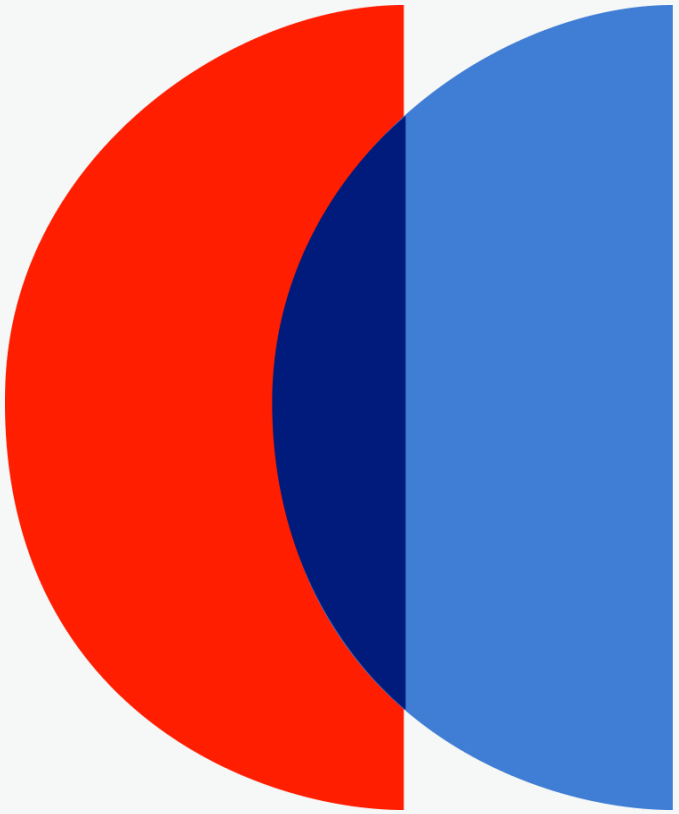


遊走紅隊與藍隊：Purple Man 我的超人

Walking around between Red Team and Blue Team – Purple Man, My Superman

Cymetrics Zet

Copyright ©2023 OneDegree Global Limited. All rights reserved.

Cymetrics

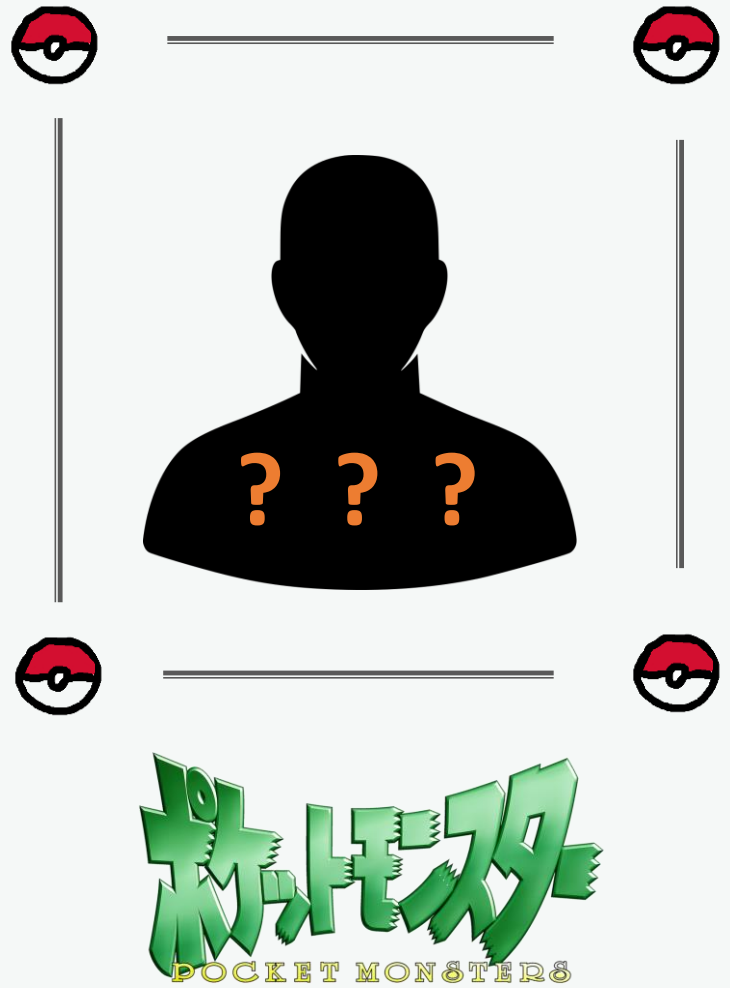
我是誰?

Zet

Security Researcher / Engineer
Cyber Security 10+ years

Interested:

- Defense Evasion
- Endpoint Threat Detection
- Malware Techniques
- IoT Vulnerability



tech-blog.cymetrics.io

linktr.ee/zet235

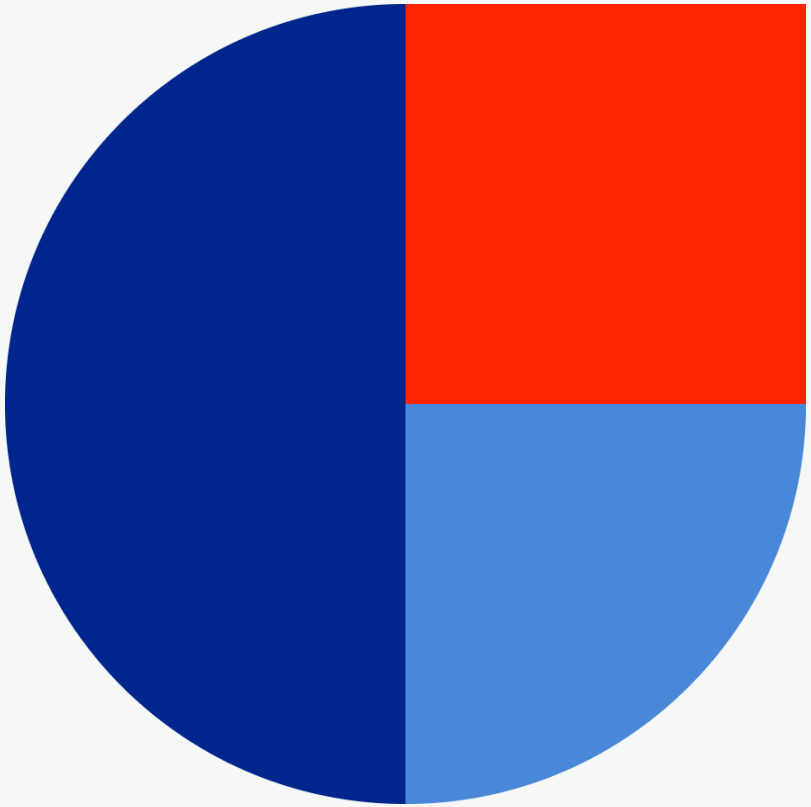
Copyright ©2023 OneDegree Global Limited. All rights reserved.

Cymetrics

OUTLINE

1. 紅藍隊實驗環境
2. 工具整合
3. 紅藍隊技術
4. 學習方法與資源

Cymetrics



藍隊

可以在任何一個環節發現並**阻斷攻擊**

紅隊

用新穎的攻擊技術突破，組成 **Kill Chain**

Copyright ©2023 OneDegree Global Limited. All rights reserved.

Cymetrics

01

架設紅藍隊實驗環境

Cymetrics

自動化架設實驗環境

AutomatedLab

> On Hyper-V or Azure

.NET 4.7.1 (Windows PowerShell)

.NET Core 2+ (PowerShell 6+)

Supported products

This solution supports setting up virtual machines with the following.

1. Windows 7, 2008 R2, 8 / 8.1 and 2012 / 2012 R2, 10 / 2016, 2019, 2022
2. SQL Server 2008, 2008R2, 2012, 2014, 2016, 2017, 2019 *more*
3. Visual Studio 2012, 2013, 2015, 2017 *more*
4. Team Foundation Services 2015+
5. Azure DevOps *more*
6. Exchange 2013, 2016, 2019
7. SharePoint 2013, 2016, 2019
8. System Center Orchestrator 2012
9. System Center Configuration Manager 1809 or 1902+
10. System Center Operations Manager
11. System Center Virtual Machine Manager
12. Microsoft Deployment Toolkit (MDT) *more*
13. ProGet (Private PowerShell Gallery)
14. Office 2013, 2016
15. DSC Pull Server (with SQL Reporting) *more*
16. Hyper-V *more*
17. Failover Clustering *more*
18. Dynamics 365 *more*

Copyright ©2023 OneDegree Global Limited. All rights reserved.

```
New-LabDefinition -Name LabEx2013 -DefaultVirtualizationEngine HyperV

$PSDefaultParameterValues = @{
    'Add-LabMachineDefinition:DomainName'      = 'contoso.com'
    'Add-LabMachineDefinition:OperatingSystem' = 'Windows Server 2012 R2 Datacenter
(Server with a GUI)'
}
```

- `Add-LabMachineDefinition -Name Ex2013DC1 -Roles RootDC -Memory 1GB`

```
$role = Get-LabPostInstallationActivity -CustomRole Exchange2013 -Properties @{
OrganizationName = 'Test1' }
```

- `Add-LabMachineDefinition -Name Ex2013EX1 -Memory 4GB -PostInstallationActivity $role`

- `Add-LabMachineDefinition -Name Ex2013Client1 -OperatingSystem 'Windows 10 Pro' -Memory 1GB`

```
Install-Lab
Show-LabDeploymentSummary -Detailed
```

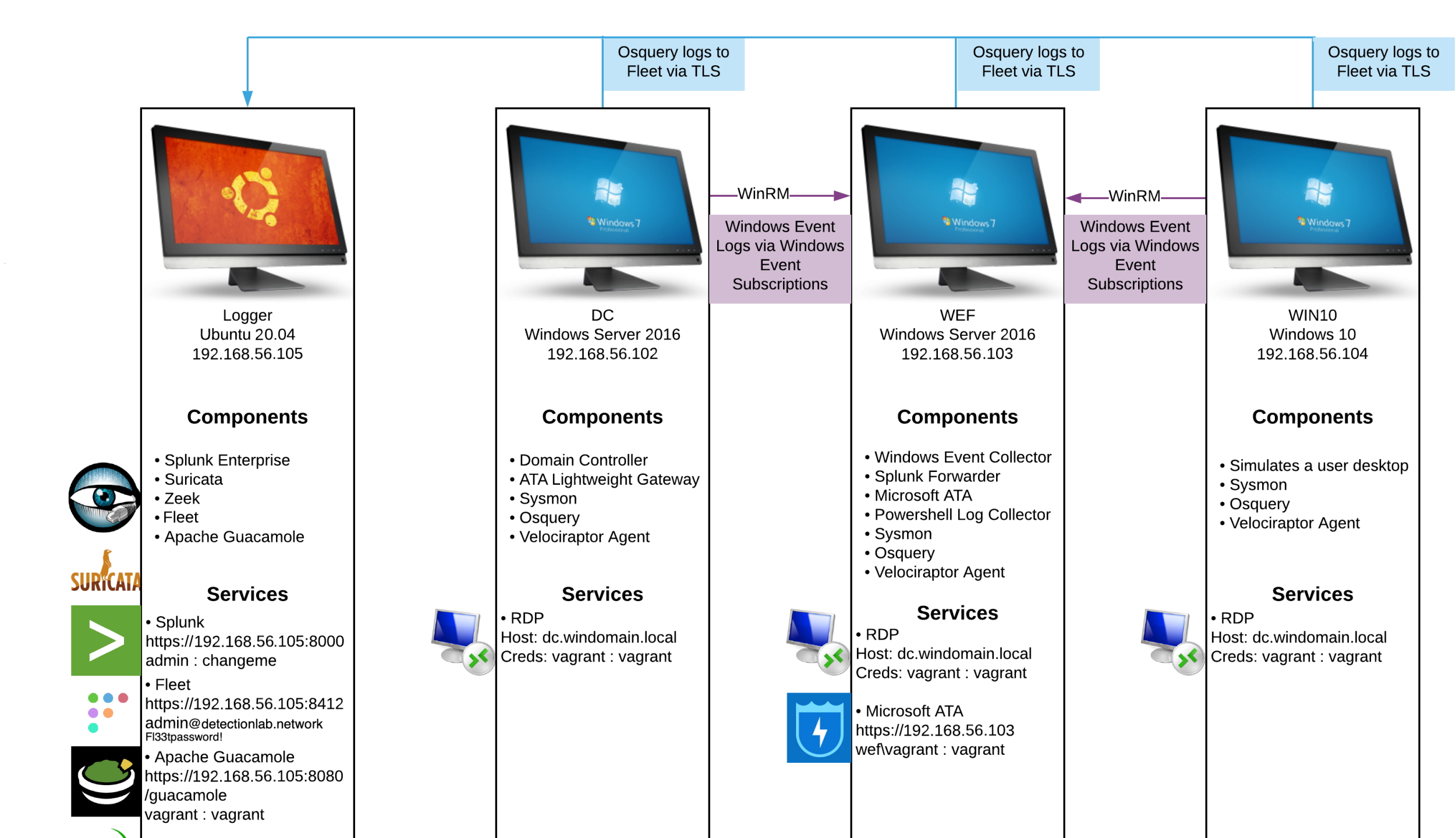
自動化架設實驗環境

Github: clong/DetectionLab

> VirtualBox, VMware Workstation, Hyper-V, AWS, Azure

- Microsoft Advanced Threat Analytics
- Splunk
- Osquery + Fleet
- Sysmon
- Zeek

Copyright ©2023 OneDegree Global Limited. All rights reserved.


Osquery logs to Fleet via TLS
Osquery logs to Fleet via TLS
Osquery logs to Fleet via TLS
WinRM
Windows Event Logs via Windows Event Subscriptions
WinRM
Windows Event Logs via Windows Event Subscriptions
Logger
Ubuntu 20.04
192.168.56.105
Components
• Splunk Enterprise
• Suricata
• Zeek
• Fleet
• Apache Guacamole
Services
• Splunk
https://192.168.56.105:8000
admin : changeme
• Fleet
https://192.168.56.105:8412
admin@detectionlab.network
Fl33tpassword!
• Apache Guacamole
https://192.168.56.105:8080
/guacamole
vagrant : vagrant
DC
Windows Server 2016
192.168.56.102
Components
• Domain Controller
• ATA Lightweight Gateway
• Sysmon
• Osquery
• Velociraptor Agent
Services
• RDP
Host: dc.windomain.local
Creds: vagrant : vagrant
WEF
Windows Server 2016
192.168.56.103
Components
• Windows Event Collector
• Splunk Forwarder
• Microsoft ATA
• Powershell Log Collector
• Sysmon
• Osquery
• Velociraptor Agent
Services
• RDP
Host: dc.windomain.local
Creds: vagrant : vagrant
• Microsoft ATA
https://192.168.56.103
wef\vagrant : vagrant
WIN10
Windows 10
192.168.56.104
Components
• Simulates a user desktop
• Sysmon
• Osquery
• Velociraptor Agent
Services
• RDP
Host: dc.windomain.local
Creds: vagrant : vagrant

02

工具整合

Cymetrics

自動化掃描整合 CI/CD

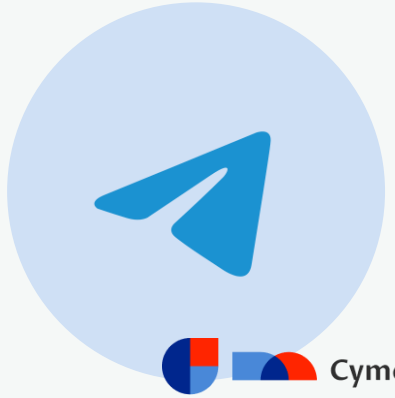
Host / URL Emulation

Scan

Tools Setup

Spider / Crawl and Analyze

Notify



Copyright ©202 gree Global Limited. All rights reserved.

Cymetrics

自動化掃描整合 CI/CD

Builds > #30 >

LOG VIEW | GRAPH VIEW

drone

adjust path env | zet pushed 57f727f4 to main

PIPELINE STAGES 1 stage

- scan 04:44
  - STEPS
    - clone 00:03
    - install 00:03
    - Ffuf 00:43
    - Nuclei 03:53

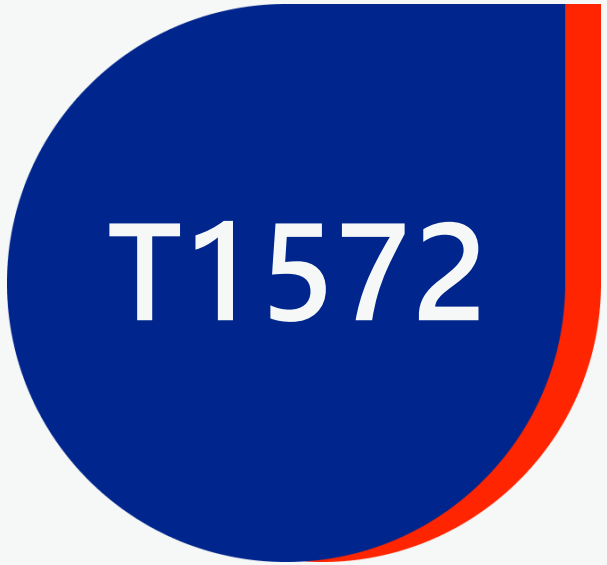
CONSOLE LOGS

```
+ export PATH=$PATH:/usr/local/go/bin:/root/go/bin
+ wget -q https://raw.githubusercontent.com/maurosoria/dirsearch/master/db/dicc.txt
+ wget -q https://raw.githubusercontent.com/ayoubfathi/leaky-paths/main/leaky-paths.txt
+ cat dicc.txt leaky-paths.txt > path.txt
+ ffuf -s -w ./path.txt -u $URL/FUZZ
FUZZ : .idea FFUFHASH : 1fe86268
FUZZ : .idea/ FFUFHASH : 1fe8626a
FFUFHASH : 1fe8626b FUZZ : .idea/.name
FUZZ : .idea/encodings.xml FFUFHASH : 1fe86277
FUZZ : .idea/misc.xml FFUFHASH : 1fe8627d
FUZZ : .idea/modules.xml FFUFHASH : 1fe8627f
FUZZ : .idea/scopes/scope_settings.xml FFUFHASH : 1fe86283
FUZZ : .idea/vcs.xml FFUFHASH : 1fe86288
FUZZ : .idea/workspace.xml FFUFHASH : 1fe86291
FUZZ : _mmServerScripts/ FFUFHASH : 1fe86718
```

03

紅藍隊技術與防禦

Cymetrics

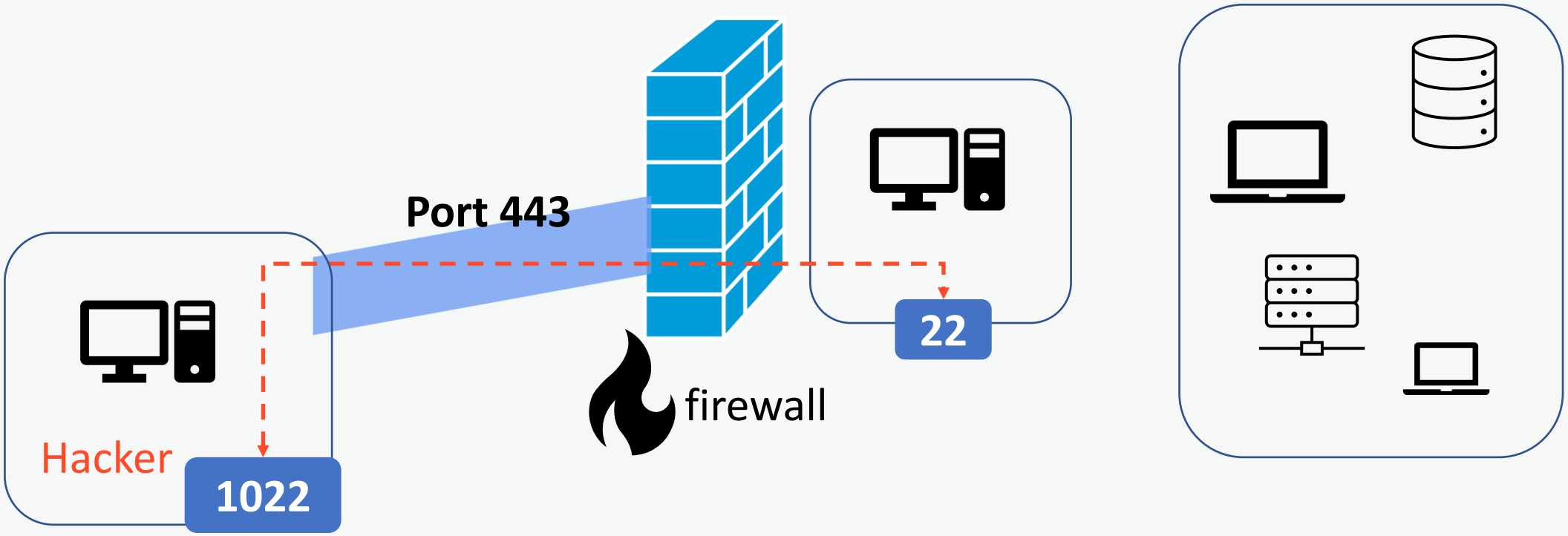


Tunneling

Copyright ©2023 OneDegree Global Limited. All rights reserved.

Cymetrics

Tunneling



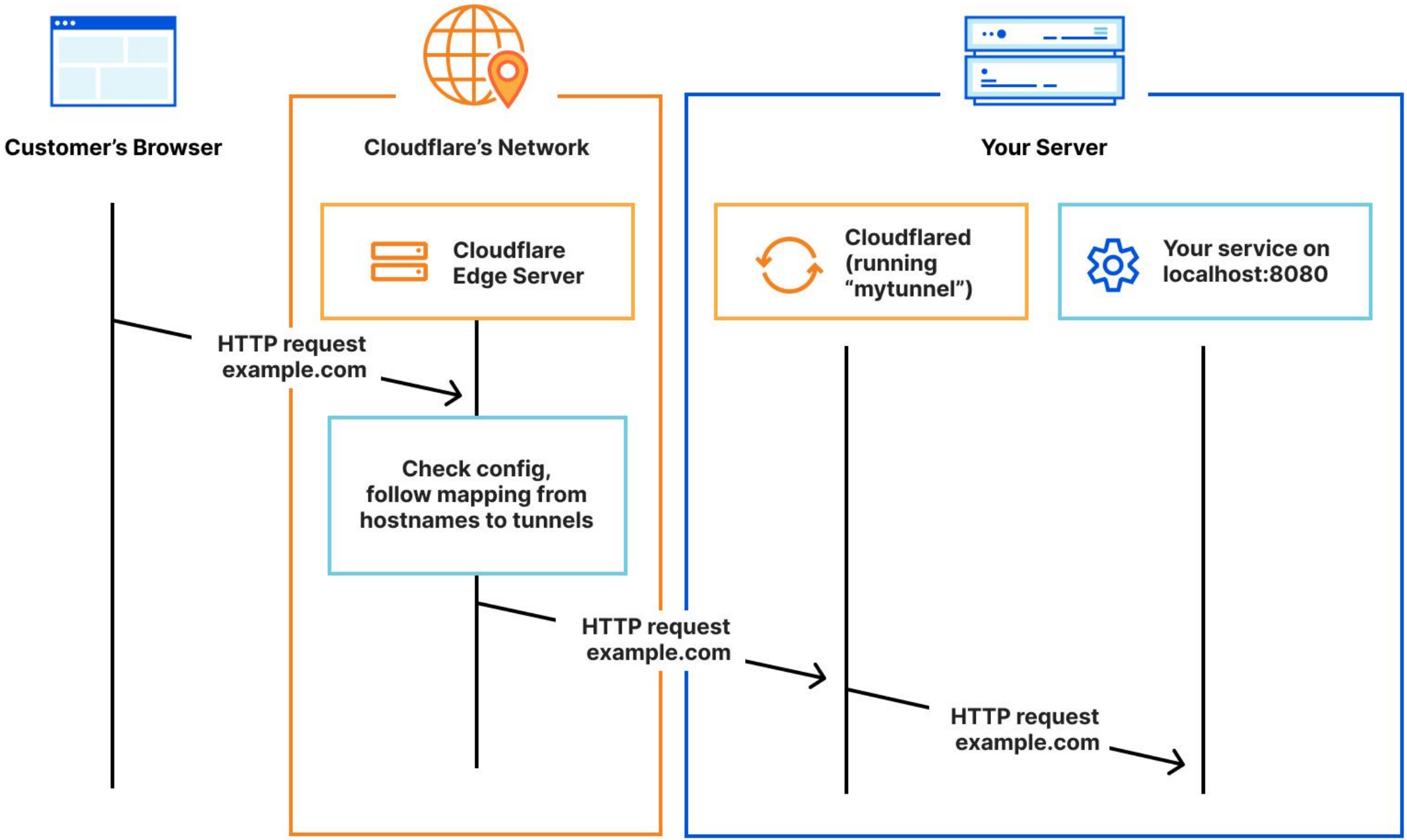
Copyright ©2023 OneDegree Global Limited. All rights reserved.

Tunnel and VPN

- Ngrok
- Cloudflared
- SoftEther
- Tailscale
- Headscale

Copyright ©2023 OneDegree Global Limited. All rights reserved.

Cymetrics


Customer's Browser
Cloudflare's Network
Your Server
Cloudflare Edge Server
Cloudflared (running "mytunnel")
Your service on localhost:8080
HTTP request example.com
Check config, follow mapping from hostnames to tunnels
HTTP request example.com
HTTP request example.com

CLOUDFLARE

[redacted]

Zero Trust overview

Analytics

Gateway

Access

- Applications
- Access Groups
- Service Auth
- **Tunnels**

My Team

Logs

← Back to tunnels

[redacted]

Overview | Public Hostname | Private Network

Private Network

+ Add a private network

#	CIDR

← Back to Profile

Manage Split Tunnels (exclude)

Configure Cloudflare Zero Trust to exclude or include traffic to a given set of IP addresses or domains. Any traffic directed to an excluded destination will be handled by the local machine. Use wildcards to match against multiple subdomains at the same time.
Learn more

Selector (Required)

IP Address

Value

192.0.2.0/24

Description (optional)

Example: additional info

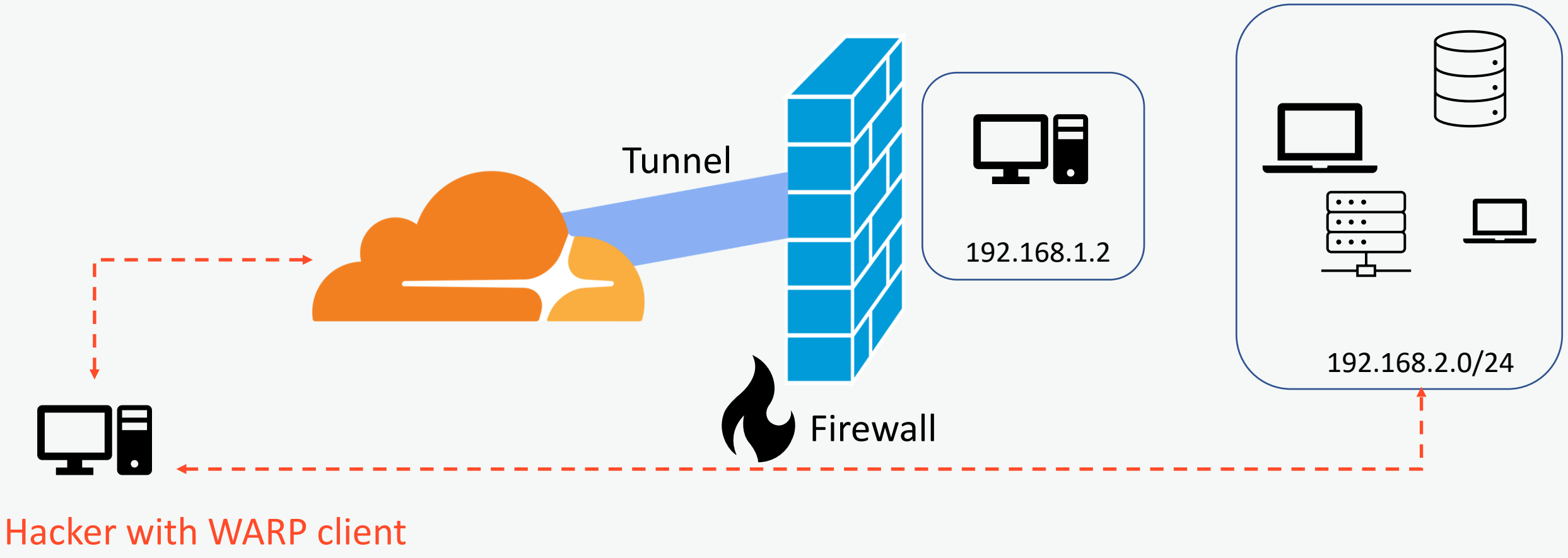
Save destination

Your Split Tunnel entries (exclude) *Showing 1-16 of 16*

View and manage the IPs and domains Cloudflare Zero Trust excludes.

Type ↑	Value
address	10.0.0.0/8
address	100.64.0.0/10
address	169.254.0.0/16
address	172.16.0.0/12
address	192.0.0.0/24
address	192.168.0.0/16
address	224.0.0.0/24
address	240.0.0.0/4
address	255.255.255.255/32
address	fe80::/10
address	fd00::/8

Cloudflare Tunnel



Copyright ©2023 OneDegree Global Limited. All rights reserved.


```
rule M_Hunting_Linux_VPNEngine_GenericSoftEther_1
{
    meta:
        author = "Mandiant"
        description = "Rule looks for SoftEther generic
terms in samples."
    strings:
        $domain = "update-check.softether-network.net"
ascii fullword
        $keepalive = "keepalive.softether.org"
        $vpn = "SoftEther Corporation" ascii fullword
    condition:
        filesize < 10MB and uint32(0) == 0x464c457f and
all of them
}
```

https://www.mandiant.com/resources/blog/burrowing-your-way-into-vpns

Cymetrics


```
detection:
    selectionDomain:
        urlMonitorEvent Hostname|contains:
            - 'get-my-ip.ddns.softether-network.net'
    filterProcessName:
        urlMonitorEvent Process|contains:
            - 'softether'
    condition: selectionDomain and not filterProcessName
fields:
    - "urlMonitorEvent Process"
    - "urlMonitorEvent Hostname"
    - "urlMonitorEvent Type"
    - "urlMonitorEvent Commandline"
level: "medium"
```

https://www.mandiant.com/resources/blog/burrowing-your-way-into-vpns

Cymetrics

Lateral Movement

Copyright ©2023 OneDegree Global Limited. All rights reserved.

Cymetrics

Lateral Movement

- **Impacket ： Implement your own tools**
  - PsExec
  - SMBExec
  - Atexec
- **CrackMapExec：support Credentials, Kerberos, module, BloodHound**
  - Enumerate
  - Password spraying
  - Command execution
  - SMB, LDAP, WINRM, MSSQL, SSH …

Copyright ©2023 OneDegree Global Limited. All rights reserved.

```
class RemoteShell(cmd.Cmd):

    def __init__(self, share, rpc, mode, serviceName, shell_type):
        cmd.Cmd.__init__(self)
        self.__share = share
        self.__mode = mode
        self.__output = '\\\\%COMPUTERNAME%\\' + self.__share + '\\' +
    OUTPUT_FILENAME
        self.__outputBuffer = b''
        self.__command = ''
        self.__shell = '%COMSPEC% /Q /c '
        self.__shell_type = shell_type
        self.__pwsh =
            'powershell.exe -NoP -NoL -sta -NonI -W Hidden -Exec Bypass -Enc '
        self.__serviceName = serviceName
        self.__rpc = rpc
        self.intro = '[!] Launching semi-interactive shell - Careful what you
    execute'
```

```
def execute_remote(self, data, shell_type='cmd'):

if shell_type == 'powershell':
    data = '$ProgressPreference="SilentlyContinue";' + data
    data = self.__pwsh + b64encode(data.encode('utf-16le')).decode()

    batchFile = '%SYSTEMROOT%\\' + \
        ''.join([random.choice(string.ascii_letters) for _ in range(8)]) +
'.bat'

    command = self.__shell + 'echo ' + data + ' ^> ' + \
              self.__output + ' 2^>^&1 > ' + batchFile + ' & ' + \
              self.__shell + batchFile
```

橫向移動攻擊的偵測與防禦

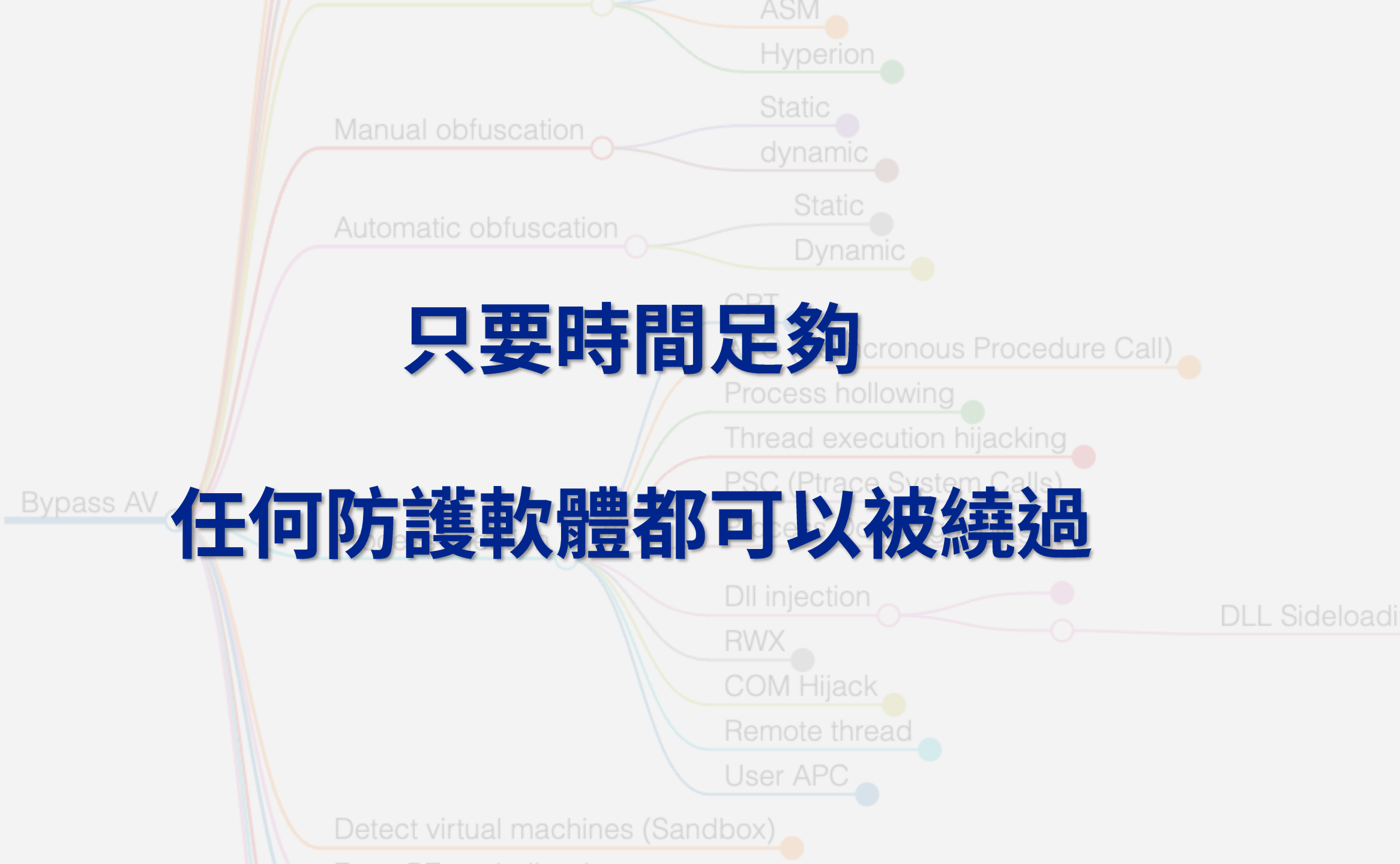
- **建置告警系統**
- **設置陷阱**
  - 資料夾 (HoneyShare)
  - 帳號 (HoneyUser)
- **網路流量分析 Network Traffic Analysis**

Cymetrics

Command-and-Control (C&C)

Copyright ©2023 OneDegree Global Limited. All rights reserved.

Cymetrics



只要時間足夠

任何防護軟體都可以被繞過

防護軟體

- **Pattern-based**
  - Web WAF
  - Antivirus
- **Behavior-based**
  - EDR
- **Indicators of Compromise (IOCs)**

Copyright ©2023 OneDegree Global Limited. All rights reserved.

Command-and-Control (C&C) Techniques

- **Kill Process(Logger, EDR)**
- **Unhook**
- **Syscall**
  - HellsGate / indirect syscalls
- **PowerShell**
  - Cobalt Strike powerpick
- **Disable AMSI, ETW, Event Log**

Copyright ©2023 OneDegree Global Limited. All rights reserved.

擁有多樣化的 Loader, Packer

大幅減少繞過防護軟體的時間

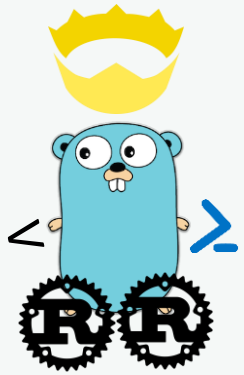
甚至有 SaaS 服務

```
options:
  -h, --help            show this help messa
  -p explorer.exe, --process explorer.exe
                        Process to inject in
  -m QueueUserAPC, --method QueueUserAPC
                        Method for shellcode
                        RemoteThreadContext,
  -u, --unhook          Unhook NTDLL in curr
  -w, --word-encode     Save shellcode in st
  -nr, --no-randomize   Disable syscall name
  -ns, --no-sandbox     Disable sandbox chec
  -l, --llvm-obfuscator
                        Use Obfuscator-LLVM
  -v, --verbose         Enable debugging mes
  -sc GetSyscallStub, --syscall GetSyscallSt
                        Syscall execution me
  -d, --dll             Generate a DLL inste
  -dp apphelp.dll, --dll-proxy apphelp.dll
                        Create Proxy DLL usi
  -s domain, --sandbox domain
                        Sandbox evasion tech
  -sa testlab.local, --sandbox-arg testlab.l
                        Argument for sandbox
  -o a.exe, --outfile a.exe
                        Name of compiled fil
```

利用各種語言實現

Offensive

C#
Nim
PowerShell
Python
Go
Rust
V



shellcode_bin.nim	Creates a suspended process and injects shellcode with VirtualAllocEx/CreateRemoteThread. Also demonstrates the usage of compile time definitions to detect arch, os etc..
minidump_bin.nim	Creates a memory dump of lsass using MiniDumpWriteDump
keylogger_bin.nim	Keylogger using SetWindowsHookEx
uuid_exec_bin.nim	Plants shellcode from UUID array into heap space and uses EnumSystemLocalesA Callback in order to execute the shellcode.

Copyright ©2023 OneDegree Global Limited. All rights reserved.

Embedded

- **Interpreter**
- **Lua**
- **.NET Assemblies**

```go
package main

import (
    "github.com/traefik/yaegi/interp"
    "github.com/traefik/yaegi/stdlib"
)

func main() {
    i := interp.New(interp.Options{})

    i.Use(stdlib.Symbols)

    _, err := i.Eval(`import "fmt"`)
    if err != nil {
        panic(err)
    }

    _, err = i.Eval(`fmt.Println("Hello Yaegi")`)
    if err != nil {
        panic(err)
    }
}
```

Copyright ©2023 OneDegree Global Limited. All rights reserved.

Threat Hunting

- YARA
- Sigma
- Elasticsearch Event Query Language
- Timeline Explorer
- Open Source / Free Scanner

Cymetrics

elastic/detection-rules

```
risk_score = 47
rule_id = "6aace640-e631-4870-ba8e-5fdda09325db"
severity = "medium"
tags = ["Elastic", "Host", "Windows", "Threat Detection"]
timestamp_override = "event.ingested"
type = "eql"

query = '''
process where host.os.type == “windows” and
event.type == "start" and
process.name: ("powershell.exe", "pwsh.exe") and
process.command_line : ("*MailboxExportRequest*")
'''
```

Eric Zimmerman/Timeline Explorer + Yamato-Security/hayabusa

Time	Computername	Eventid	Level	Alert	Details
2021-05-22 05:43:18.227 +09:00	fs01.offsec.lan	4648	informational	Explicit Logon	Source User: FS01$: Target User: admmig
2021-05-22 05:43:22.562 +09:00	fs01.offsec.lan	4625	low	Logon Failure - Wrong Password	User: admmig@offsec.lan : Type: 8 : Wor
2021-05-22 05:43:49.345 +09:00	fs01.offsec.lan	4625	low	Logon Failure - Wrong Password	User: admmig@offsec.lan : Type: 8 : Wor
2021-05-22 05:43:50.131 +09:00	fs01.offsec.lan	4625	low	Logon Failure - Wrong Password	User: admmig@offsec.lan : Type: 8 : Wor
2021-05-22 05:43:50.607 +09:00	fs01.offsec.lan	4625	low	Logon Failure - Wrong Password	User: admmig@offsec.lan : Type: 8 : Wor
2021-05-22 05:43:50.866 +09:00	fs01.offsec.lan	4625	low	Logon Failure - Wrong Password	User: admmig@offsec.lan : Type: 8 : Wor
2021-05-23 06:56:57.685 +09:00	fs01.offsec.lan	1102	high	Security log was cleared	User: admmig
2021-05-23 06:57:11.842 +09:00	fs01.offsec.lan	4688	high	Relevant Anti-Virus Event	
2021-05-23 06:57:11.842 +09:00	fs01.offsec.lan	4688	critical	Mimikatz Use	
2021-05-26 22:02:27.149 +09:00	mssql01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Addr
2021-05-26 22:02:27.155 +09:00	mssql01.offsec.lan	5145	medium	DCERPC SMB Spoolss Named Pipe	
2021-05-26 22:02:27.155 +09:00	mssql01.offsec.lan	5145	critical	CVE-2021-1675 Print Spooler Exploitation IPC Access	
2021-05-26 22:02:29.726 +09:00	mssql01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Addr
2021-05-26 22:02:29.734 +09:00	mssql01.offsec.lan	5145	medium	DCERPC SMB Spoolss Named Pipe	
2021-05-26 22:02:29.734 +09:00	mssql01.offsec.lan	5145	critical	CVE-2021-1675 Print Spooler Exploitation IPC Access	
2021-05-26 22:02:34.373 +09:00	mssql01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Addr
2021-05-26 22:02:34.375 +09:00	mssql01.offsec.lan	5145	medium	DCERPC SMB Spoolss Named Pipe	
2021-05-26 22:02:34.379 +09:00	mssql01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Addr
2021-05-26 22:02:34.379 +09:00	mssql01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Addr
2021-05-26 22:02:34.380 +09:00	mssql01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Addr
2021-05-27 05:24:46.570 +09:00	rootdc1.offsec.lan	4768	medium	Possible AS-REP Roasting	Possible AS-REP Roasting
2021-05-27 05:24:46.570 +09:00	rootdc1.offsec.lan	4768	informational	Kerberos TGT was requested	User: admin-test : Service: krbtgt : IP
2021-06-01 23:06:34.542 +09:00	fs01.offsec.lan	4720	medium	Local user account created	User: WADGUtilityAccount : SID:S-1-5-21-1
2021-06-01 23:08:21.225 +09:00	fs01.offsec.lan	4720	medium	Local user account created	User: elie : SID:S-1-5-21-1081258321-3780
2021-06-03 21:17:56.988 +09:00	fs01.offsec.lan	1102	high	Security log was cleared	User: admmig
2021-06-03 21:18:12.941 +09:00	fs01.offsec.lan	4672	informational	Admin Logon	User: admmig : LogonID: 0x322e5b7
2021-06-03 21:18:12.942 +09:00	fs01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Addr
2021-06-04 03:34:12.672 +09:00	fs01.offsec.lan	4104	high	Windows Firewall Profile Disabled	
2021-06-04 04:17:44.873 +09:00	fs01.offsec.lan	1102	high	Security log was cleared	User: admmig

Thor lite

Scan Information

[redacted]	0	4	2	678	1
[redacted]	0	17	7	1108	1
[redacted]	0	13	83	1190	1
[redacted]	0	4	2	689	1
[redacted]	0	260	11	935	1
[redacted]	0	9	2	1325	1
[redacted]	0	14	2	1312	1
[redacted]	0	260	11	935	1
[redacted]	0	22	2	905	1
[redacted]	0	326	4	700	2
[redacted]	0	4	5	873	1
[redacted]	0	126	8	726	2
[redacted]	0	257	2	849	1
DC01	0	271	11	942	1
DC02	0	256	11	929	1
DC03	2	452	386	925	1
01	0	280	19	1605	2

Modules

Autoruns	8
Filescan	178
LogScan	3058
ProcessCheck	102
ProcessConnections	0
ProcessIntegrity	261
RuntimeWatcher	0

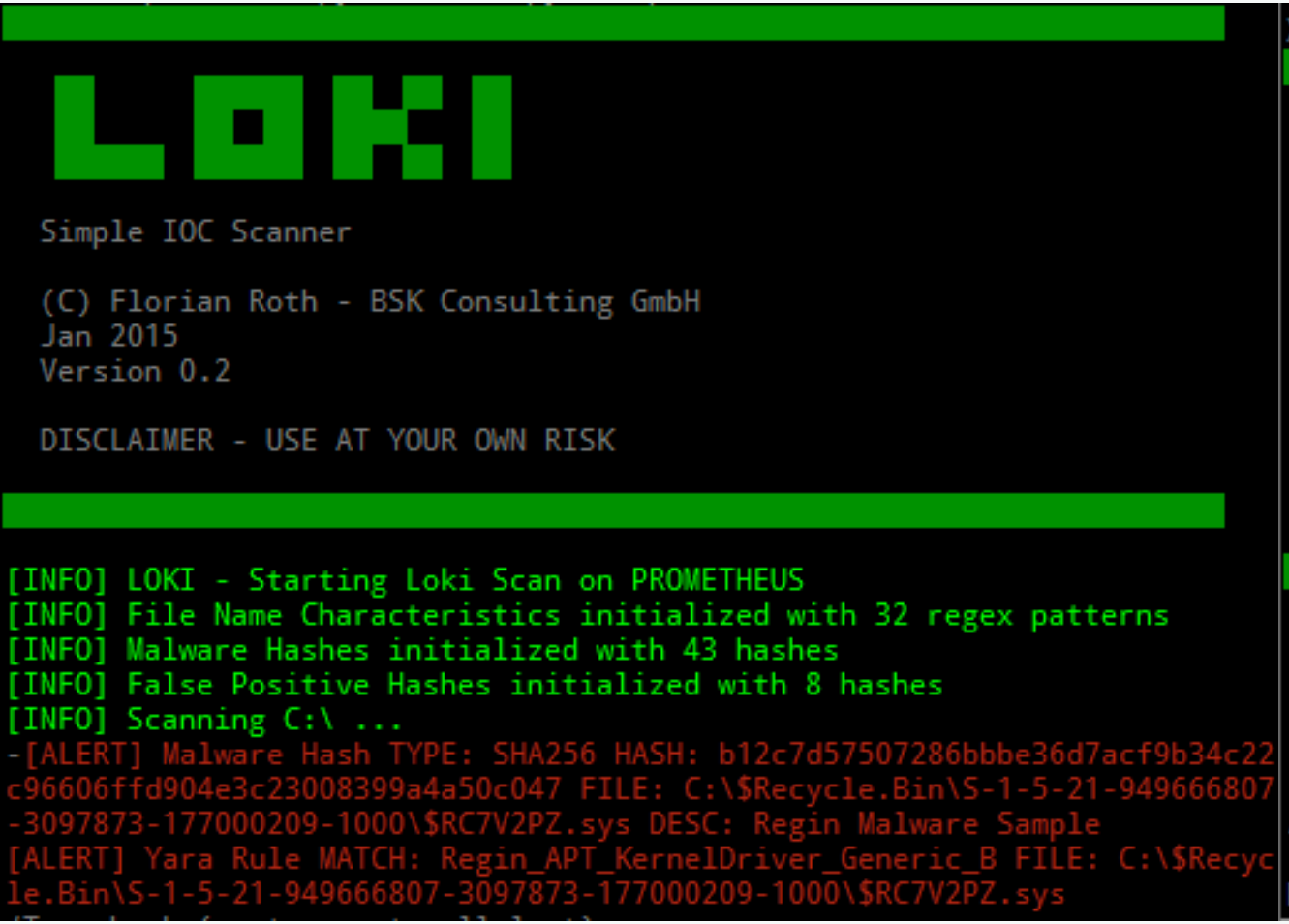
Statistics

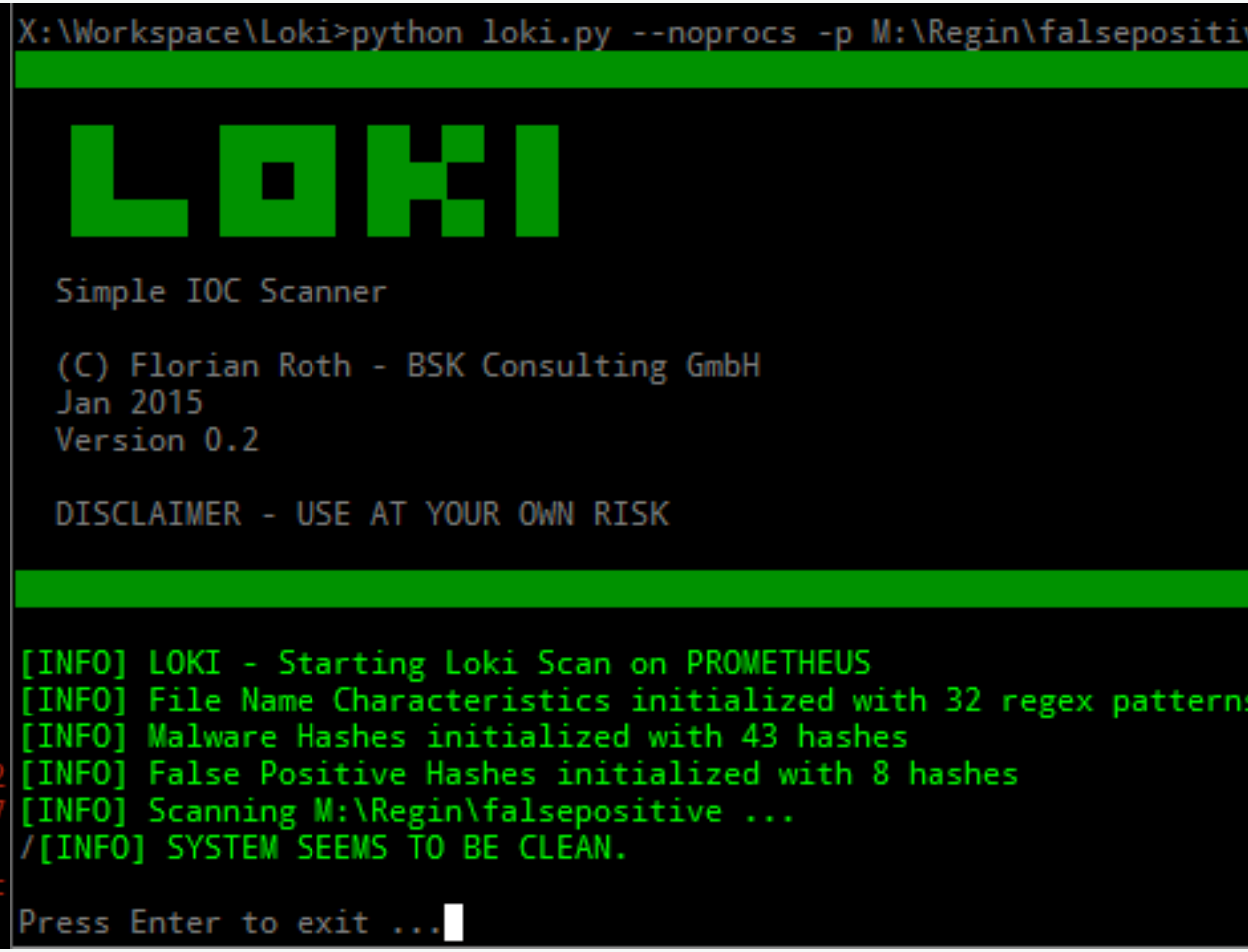
Alerts	2
Warnings	2987
Notice	674
Info	29202
Errors	36

Help

Shortcuts	Use Ctrl+⬆ (Windows/Linux) or ⌘+⬆ (macOS) to return to the top of the page
Filters	You can provide a file (--filter file) with regular expressions to suppress false positives
Hint 1	Select text and use the context menu to filter / select / lookup strings

Loki


LOKI
Simple IOC Scanner
(C) Florian Roth - BSK Consulting GmbH
Jan 2015
Version 0.2
DISCLAIMER - USE AT YOUR OWN RISK
[INFO] LOKI - Starting Loki Scan on PROMETHEUS
[INFO] File Name Characteristics initialized with 32 regex patterns
[INFO] Malware Hashes initialized with 43 hashes
[INFO] False Positive Hashes initialized with 8 hashes
[INFO] Scanning C:\ ...
-[ALERT] Malware Hash TYPE: SHA256 HASH: b12c7d57507286bbbe36d7acf9b34c22c96606ffd904e3c23008399a4a50c047 FILE: C:\$Recycle.Bin\S-1-5-21-949666807-3097873-177000209-1000\$RC7V2PZ.sys DESC: Regin Malware Sample
[ALERT] Yara Rule MATCH: Regin_APT_KernelDriver_Generic_B FILE: C:\$Recycle.Bin\S-1-5-21-949666807-3097873-177000209-1000\$RC7V2PZ.sys


X:\Workspace\Loki>python loki.py --noprocs -p M:\Regin\falsepositi
LOKI
Simple IOC Scanner
(C) Florian Roth - BSK Consulting GmbH
Jan 2015
Version 0.2
DISCLAIMER - USE AT YOUR OWN RISK
[INFO] LOKI - Starting Loki Scan on PROMETHEUS
[INFO] File Name Characteristics initialized with 32 regex patterns
[INFO] Malware Hashes initialized with 43 hashes
[INFO] False Positive Hashes initialized with 8 hashes
[INFO] Scanning M:\Regin\falsepositive ...
/[INFO] SYSTEM SEEMS TO BE CLEAN.
Press Enter to exit ...

藍隊的一些小建議

- 資產盤點
- 可以聯網的裝置，盡可能的更新上 patch
  - Router, Switch, IoT, Printer, Endpoint
- 架設 Log Server，Log 盡量搜集完整
  - Firewall, Endpoint, Server
- 定期弱點掃描與滲透測試，DevSecOps 規劃
- 訂閱產品弱點與情資，了解相關手法與知識

Cymetrics

對於 **藍隊**

紅隊 是 **工具** 用於驗證與發現問題

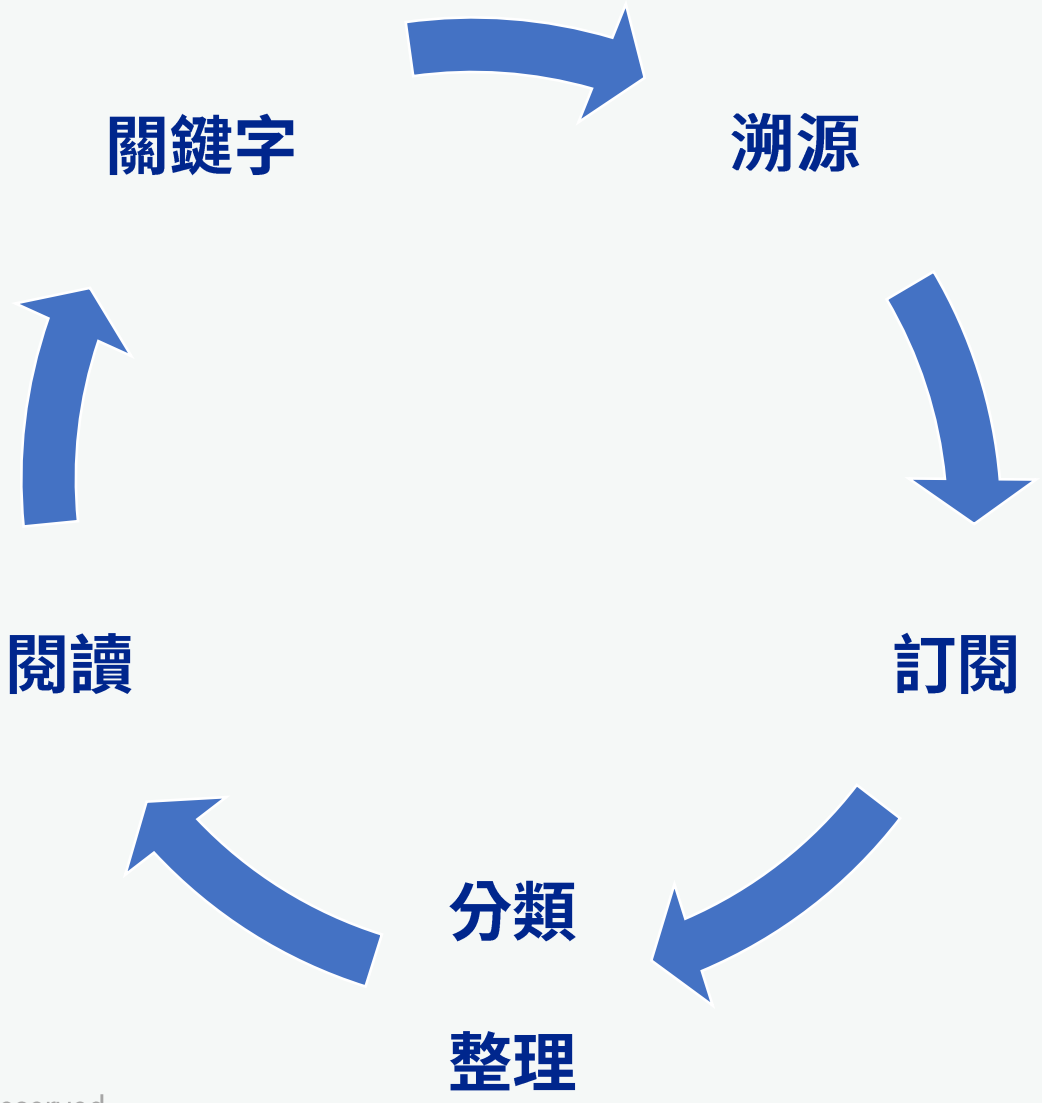
Cymetrics

04

如何有效學習資訊安全技術

Cymetrics

有效學習方式

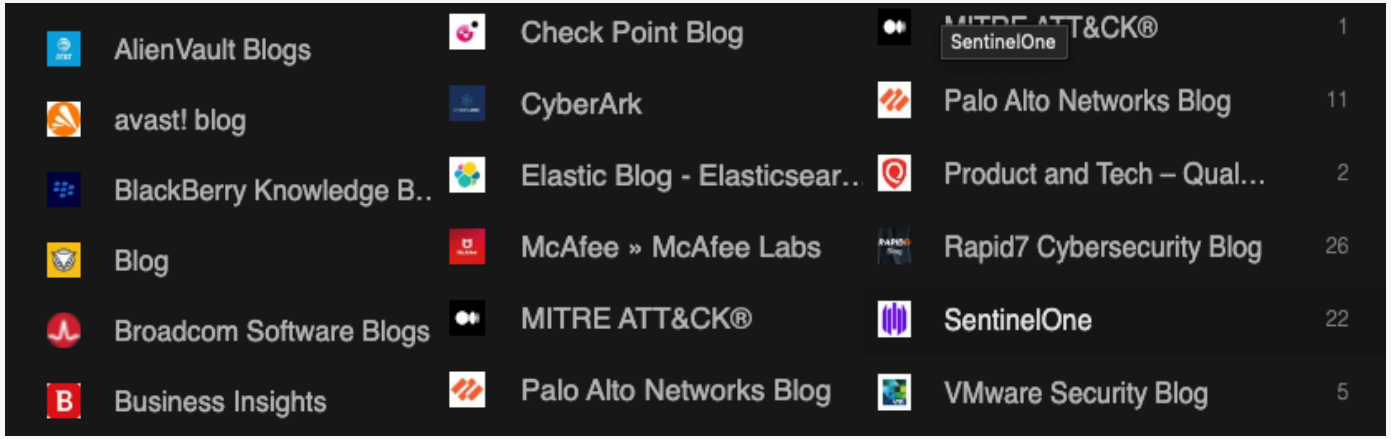


Copyright ©2023 OneDegree Global Limited. All rights reserved.

Cymetrics

RSS 訂閱

- TVN, Exploit Database, ZDI
- 有去參加 MITRE ATT&CK 評比的訂閱一輪
  - Gartner 觀察相似公司
- Reddit, 社團, 論壇, Youtube



Copyright ©2023 OneDegree Global Limited. All rights reserved.

Cymetrics

資訊安全

資訊安全 | Metasploit | Wireshark | Penetration-test 滲透測試 | kali-linux

資訊安全

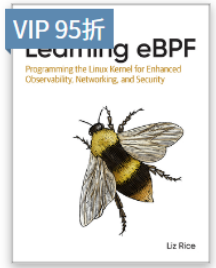
讚 1 分享

相關書籍

排序： 銷售排行 出版日期 語系： 繁中 簡中 英文 全部 庫存： 可立即出貨 可購買商品 特價商品

~~$880~~ **$695**

親密的駭人 – 堅固網



~~$1,930~~ **$1,834**

Learning eBPF: Programming the

~~$480~~ **$379**

加密・解謎・密碼學：從歷史發展到關

~~$1,340~~ **$1,273**

IoT and OT Security Handbook: Assess

~~$1,490~~ **$1,416**

Azure Security Cookbook: Practical

~~$880~~ **$695**

駭客就在你旁邊：內網安全攻防滲透

www.tenlong.com.tw

ZERO POINT SECURITY

SWAG COURSES LABS SIGN IN

All Courses, Red Team Courses

Red Team Ops II

★★★★★ (18)

88 Lessons | £399.00

All Courses, Programming Courses

C2 Development in C#

★★★★★ (19)

28 Lessons | £52.29

All Courses, Programming Courses

Offensive Driver Development

★★★★★ (4)

36 Lessons | £52.29

‹ 1 2 ›

sektor7 institute

Login

$199

RED TEAM Operator: Malware Development Essentials Course

A course on becoming a better ethical hacker, pentester and red teamer by learning offensive security tools development in Windows.

View product

$229

RED TEAM Operator: Malware Development Intermediate Course

More advanced offensive security tools (OST) development techniques in Windows, including: API hooking, 32-/64-bit migrations, reflective binaries and more.

View product

PentesterAcademy | Courses and Online Labs

Follow @SecurityTube

COURSES | LABS | PRICING | WHY SUBSCRIBE | TESTIMONIALS | BOOTCAMPS | ENTERPRISE SECURITY LABS | GET STARTED

Our Online Labs and Course Library:

Video Courses | 2000+ Live Online Labs

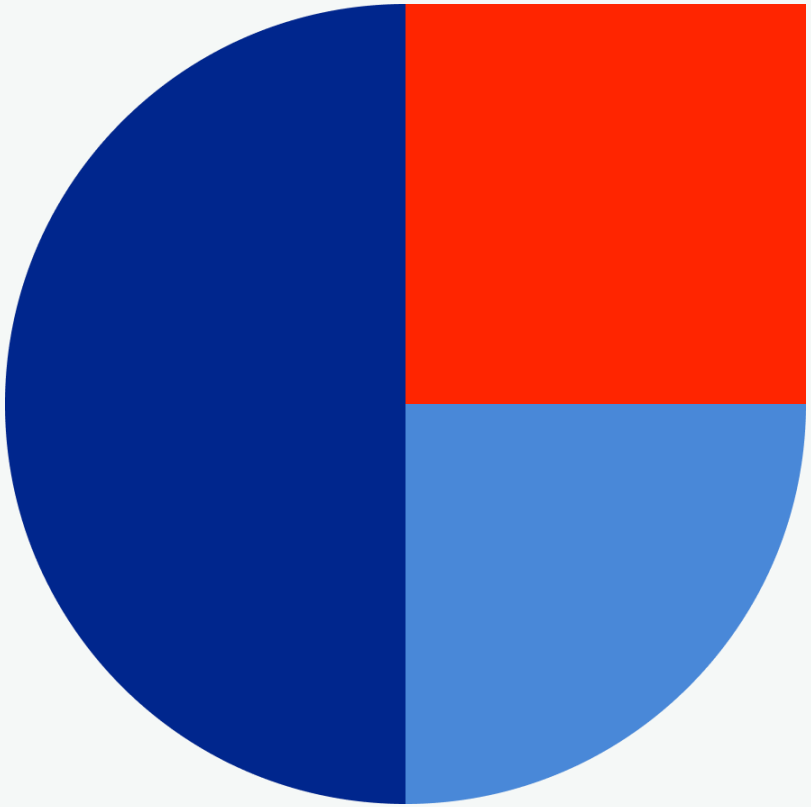
Python for Pentesters

This course will teach you Python scripting and its application to problems in computer and network security. This course is ideal for penetration testers, security enthusiasts and network administrat...

View Details

Windows Process Injection for Red-Blue Teams

In this course, we will understand the basics of Windows processes, virtual memory and different techniques to enumerate processes. Then we will look at the fundamentals of process injection and tr...



藍隊

在學習紅隊的攻擊手法後，在面對發生的威脅可以更快的掌握情況

紅隊

知道藍隊如何偵測可以聰明的規避

Copyright ©2023 OneDegree Global Limited. All rights reserved.

Cymetrics

Cymetrics 攤位 C258

Cymetrics

Q & A

ask@cymetrics.io

Cymetrics