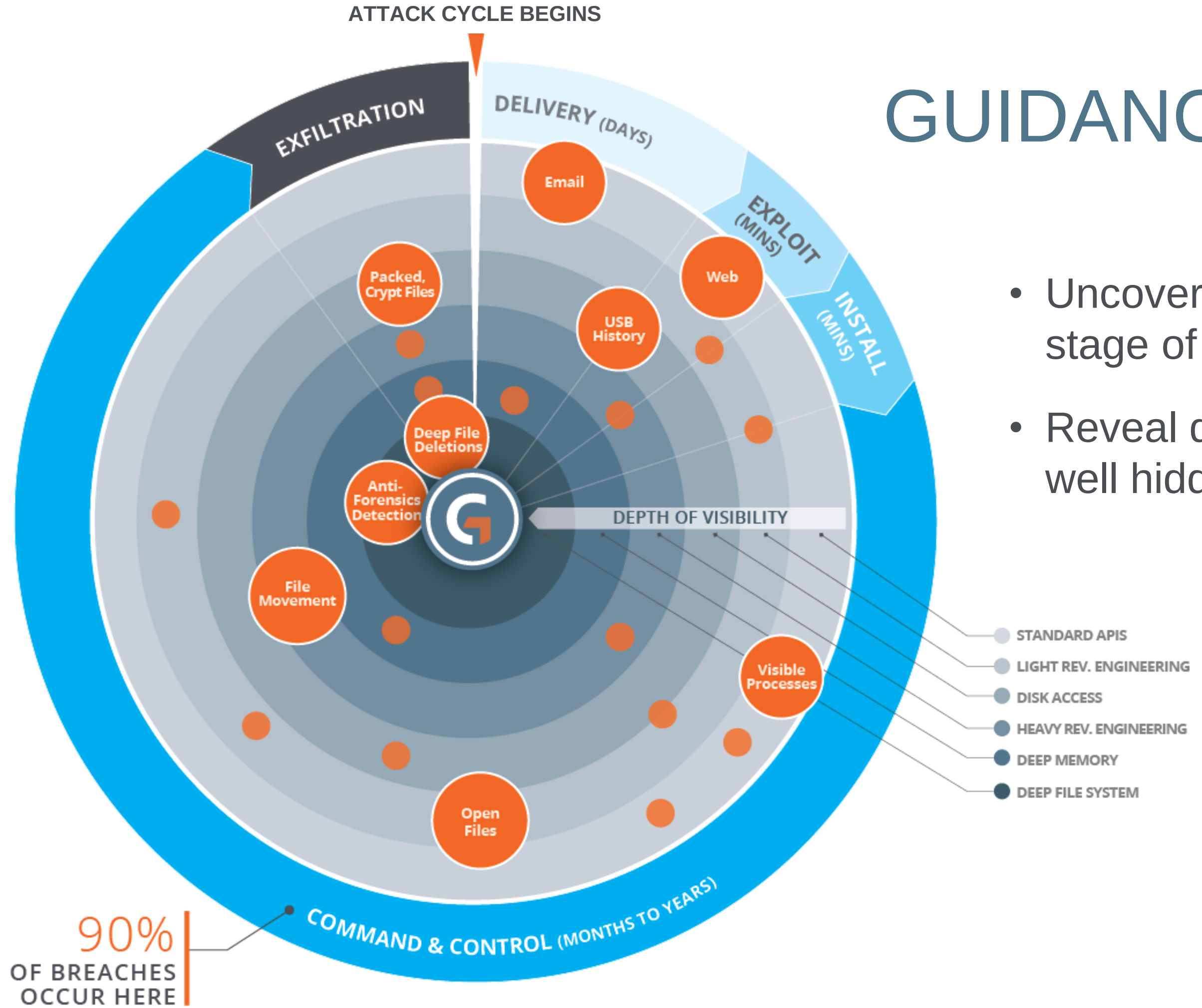
BEHAVIORS

FLIR
Manual
1 35.0
36.5
40
23
Trefl=23 Tatm=23 Dst=3.0 FOV 23
2015-06-21 10:55:05 -40 - +120 e=0.98
°C
LG

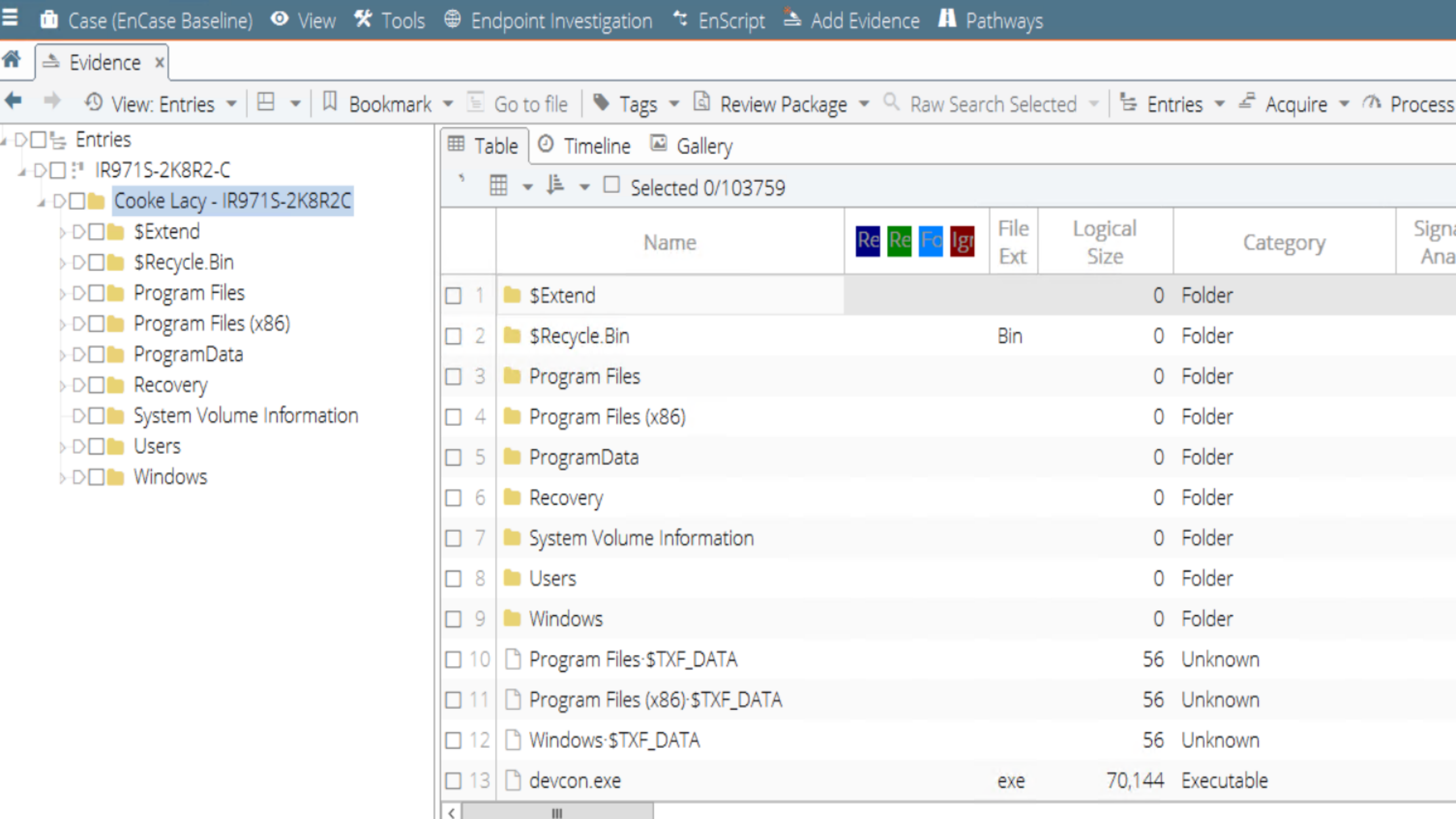
STOP

KERNEL LEVEL VISIBILITY

GUIDANCE 360° VISIBILITY



- Uncover forensic residue across every stage of the attack cycle
- Reveal data security risk, no matter how well hidden



Selected 0/103759

- Entries
  - IR971S-2K8R2-C
    - Cooke Lacy - IR971S-2K8R2C
      - $Extend
      - $Recycle.Bin
      - Program Files
      - Program Files (x86)
      - ProgramData
      - Recovery
      - System Volume Information
      - Users
      - Windows

	Name	Re Re Fo Igr	File Ext	Logical Size	Category	Signa Ana
□ 1	$Extend			0	Folder	
□ 2	$Recycle.Bin		Bin	0	Folder	
□ 3	Program Files			0	Folder	
□ 4	Program Files (x86)			0	Folder	
□ 5	ProgramData			0	Folder	
□ 6	Recovery			0	Folder	
□ 7	System Volume Information			0	Folder	
□ 8	Users			0	Folder	
□ 9	Windows			0	Folder	
□ 10	Program Files·$TXF_DATA			56	Unknown	
□ 11	Program Files (x86)·$TXF_DATA			56	Unknown	
□ 12	Windows·$TXF_DATA			56	Unknown	
□ 13	devcon.exe		exe	70,144	Executable	

ENCASE ENDPOINT SECURITY

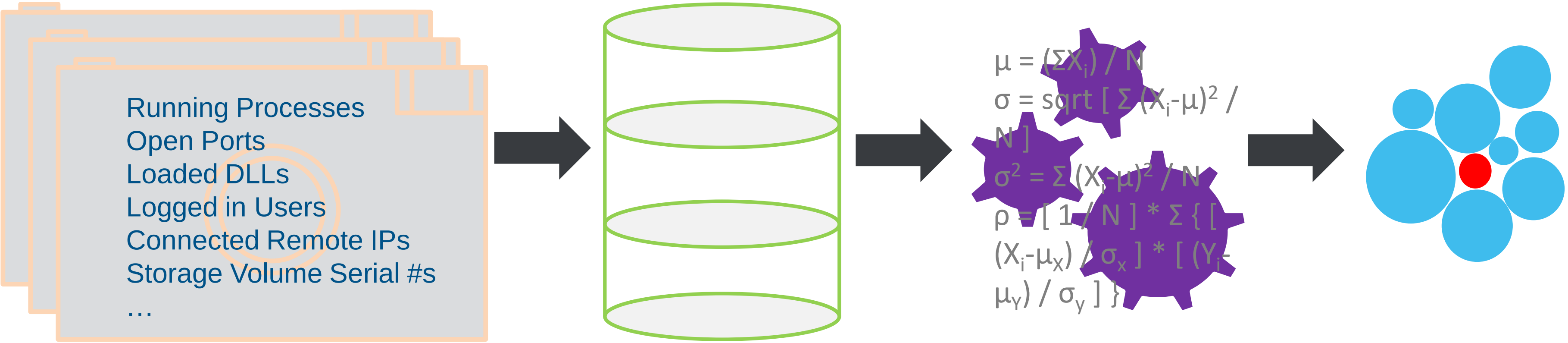
THREE PRIMARY SECURITY STEPS

- Threat Detection and Threat Hunting
- Active Response / Alert Triage
- Incident Response Support

STEP 1

ADVANCED THREAT DETECTION

THREAT DETECTION – ANALYTICS ON ENTERPRISE-WIDE SNAPSHOTS



Running Processes
Open Ports
Loaded DLLs
Logged in Users
Connected Remote IPs
Storage Volume Serial #s
…

$\mu = (\Sigma X_i) / N$

$\sigma = sqrt\ [\ \Sigma\ (X_i-\mu)^2 / N\ ]$

$\sigma^2 = \Sigma\ (X_i-\mu)^2 / N$

$\rho = [\ 1 / N\ ] * \Sigma\ \{\ [\ (X_i-\mu_X) / \sigma_x\ ] * [\ (Y_i-\mu_Y) / \sigma_y\ ]\ \}$

Enterprise-wide Endpoint scans

Scales to 100s of thousands of endpoints

Data Warehousing

Historical database of endpoint telemetry

Analytics

System performs statistical analysis to compute baseline behavior and identify outliers

Visualization

Results are visualized to easily spot anomalies and potential threats

ARTIFACTS COLLECTED WITH EACH SCAN

Each scan takes seconds, payload is 0.3 – 0.5 MB and is extremely scalable

- Host Information
- Hostname
- IP address
- Operating System
- Processor
- System Type
- System version
- Service Pack
- Is64Bit [Y/N]
- Accounts and Users
- Account Name
- SID
- Last Accessed (logged in)
- Open Files
- Full Path
- Filename
- Process Name
- Process Path
- Process ID

Processes

- Process Name
- Instance Name
- Hidden [Y/N]
- Process ID
- Parent Process ID
- Executable Size
- Executable Hash
- File Path
- Parameter
- Service DLL Path
- Process Type
- Service DLL
- Start Time
- User Name
- DLL Count
- Child Processes
- Service Type
- Is64Bit [Y/N]
- Running [Y/N]
- File Name Only [Y/N]
- Root Directory
- User ID

DLLs

- DLL Path
- DLL Name
- Injected DLL [Y/N]
- DLL Size
- DLL Hash
- Related Process Metadata (see "Process" section)

(Network) ARP Cache

- IP
- M
- AR
- Ac

(Netw

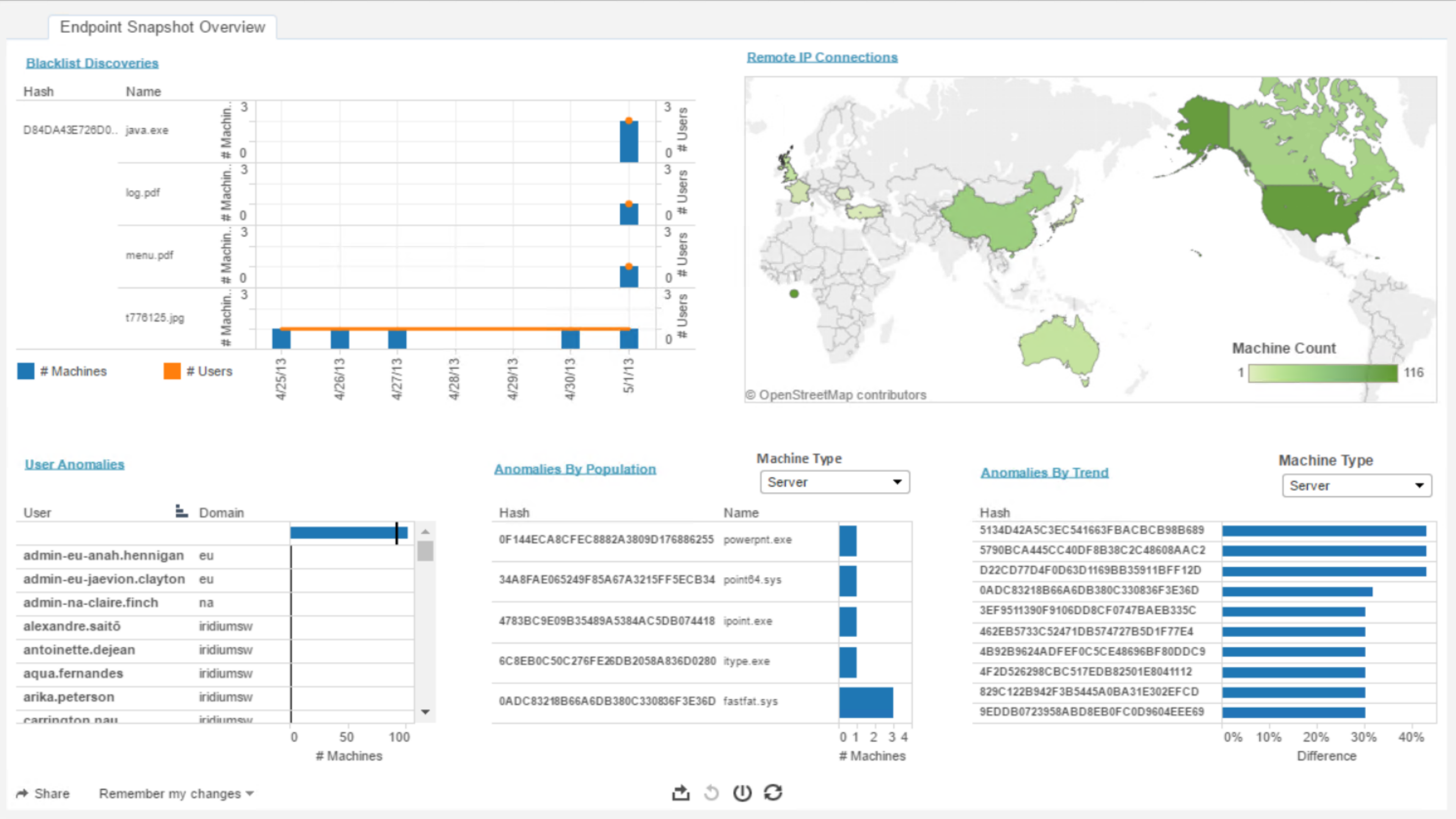
- In
- IP
- N
- M

(Network) Open Ports

- Local Port
- Local IP
- Remote Port
- Remote IP
- Protocol
- State
- Port Name
- Process Name

Anomalous Process Spread

These artifacts are used to baseline process activity on endpoints across the enterprise and detect net new processes or processes spreading across machines at an unusual rate in a malware-like behavior.



Endpoint Snapshot Overview

Blacklist Discoveries

Hash	Name
D84DA43E726D0..	java.exe
	log.pdf
	menu.pdf
	t776125.jpg

Remote IP Connections

User Anomalies

User	Domain
admin-eu-anah.hennigan	eu
admin-eu-jaevion.clayton	eu
admin-na-claire.finch	na
alexandre.saitō	iridiumsw
antoinette.dejean	iridiumsw
aqua.fernandes	iridiumsw
arika.peterson	iridiumsw
carrington.nau	iridiumsw

Anomalies By Population

Machine Type: Server

Hash	Name
0F144ECA8CFEC8882A3809D176886255	powerpnt.exe
34A8FAE065249F85A67A3215FF5ECB34	point64.sys
4783BC9E09B35489A5384AC5DB074418	ipoint.exe
6C8EB0C50C276FE26DB2058A836D0280	itype.exe
0ADC83218B66A6DB380C330836F3E36D	fastfat.sys

Anomalies By Trend

Machine Type: Server

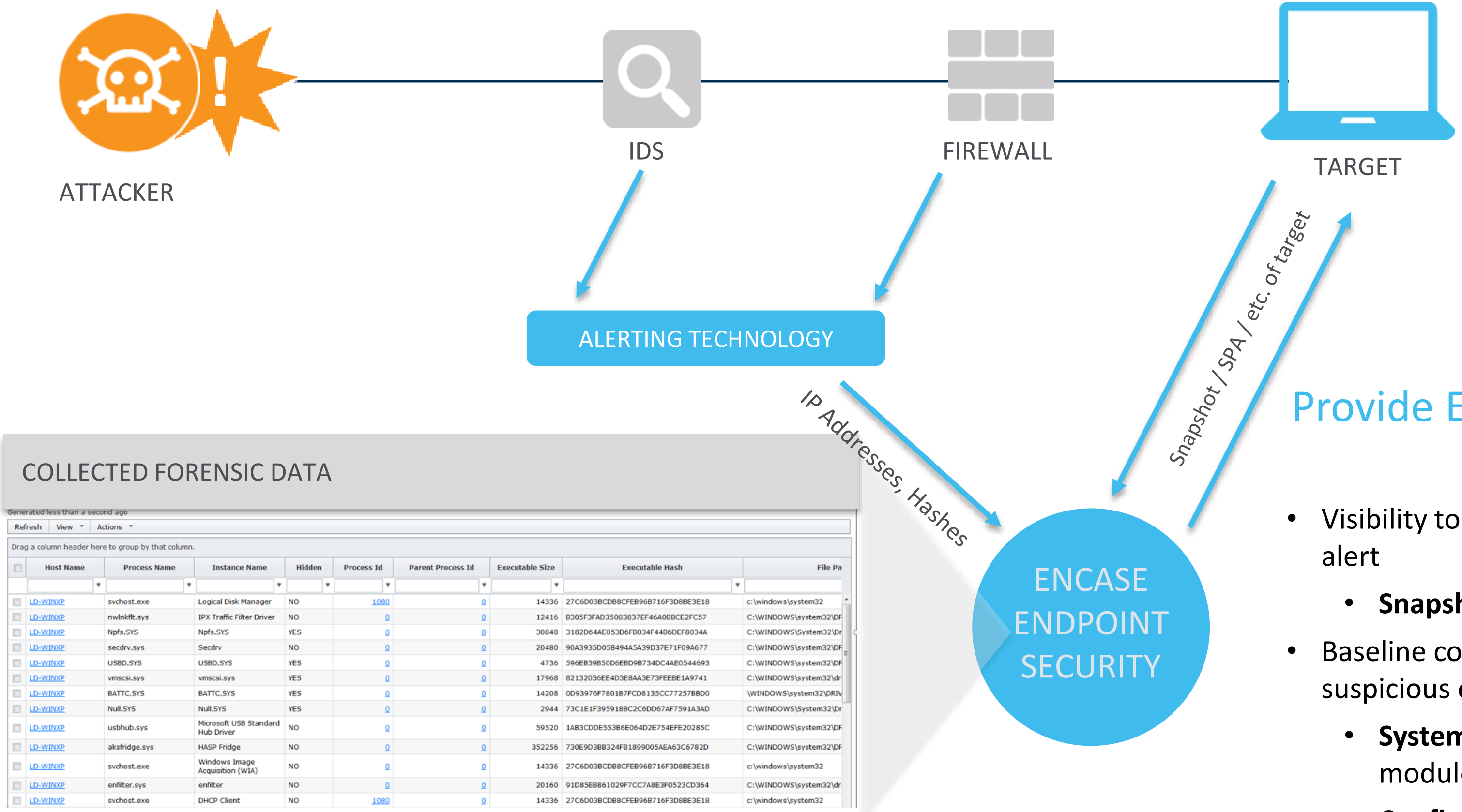
Hash
5134D42A5C3EC541663FBACBCB98B689
5790BCA445CC40DF8B38C2C48608AAC2
D22CD77D4F0D63D1169BB35911BFF12D
0ADC83218B66A6DB380C330836F3E36D
3EF9511390F9106DD8CF0747BAEB335C
462EB5733C52471DB574727B5D1F77E4
4B92B9624ADFEF0C5CE48696BF80DDC9
4F2D526298CBC517EDB82501E8041112
829C122B942F3B5445A0BA31E302EFCD
9EDDB0723958ABD8EB0FC0D9604EEE69

STEP 2

ACTIVE RESPONSE / ALERT TRIAGE:

CONFIRM AND PRIORITIZE SECURITY ALERTS

ACTIVE RESPONSE / ALERT TRIAGE – INTEGRATION AND AUTOMATION



ATTACKER

IDS

FIREWALL

TARGET

ALERTING TECHNOLOGY

IP Addresses, Hashes

Snapshot / SPA / etc. of target

ENCASE ENDPOINT SECURITY

COLLECTED FORENSIC DATA

Generated less than a second ago

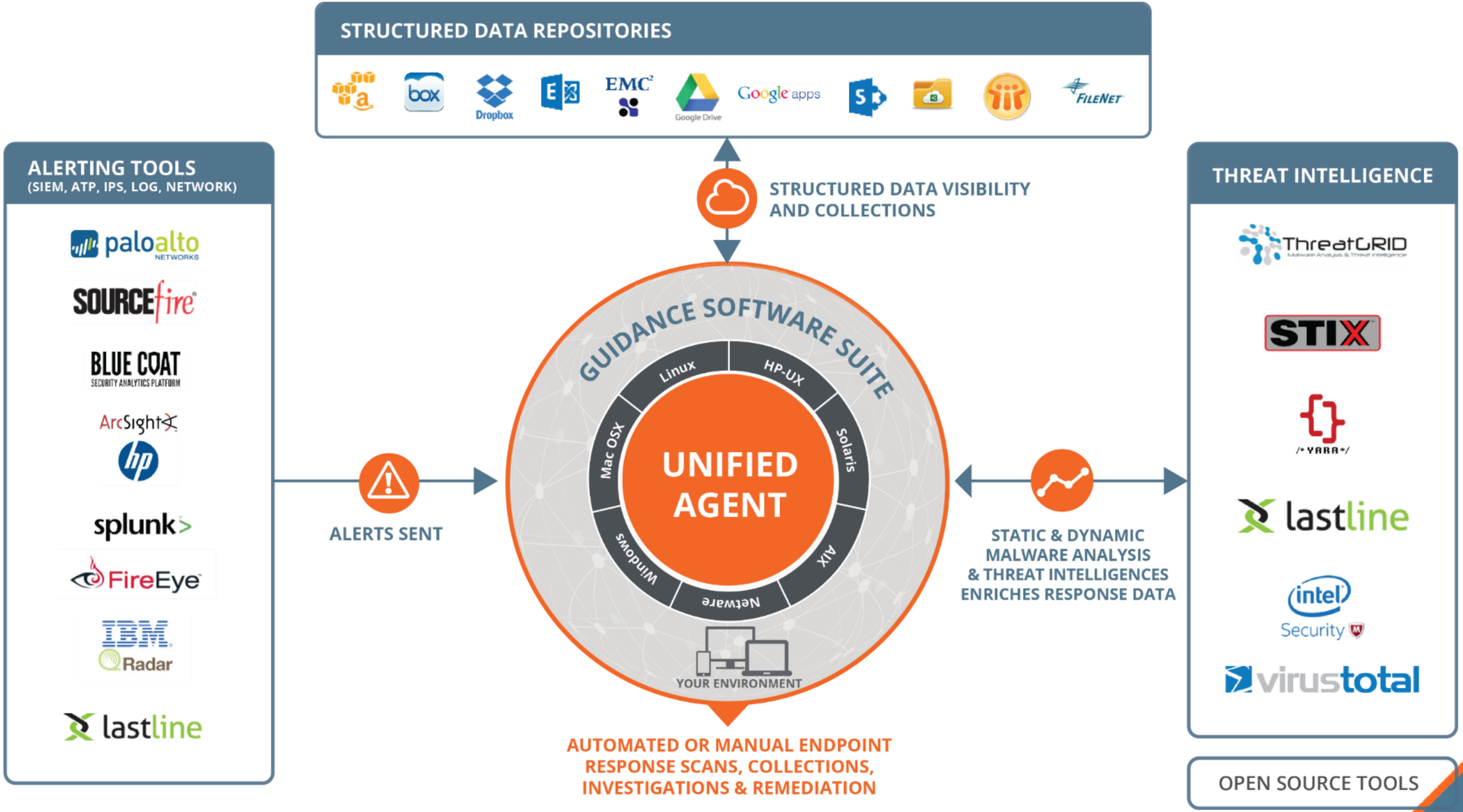
Drag a column header here to group by that column.

□	Host Name	Process Name	Instance Name	Hidden	Process Id	Parent Process Id	Executable Size	Executable Hash	File Pa
□	LD-WINXP	svchost.exe	Logical Disk Manager	NO	1080	0	14336	27C6D03BCDB8CFEB96B716F3D8BE3E18	c:\windows\system32
□	LD-WINXP	nwlnkflt.sys	IPX Traffic Filter Driver	NO	0	0	12416	B305F3FAD35083837EF46A0BBCE2FC57	C:\WINDOWS\system32\DF
□	LD-WINXP	Npfs.SYS	Npfs.SYS	YES	0	0	30848	3182D64AE053D6FB034F44B6DEF8034A	C:\WINDOWS\System32\Dr
□	LD-WINXP	secdrv.sys	Secdrv	NO	0	0	20480	90A3935D05B494A5A39D37E71F09A677	C:\WINDOWS\system32\DF
□	LD-WINXP	USBD.SYS	USBD.SYS	YES	0	0	4736	596EB39B50D6EBD9B734DC4AE0544693	C:\WINDOWS\system32\DF
□	LD-WINXP	vmscsi.sys	vmscsi.sys	YES	0	0	17968	82132036EE4D3E8AA3E73FEEBE1A9741	C:\WINDOWS\system32\dr
□	LD-WINXP	BATTC.SYS	BATTC.SYS	YES	0	0	14208	0D93976F7801B7FCD8135CC77257BBD0	\WINDOWS\system32\DRIV
□	LD-WINXP	Null.SYS	Null.SYS	YES	0	0	2944	73C1E1F395918BC2C6DD67AF7591A3AD	C:\WINDOWS\System32\Dr
□	LD-WINXP	usbhub.sys	Microsoft USB Standard Hub Driver	NO	0	0	59520	1AB3CDDE553B6E064D2E754EFE20285C	C:\WINDOWS\system32\DF
□	LD-WINXP	aksfridge.sys	HASP Fridge	NO	0	0	352256	730E9D3BB324FB1899005AEA63C6782D	C:\WINDOWS\system32\DF
□	LD-WINXP	svchost.exe	Windows Image Acquisition (WIA)	NO	0	0	14336	27C6D03BCDB8CFEB96B716F3D8BE3E18	c:\windows\system32
□	LD-WINXP	enfilter.sys	enfilter	NO	0	0	20160	91D85EB861029F7CC7A8E3F0523CD364	C:\WINDOWS\system32\dr
□	LD-WINXP	svchost.exe	DHCP Client	NO	1080	0	14336	27C6D03BCDB8CFEB96B716F3D8BE3E18	c:\windows\system32

Provide Endpoint Context to Security Alerts

- Visibility to endpoint state at time of alert
  - **Snapshot** module
- Baseline comparison to detect suspicious observables
  - **System Profile Analysis** module
  - **Configuration Assessment** module

KEY INTEGRATIONS



STRUCTURED DATA REPOSITORIES

STRUCTURED DATA VISIBILITY AND COLLECTIONS

ALERTING TOOLS (SIEM, ATP, IPS, LOG, NETWORK)

ALERTS SENT

AUTOMATED OR MANUAL ENDPOINT RESPONSE SCANS, COLLECTIONS, INVESTIGATIONS & REMEDIATION

STATIC & DYNAMIC MALWARE ANALYSIS & THREAT INTELLIGENCES ENRICHES RESPONSE DATA

THREAT INTELLIGENCE

OPEN SOURCE TOOLS

STEP 3

INCIDENT RESPONSE: INVESTIGATION TO REMEDIATION

DETERMINE ROOT CAUSE AND SCOPE OF INCIDENT

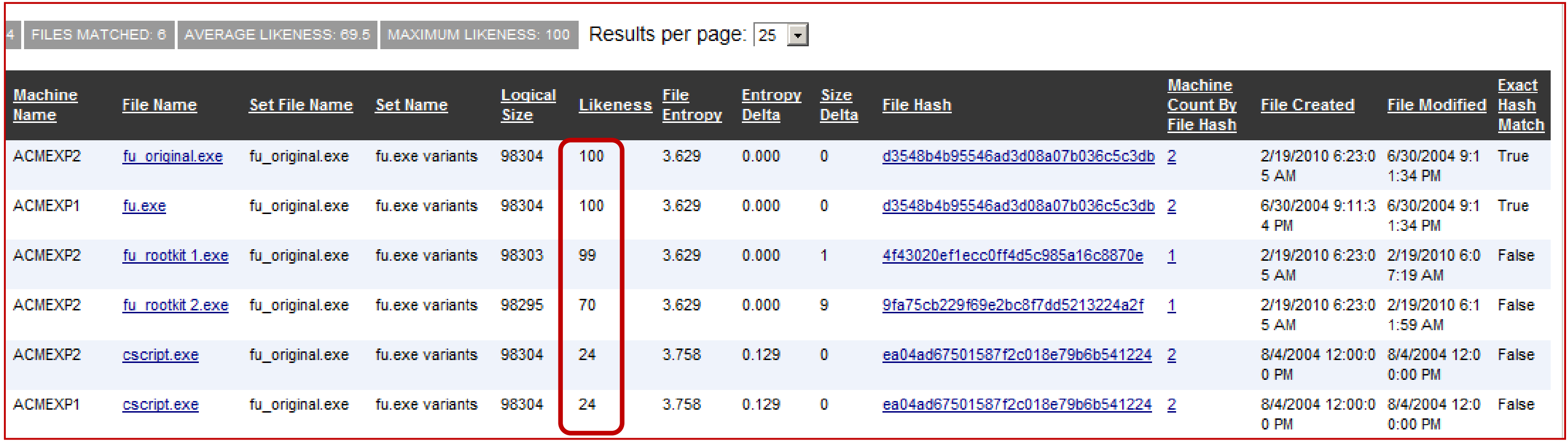
Incident Response Modules

- Host based artifacts collection
- Internet artifact collection
- Live RAM acquisition
- Registry Search
- Entropy Near Match
- IOC Search using YARA rules / STIX
- Forensic Endpoint Event Timeline

ENCASE® ENTROPY

Expose additional instances or variations of malware on systems

- Find like binaries
- Signature-less triage of advanced malware
- Based on “Entropy” and file size

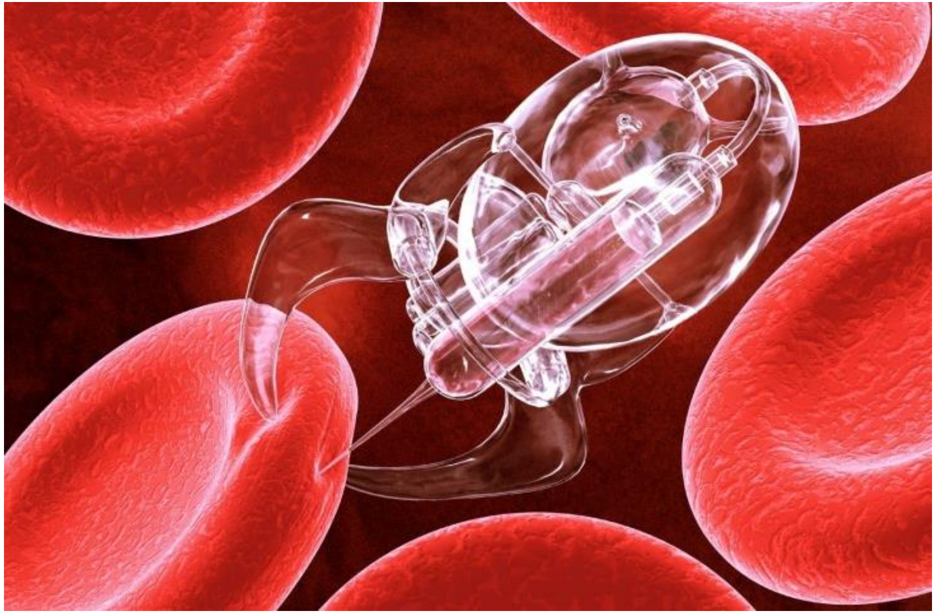


4 | FILES MATCHED: 6 | AVERAGE LIKENESS: 69.5 | MAXIMUM LIKENESS: 100 | Results per page: 25

Machine Name	File Name	Set File Name	Set Name	Logical Size	Likeness	File Entropy	Entropy Delta	Size Delta	File Hash	Machine Count By File Hash	File Created	File Modified	Exact Hash Match
ACMEXP2	fu_original.exe	fu_original.exe	fu.exe variants	98304	100	3.629	0.000	0	d3548b4b95546ad3d08a07b036c5c3db	2	2/19/2010 6:23:05 AM	6/30/2004 9:11:34 PM	True
ACMEXP1	fu.exe	fu_original.exe	fu.exe variants	98304	100	3.629	0.000	0	d3548b4b95546ad3d08a07b036c5c3db	2	6/30/2004 9:11:34 PM	6/30/2004 9:11:34 PM	True
ACMEXP2	fu_rootkit_1.exe	fu_original.exe	fu.exe variants	98303	99	3.629	0.000	1	4f43020ef1ecc0ff4d5c985a16c8870e	1	2/19/2010 6:23:05 AM	2/19/2010 6:07:19 AM	False
ACMEXP2	fu_rootkit_2.exe	fu_original.exe	fu.exe variants	98295	70	3.629	0.000	9	9fa75cb229f69e2bc8f7dd5213224a2f	1	2/19/2010 6:23:05 AM	2/19/2010 6:11:59 AM	False
ACMEXP2	cscript.exe	fu_original.exe	fu.exe variants	98304	24	3.758	0.129	0	ea04ad67501587f2c018e79b6b541224	2	8/4/2004 12:00:00 PM	8/4/2004 12:00:00 PM	False
ACMEXP1	cscript.exe	fu_original.exe	fu.exe variants	98304	24	3.758	0.129	0	ea04ad67501587f2c018e79b6b541224	2	8/4/2004 12:00:00 PM	8/4/2004 12:00:00 PM	False

TARGETED CONTAINMENT AND REMEDIATION

- Remote Process Kill
- Remote File Wipe
- Remote Registry Key Deletion



Alter endpoint state remotely and discreetly, without reboot, to contain threats and remediate them.

POLICY

THANK YOU

Yasser Anter

Solutions Consultant, Guidance Software

yasser.anter@guid.com