

```
root@hacklab:~/parte-02/lezione-15
```

ETHICAL HACKING POTENZIATO DALL'IA // PARTE II

LEZIONE 15

Cyber Threat Intelligence e OSINT avanzato

Conoscere l'avversario: intelligence sulle minacce e OSINT investigativo a supporto di difesa e red team.

docente **Vincenzo Calabro** fase Specializzazione: Cyber Threat Intelligence

```
root@hacklab:~/lezione-15/agenda $
```

LEZIONE 15 / AGENDA

In questa lezione

// PERCORSO

- > Livelli di CTI e ciclo dell'intelligence
- > IOC, TTP e piramide del dolore
- > Threat sharing (MISP, STIX/TAXII)
- > OSINT avanzato e dark web
- > Attribuzione e bias

metodo obiettivi -> teoria -> strumenti -> laboratorio -> caso di studio -> etica -> verifica

```
root@hacklab:~/lezione-15/obiettivi $
```

LEZIONE 15 / OBIETTIVI

Obiettivi di apprendimento

// AL TERMINE SAPRAI (TASSONOMIA DI BLOOM)

- > Comprendere – livelli di CTI e ciclo dell'intelligence
- > Applicare – raccogliere e condividere IOC e TTP
- > Analizzare – le TTP di un attore su MITRE ATT&CK
- > Valutare – affidabilità delle fonti e attribuzione
- > Creare – un report di threat intelligence

```
root@hacklab:~/lezione-15/inquadramento $
```

LEZIONE 15 / INQUADRAMENTO

Inquadramento

// DI COSA PARLIAMO

Trasformare dati grezzi in intelligence azionabile guida prioritaria e difese. La lezione struttura il ciclo di Cyber Threat Intelligence, l'attribuzione prudente e l'uso di framework come MITRE ATT&CK.

// PERCHE' CONTA

Conoscere l'avversario: intelligence sulle minacce e OSINT investigativo a supporto di difesa e red team.

```
root@hacklab:~/lezione-15/mappa-insieme $
```

LEZIONE 15 / MAPPA // INSIEME

Mappa d'insieme del modulo

■ Attacco/tecnica ■ Difesa ■ Norme & metodo ■ IA

FONDAMENTI

- 01 Livelli di CTI e piramide del dolore
- 02 Modelli e condivisione dell'intelligence
- 03 OSINT avanzato e pivoting
- 04 Attribuzione e bias
- 05 IA per aggregazione e correlazione

APPROFONDIMENTI

- 06 Diamond Model e Kill Chain
- 07 Qualità e scadenza degli IOC
- 08 Pivoting su infrastruttura
- 09 False flag e limiti
- 10 IA nell'analisi di intelligence

```
root@hacklab:~/lezione-15/flusso-1 $
```

LEZIONE 15 / FLUSSO // FONDAMENTI

Sequenza di fasi – Fondamenti

■ Attacco/tecnica ■ Difesa ■ Norme & metodo ■ IA



> Le fasi si susseguono: l'esito di ciascuna alimenta la successiva.

```
root@hacklab:~/lezione-15/concetto-1 $
```

LEZIONE 15 / CONCETTO 1/10

[Attacco/tecnica]

Livelli di CTI e piramide del dolore

// SPIEGAZIONE

La threat intelligence si declina su tre livelli: strategica per i decisori, operativa sulle campagne, tattica sugli indicatori. La piramide del dolore ordina gli indicatori per quanto costa all'avversario cambiarli: colpire le TTP fa piu male che bloccare un hash.

// ESEMPIO

> Bloccare un hash e banale per l'attaccante; cambiargli le TTP e molto piu costoso.

```
root@hacklab:~/lezione-15/concetto-2 $
```

LEZIONE 15 / CONCETTO 2/10

[Norme & metodo]

Modelli e condivisione dell'intelligence

// SPIEGAZIONE

Diamond Model, Cyber Kill Chain e MITRE ATT&CK offrono quadri per analizzare gli attacchi; MISP e gli standard STIX/TAXII permettono di scambiare intelligence in modo strutturato tra organizzazioni e CERT.

// ESEMPIO

> Un indicatore condiviso in STIX via TAXII si integra automaticamente nel MISP ricevente.

```
root@hacklab:~/lezione-15/concetto-3 $
```

LEZIONE 15 / CONCETTO 3/10

[Attacco/tecnica]

OSINT avanzato e pivoting

// SPIEGAZIONE

Il pivoting collega entita a partire da un indicatore: da un dominio a certificati, IP, registranti e infrastrutture correlate. Esteso a fonti chiuse e dark web, ricostruisce l'infrastruttura di un attore oltre il singolo IOC.

// ESEMPIO

> Da un certificato TLS riutilizzato si scoprono altri domini della stessa campagna.

```
root@hacklab:~/lezione-15/concetto-4 $
```

LEZIONE 15 / CONCETTO 4/10

[Attacco/tecnica]

Attribuzione e bias

// SPIEGAZIONE

Attribuire un attacco è difficile e rischioso: gli indizi possono essere depistaggi (false flag) e l'analista è esposto a bias di conferma. L'attribuzione prudente distingue i fatti dalle ipotesi e dichiara sempre il livello di confidenza.

// ESEMPIO

> Stringhe in una certa lingua nel malware possono essere inserite apposta per depistare.

```
root@hacklab:~/lezione-15/concetto-5 $
```

LEZIONE 15 / CONCETTO 5/10

[Attacco/tecnica]

IA per aggregazione e correlazione

// SPIEGAZIONE

Sui grandi volumi di dati di intelligence l'IA aiuta a raccogliere e correlare, proponendo collegamenti tra eventi e attori. I legami vanno verificati: un'associazione sbagliata produce attribuzioni e priorità errate.

// ESEMPIO

> Il modello raggruppa campagne per TTP simili; l'analista conferma con prove indipendenti.

```
root@hacklab:~/lezione-15/flusso-2 $
```

LEZIONE 15 / FLUSSO // APPROFONDIMENTI

Sequenza di fasi – Approfondimenti

■ Attacco/tecnica ■ Difesa ■ Norme & metodo ■ IA



> Le fasi si susseguono: l'esito di ciascuna alimenta la successiva.

```
root@hacklab:~/lezione-15/concetto-6 $
```

LEZIONE 15 / CONCETTO 6/10

[Difesa]

Diamond Model e Kill Chain

// SPIEGAZIONE

Il Diamond Model lega avversario, capacita, infrastruttura e vittima; la Kill Chain scompone l'attacco in fasi sequenziali. Usati insieme aiutano a capire chi, come e dove intervenire per spezzare la catena.

// ESEMPIO

> Interrompere la fase di delivery blocca l'attacco prima dell'exploitation.

```
root@hacklab:~/lezione-15/concetto-7 $
```

LEZIONE 15 / CONCETTO 7/10

[Attacco/tecnica]

Qualita e scadenza degli IOC

// SPIEGAZIONE

Gli indicatori invecchiano: un IP malevolo oggi domani puo essere riassegnato. Un buon feed valuta affidabilita, contesto e scadenza, altrimenti genera falsi positivi e alert inutili. La qualita conta piu della quantita.

// ESEMPIO

> Un IOC senza data e contesto rischia di bloccare traffico ormai legittimo.

```
root@hacklab:~/lezione-15/concetto-8 $
```

LEZIONE 15 / CONCETTO 8/10

[Difesa]

Pivoting su infrastruttura

// SPIEGAZIONE

Partendo da un singolo artefatto si espande la conoscenza dell'infrastruttura avversaria: domini registrati insieme, certificati condivisi, IP riusati. Il pivoting trasforma un indizio isolato in una mappa di campagna.

// ESEMPIO

> Stesso registrante e stesso name server collegano dieci domini a un unico attore.

```
root@hacklab:~/lezione-15/concetto-9 $
```

LEZIONE 15 / CONCETTO 9/10

[Attacco/tecnica]

False flag e limiti

// SPIEGAZIONE

Gli attori sofisticati impiantano prove fuorvianti per attribuire l'attacco ad altri. Per questo l'attribuzione tecnica va accompagnata da cautela, confidenza dichiarata e, quando conta davvero, da fonti non solo tecniche.

// ESEMPIO

> Riuso deliberato degli strumenti di un altro gruppo per farne ricadere la colpa.

```
root@hacklab:~/lezione-15/concetto-10 $
```

LEZIONE 15 / CONCETTO 10/10

[Attacco/tecnica]

IA nell'analisi di intelligence

// SPIEGAZIONE

Su volumi enormi l'IA individua pattern e connessioni che sfuggirebbero, ma non comprende il contesto geopolitico ne pesa la confidenza come un analista. Resta un acceleratore, non il giudice finale dell'attribuzione.

// ESEMPIO

> L'IA segnala una possibile correlazione tra due campagne; l'analista valuta se regge.

```
root@hacklab:~/lezione-15/strumenti $
```

LEZIONE 15 / STRUMENTI

Strumenti della lezione

// TOOLKIT

MISP

OpenCTI

Maltego

STIX/TAXII

dark web monitoring

VirusTotal

// NOTA OPERATIVA

> Ogni strumento si usa in ambiente virtualizzato e isolato, solo su bersagli di proprietà o autorizzati. Output e artefatti vanno protetti e, a fine ingaggio, gestiti o distrutti.

```
root@hacklab:~/lezione-15/lab-1 $
```

LEZIONE 15 / LABORATORIO 1

Laboratorio 1

\$ Profilo di un threat actor (TTP -> ATT&CK, MISP)

// PROCEDURA

[1] Estrai IOC e TTP da un report

[2] mappali su ATT&CK e registrati in MISP

[!] Verifica: Perché gli IOC in cima alla piramide del dolore sono più preziosi?

```
root@hacklab:~/lezione-15/lab-2 $
```

LEZIONE 15 / LABORATORIO 2

Laboratorio 2

\$ Pivoting infrastrutturale (domini/certificati/IP)

// PROCEDURA

[1] Pivota da un indicatore per ricostruire l'infrastruttura di una campagna

[!] Verifica: Quali bias minacciano un'attribuzione?

```
root@hacklab:~/lezione-15/caso-di-studio $
```

LEZIONE 15 / CASO DI STUDIO

Caso di studio

// SCENARIO

> Ricostruzione CTI delle TTP di un APT noto (es. la catena SolarWinds).

// ANALISI RICHIESTA

- > Ricostruisci la dinamica dei fatti con metodo e tracciabilità
- > Individua errori, cause radice e punti di decisione critici
- > Proponi contromisure, controlli e lezioni apprese

```
root@hacklab:~/lezione-15/etica $
```

LEZIONE 15 / ETICA & DIRITTO

Nota etico-legale

// PRINCIPI INDEROGABILI

> autorizzazione scritta scope definito ambiente isolato dati protetti responsible disclosure

// SPECIFICO DELLA LEZIONE

[!] Dark web e OSINT su persone con cautela legale e GDPR; nessuna interazione con marketplace illeciti.

```
root@hacklab:~/lezione-15/ricapitolazione $
```

LEZIONE 15 / RICAPITOLAZIONE

Ricapitolazione

// PUNTI CHIAVE

- > Livelli di CTI e ciclo dell'intelligence
- > Raccogliere e condividere IOC e TTP
- > Le TTP di un attore su MITRE ATT&CK
- > Affidabilità delle fonti e attribuzione
- > Un report di threat intelligence

```
root@hacklab:~/lezione-15/verifica $
```

LEZIONE 15 / AUTOVALUTAZIONE

Autovalutazione

// DOMANDE DI VERIFICA

- ? Perché gli IOC in cima alla piramide del dolore sono più preziosi?
- ? Quali bias minacciano un'attribuzione?
- ? Come si valuta l'affidabilità di una fonte?

// VALUTAZIONE

Report di CTI su un attore (rigore, mappatura ATT&CK, fonti).

// LETTURE

MITRE ATT&CK; doc. MISP; paper del Diamond Model.

lezione 15 completata

\$ next

Cyber Threat Intelligence e OSINT avanzato

[!] Le competenze di questa lezione si impiegano esclusivamente in contesti legali, autorizzati e deontologicamente corretti, entro lo scope e con autorizzazione scritta.

root@hacklab:~# _

```
root@hacklab:~/contatti $
```

CONTATTI / RISORSE

Restiamo in contatto

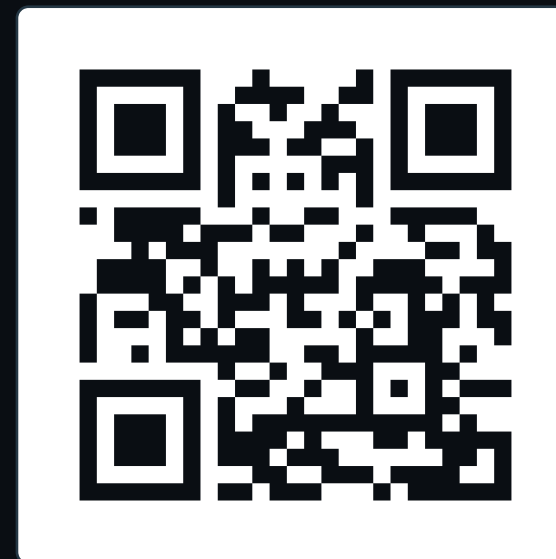


Vincenzo Calabro

cyber security / digital forensics /
docenza e divulgazione

// SCANSIONA O VISITA

> vincenzocalabro.it



Inquadra il QR con la fotocamera
per aprire il sito.