
# Cyber Threat Intelligence e Threat Hunting nel settore dell'energia

## CSP006_S_E

PRESENTAZIONE DA PARTE DI:
DR. STEFAN SCHAUER
DR. ABDELKADER SHAABAN
**AIT ISTITUTO AUSTRIACO DI TECNOLOGIA**


# Riconoscimento


- *Co-finanziato dall'Unione Europea. I punti di vista e le opinioni espresse sono tuttavia esclusivamente quelli dell'autore o degli autori e non riflettono necessariamente quelli dell'Unione Europea o di HADEA. Né l'Unione Europea né l'autorità che ha concesso il finanziamento possono essere ritenute responsabili.*
- *Accordo di progetto n. 101083594*

# Cyber Threat Intelligence e Threat Hunting nel settore dell'energia

## Panoramica

- Argomento-1: Introduzione all'intelligence delle minacce e alla caccia alle minacce
- Argomento-2: Fonti e raccolta dei dati
- Argomento 3: Attori e tattiche di minaccia
- Argomento 4: Modellazione pratica delle minacce e indagini sulla sicurezza

# Ordine del giorno

01. Che cos'è la modellazione delle minacce

02. Metodi di modellazione delle minacce

03. Analisi delle minacce

04. MinacciaVenere

05. Pratico: ThreatGet

# Obiettivi

Al termine di questo modulo, i partecipanti dovrebbero essere in grado :

1. Panoramica dei diversi metodi di modellazione delle minacce.
2. Capire che pensare come un attaccante può migliorare le vostre difese di sicurezza informatica.
3. Spiegare la "kill chain" e come utilizzarla per anticipare gli attacchi e difendere una rete.
4. Descrivere le minacce in base alle tattiche, alle tecniche e alle procedure utilizzate per attaccare.
5. Identificare come le caratteristiche delle minacce possono informare la pianificazione della sicurezza informatica.

# Cos'è la modellazione delle minacce

# Modellazione delle minacce

- La modellazione delle minacce è un elemento costitutivo dell'ingegneria della sicurezza che identifica le minacce potenziali definire le relative mitigazioni in diversi domini industriali.

- Con la modellazione delle minacce, una rappresentazione della sicurezza viene applicata alla rappresentazione di un sistema. per identificare potenziali problemi di sicurezza

  - I metodi di modellazione delle minacce vengono utilizzati per creare
    - un'astrazione del sistema
    - i profili dei potenziali aggressori, compresi i loro obiettivi e i loro metodi
    - un catalogo di potenziali minacce che possono sorgere

# Metodi di modellazione delle minacce

# Panoramica

- STRISCIA
- Il processo di simulazione degli attacchi e analisi delle minacce (PASTA)
- LINDDUN (collegabilità, identificabilità, non ripudio, rilevabilità, divulgazione di informazioni, inconsapevolezza, non conformità)
- Sistema comune di valutazione delle vulnerabilità (CVSS)
- Alberi da attacco
- Persona Non Grata (PnG)
- Pubblicazione speciale NIST 800-154
- Carte di sicurezza
- Metodo ibrido di modellazione delle minacce (hTMM)
- Metodo di modellazione quantitativa delle minacce (Quantitative TMM)
- Trike
- Modellazione visiva, agile e semplice delle minacce (VAST)
- Valutazione delle minacce, degli asset e delle vulnerabilità critiche dal punto di vista operativo (OCTAVE´)



https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/

# Panoramica

- Inventato nel 1999 e adottato da Microsoft nel 2002
- il metodo di modellazione delle minacce più maturo
- tabelle specifiche per le minacce
- le varianti STRIDE-per-elemento e STRIDE-per-Interazione.

| | Threat | Property Violated | Threat Definition |
|---|---|---|---|
| S | Spoofing identify | Authentication | Pretending to be something or someone other than yourself |
| T | Tampering with data | Integrity | Modifying something on disk, network, memory, or elsewhere |
| R | Repudiation | Non-repudiation | Claiming that you didn't do something or were not responsible; can be honest or false |
| I | Information disclosure | Confidentiality | Providing information to someone not authorized to access it |
| D | Denial of service | Availability | Exhausting resources needed to provide service |
| E | Elevation of privilege | Authorization | Allowing someone to do something they are not authorized to do |

https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/

# STRISCIA

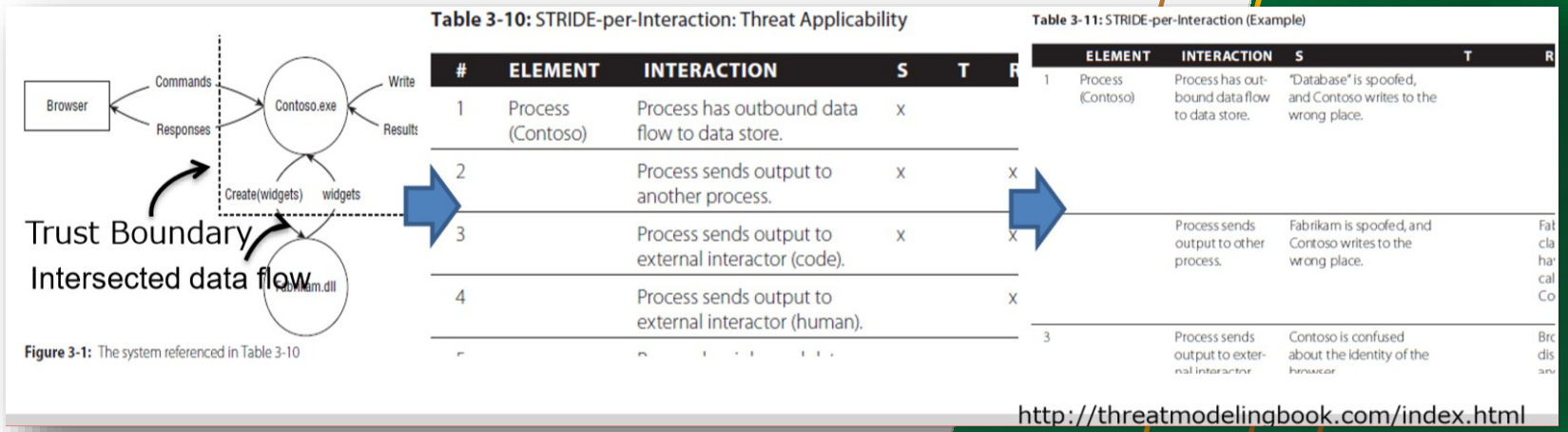
- Inventato nel 1999 e adottato da Microsoft nel 2002
- il metodo di modellazione delle minacce più maturo
- tabelle specifiche per le minacce
  - varianti **STRIDE-per-elemento** e STRIDE-per-interazione.

| | S | T | R | I | D | E |
|---|---|---|---|---|---|---|
| External Entity | ✓ | | ✓ | | | |
| Process | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Data Flow | | ✓ | | ✓ | ✓ | |
| Data Store | | ✓ | ? | ✓ | ✓ | |

https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/

# STRISCIA

- Inventato nel 1999 e adottato da Microsoft nel 2002
- il metodo di modellazione delle minacce più maturo
- tabelle specifiche per le minacce
  - varianti STRIDE-per-elemento e **STRIDE-per-interazione**.




http://threatmodelingbook.com/index.html

https://insights.sei.carnegie.edu/blog/threat-modeling-12-available-methods/

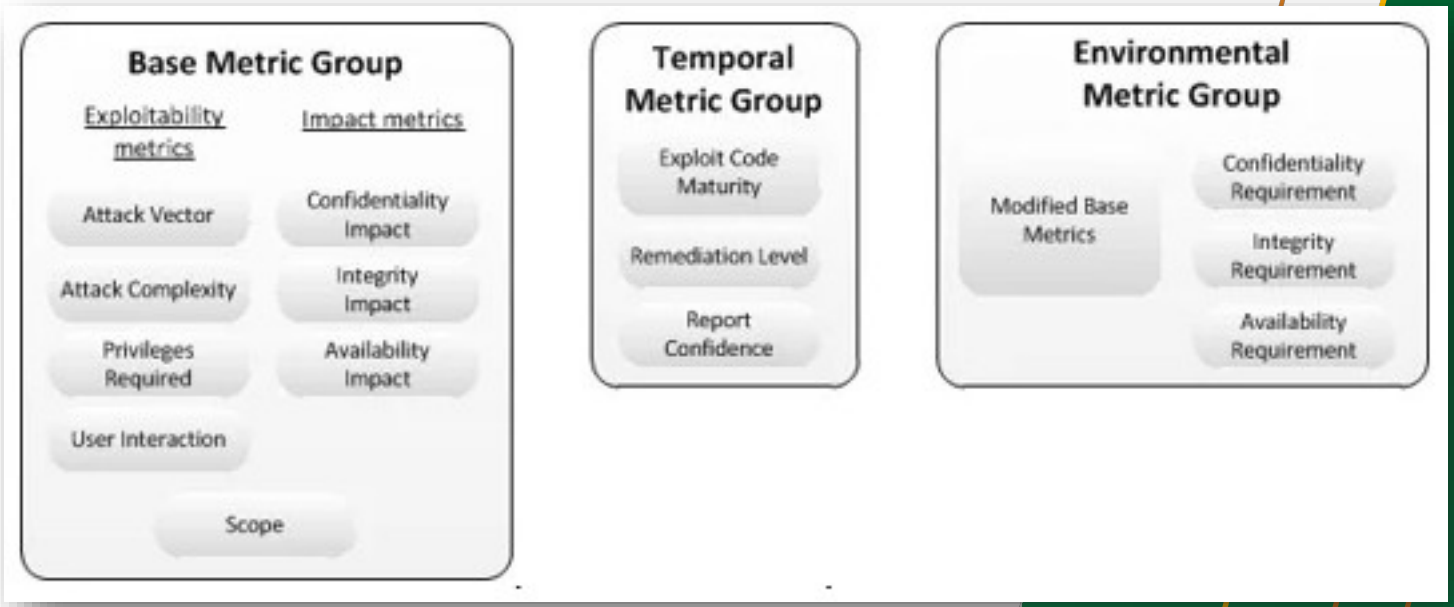
# Processo di simulazione degli attacchi e analisi delle minacce (PASTA)

- Processo di simulazione degli attacchi e analisi delle minacce (PASTA)
- Quadro di modellazione delle minacce incentrato sul rischio
- Combinare obiettivi aziendali e requisiti tecnici
- Richiedere l'input di sicurezza da parte delle operazioni, governance, architettura e sviluppo.


https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/

# Il sistema comune di valutazione delle vulnerabilità (CVSS)

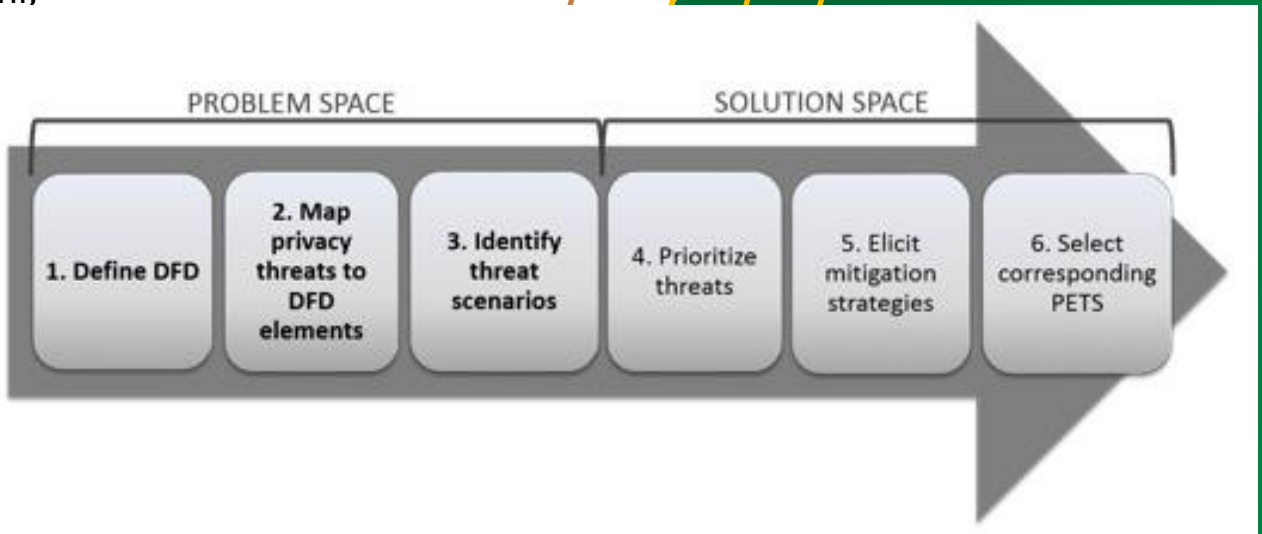
- cattura le caratteristiche di una vulnerabilità
- produce un punteggio numerico di gravità




https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/

# LINDDUN

- LINDDUN (collegabilità, identificabilità, non ripudiabilità, rilevabilità, divulgazione di informazioni, inconsapevolezza, non conformità
- Si concentra sulla privacy
- Può essere utilizzato per la sicurezza dei dati

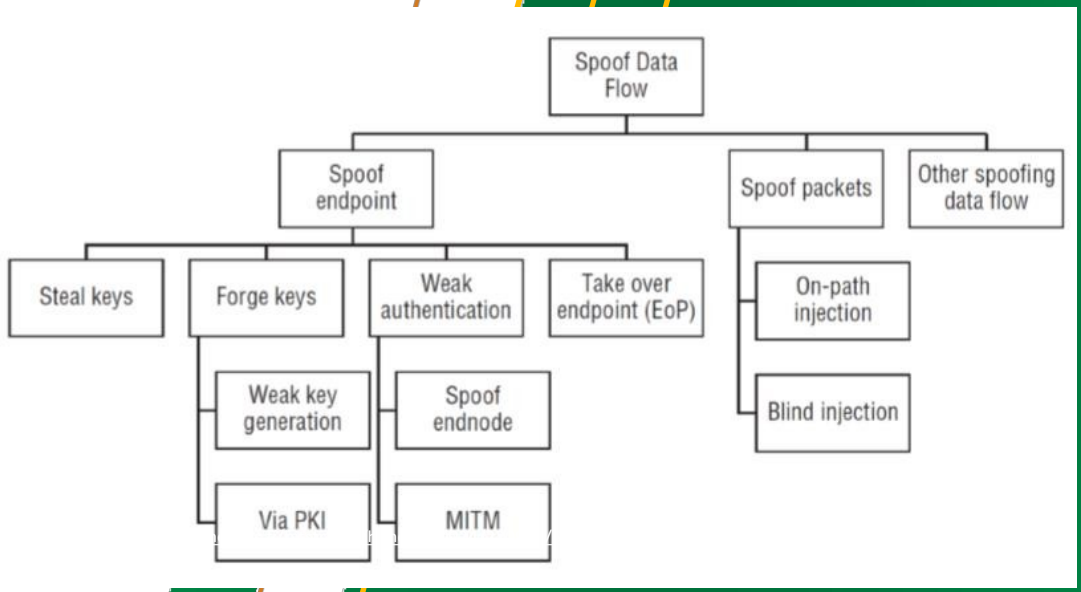





https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/

# Alberi da attacco

- Diagrammi che raffigurano gli attacchi a un sistema ad albero
- La radice dell'albero è l'obiettivo dell'attacco
- Le foglie sono un modo per raggiungere questo obiettivo
- Può essere utilizzato in combinazione con altre tecniche come STRIDE, CVSS o PASTA.




https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/

# Persona non grata

- Guardare il sistema da un punto di vista di uso non intenzionale
- può essere utile prime fasi di sviluppo della
- esaminare le capacità e le motivazioni dell'attaccante, e obiettivi

**Description:** Mike worked as a contractor installing SCADA radio-controlled sewage equipment for a municipal authority. After leaving the contractor, Mike applied for a job with the municipality but was rebuffed. Feeling bitter and rejected, Mike decides to get even with the municipality and his former employer.

**Goals:** Cause raw sewage to leak into local parks and rivers and make the events appear as malfunctions. Create a public backlash against the contractor and municipality.

"Mike" is based on the true story of Vitek Boden, who was convicted of causing the release of sewage in Maroochy Shire Council in Queensland, Australia in 2000 after hacking the associated SCADA system. See Abrams & Weiss, 2008.



https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/

# Pubblicazione speciale NIST 800-154

- Modellazione delle minacce dei sistemi incentrati sui dati
- Concentrarsi sulla protezione di particolari tipi di dati all'interno dei sistemi




https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/

# Carte di sicurezza

tecnica di brainstorming

Set di carte

- Chi potrebbe attaccare?
- Perché il sistema potrebbe essere attaccato?
- Quali sono gli asset di interesse?
- Come possono essere attuati questi attacchi?




https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/

# Metodo ibrido di modellazione delle minacce (hTMM)

| | |
|---|---|
| **Identificare** | Identificare il sistema da modellare in base alle minacce. |
| **Applicare** | Applicare le carte di sicurezza in base ai suggerimenti degli sviluppatori. |
| **Rimuovere** | Eliminare i PnG improbabili (cioè, non ci sono vettori di attacco realistici). |
| **Riassumere** | Riassumere i risultati utilizzando il supporto dello strumento. |
| **Continua** | Continuare con un metodo formale di valutazione del rischio |





https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/

# Metodo di modellazione quantitativa delle minacce

Alberi di attacco, STRIDE e metodi CVSS

applicato in sinergia

costruire alberi di attacco dei componenti per le cinque categorie di minacce di STRIDE

dipendenze tra le categorie di attacco e gli attributi dei componenti di basso livello

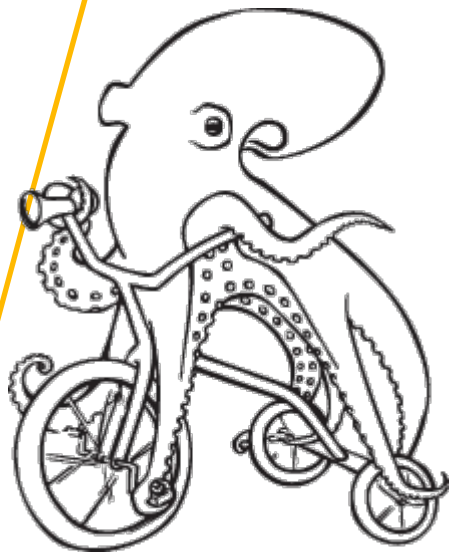
Metodo CVSS per calcolare i punteggi dei componenti dell'albero





https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/

# Trike



- Il framework di audit della sicurezza che utilizza la modellazione delle minacce come tecnica
- **Versione 1**
  - generazione automatica di minacce a livello di requisiti
  - generazione automatica di alberi di attacco.
- **Versione**
  - ponte intermedio tra la versione 1 e la versione 2.
  - I punti salienti includono una migliore generazione automatica delle minacce a livello di requisiti, obiettivi di sicurezza, assenza totale di alberi delle minacce e analisi HAZOP.
- **Versione 2**
  - generazione semi-automatica di minacce a livello architettonico e concatenamento di attacchi.
  - La versione 2 è in fase di sviluppo attivo

https://insights.sei.carnegie.edu/blog/threat-modeling-12-available-methods/

# VASTO

- Modellazione visiva, agile e semplice delle minacce (VAST)
- Basato su ThreatModeler, una piattaforma di modellazione automatizzata delle minacce.
- Due tipi di modelli:
  - Modelli di minaccia per le applicazioni
    - Diagrammi di flusso dei processi, che rappresentano il punto di vista architettonico
  - Modelli di minaccia operativa
    - Punto di vista dell'attaccante basato sulle DFD

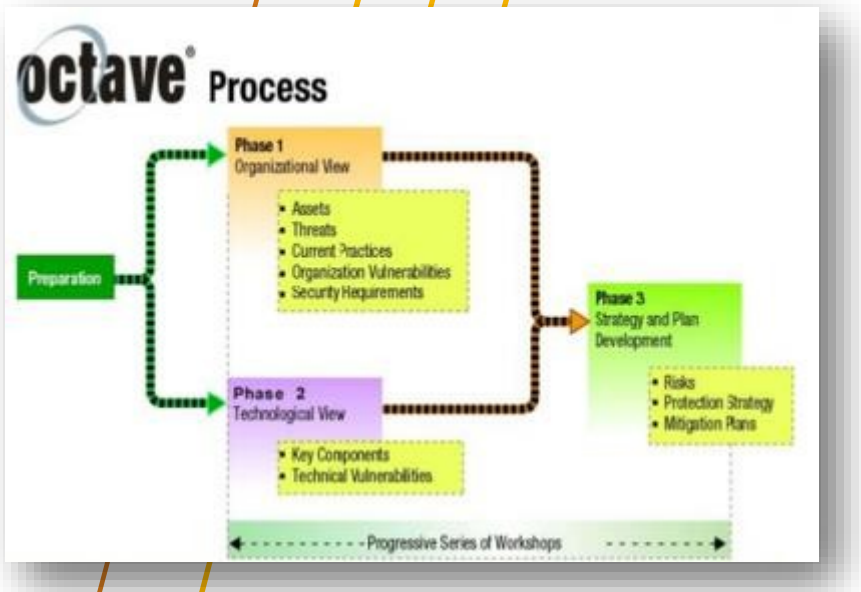




https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/

# OCTAVE

- Valutazione delle minacce, degli asset e delle vulnerabilità critiche a livello operativo (OCTAVE)
- Valutazione e pianificazione strategica basata sul rischio metodo per la sicurezza informatica
- Valutare i rischi organizzativi e non affrontare i rischi tecnologici
  - Creare profili di minaccia basati sulle risorse
  - Identificare la vulnerabilità dell'infrastruttura
  - Sviluppare una strategia e dei piani di sicurezza




https://insights.sei.carnegie.edu/blog/threat-modeling-12-available-methods/

# Analisi delle minacce

# Analisi delle minacce e ciclo di vita degli attacchi

- Le informazioni sulle minacce possono servire come base per costruire e selezionare le misure di sicurezza.

- Diverse tattiche, tecniche e procedure (TTP) potrebbero essere utilizzate contro obiettivi del settore energetico durante le varie fasi di un attacco informatico (o ciclo di vita dell'attacco).

**Minaccia e analisi della minaccia**

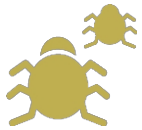
Come definiamo le minacce, gli attori delle minacce e come le analizziamo?

**Definizione del ciclo di vita dell'attacco**

La comprensione delle fasi di un attacco informatico può migliorare la sicurezza e ridurre il rischio?


**Attributi della minaccia**

Quali sono gli attributi della minaccia che destano maggiore preoccupazione?



**Classificazione e priorità delle minacce**

Qual è il processo di classificazione e priorità degli attributi delle minacce?

Qual è la differenza tra analisi delle minacce e ciclo di vita dell'attacco?

# Il successo degli attacchi informatici di

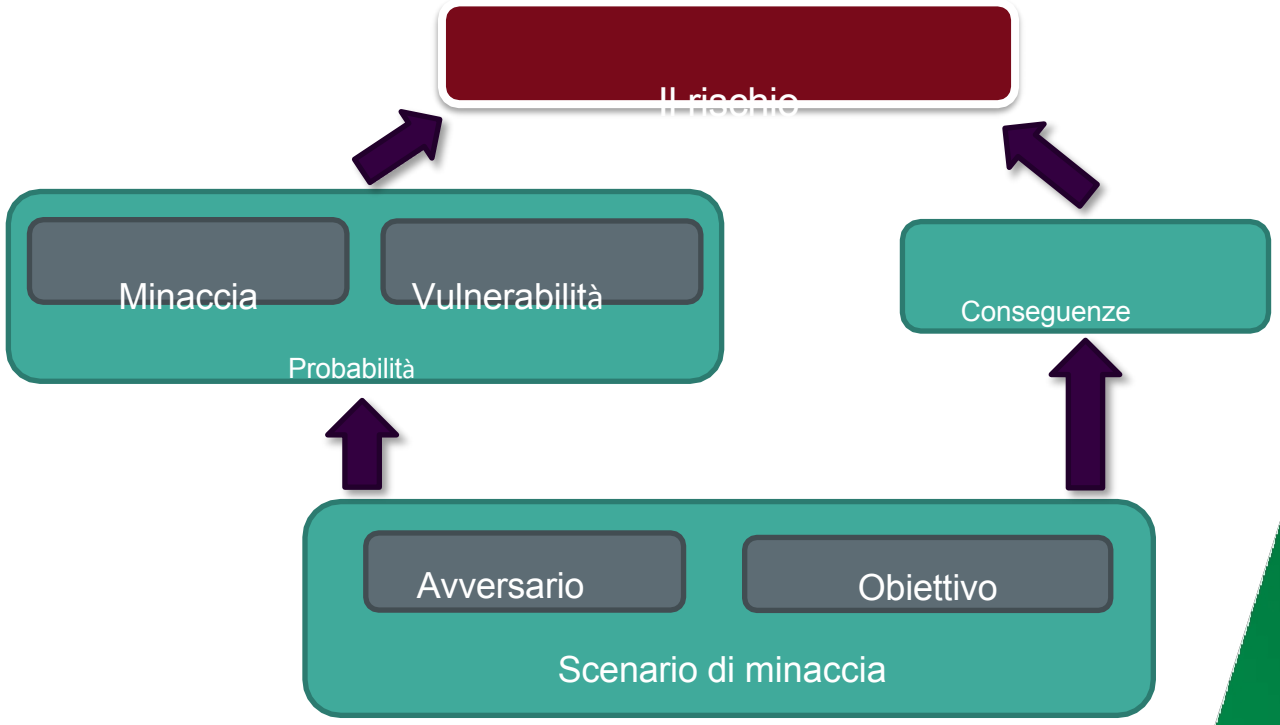
- Esistono diverse condizioni per il successo di un attacco informatico:
  - L'obiettivo deve presentare vulnerabilità o debolezze rilevabili nei sistemi e nei processi.
  - Un attore della minaccia deve disporre di risorse sufficienti per utilizzare le vulnerabilità e sfruttare il sistema.
  - L'attore della minaccia deve ritenere di poter trarre vantaggio dall'esecuzione dell'attacco - attrattività

- Possiamo utilizzare i dati sulle minacce per informare la sicurezza:
  - Possiamo progettare e difendere meglio i nostri sistemi se sappiamo come classificare le minacce (e i loro metodi).

  attributi)


Alcuni degli hacker "più ricercati" dell'FBI.
Fonte: fbi.gov/wanted/cyber

# Il successo degli attacchi informatici di



# Caratterizzazione dell'attore della minaccia

- **Motivazione e intenzione**
  - Motivo e obiettivo che l'avversario cerca di raggiungere: finanziario o ideologico o di furto o di sabotaggio.

- **Capacità**
  - Capacità e strumenti dell'avversario per raggiungere con successo l'obiettivo - le loro tattiche, tecniche e procedure (TTP).

- **Opportunità**
  - Conoscenza delle vulnerabilità e della capacità dell'attore della minaccia di sfruttarle e sfruttarle per violare il sistema.

# Tipi di attacco informatico

**Attacchi alle informazioni**

- Capacità
  - Molti strumenti disponibili
- Motivo
  - Guadagno finanziario
  - Spionaggio
  - Vantaggio competitivo
  - Preparazione per l'attacco OT
- Intento
  - Acquisire e sfruttare le informazioni

Gli attacchi informativi di successo possono indicare all'aggressore cosa fare per un attacco ai sistemi OT

Quali tipi di capacità sono necessarie per i diversi tipi di attacchi?

**Attacchi operativi**

- Capacità
  - Richiede competenze specialistiche
- Motivo
  - Politica
  - Terrore
- Intento
  - Danno fisico
  - Interruzione delle infrastrutture critiche

# Analisi delle minacce

- Che cos'?
  - Un'analisi delle caratteristiche degli attori delle minacce e delle loro attività
  - Raccogliere e confrontare i dati relativi alle minacce per identificarne l'intento, la motivazione e le capacità.

- Perché ?
  - L'analisi delle tendenze dell'attività delle minacce può essere utilizzata per creare difese efficaci.
  - Creare una consapevolezza situazionale delle tendenze delle minacce
  - Identificare i potenziali punti di rilevamento se gli avversari tentano di utilizzare gli stessi TTP.

**Dove possiamo trovare dati sulle minacce?**

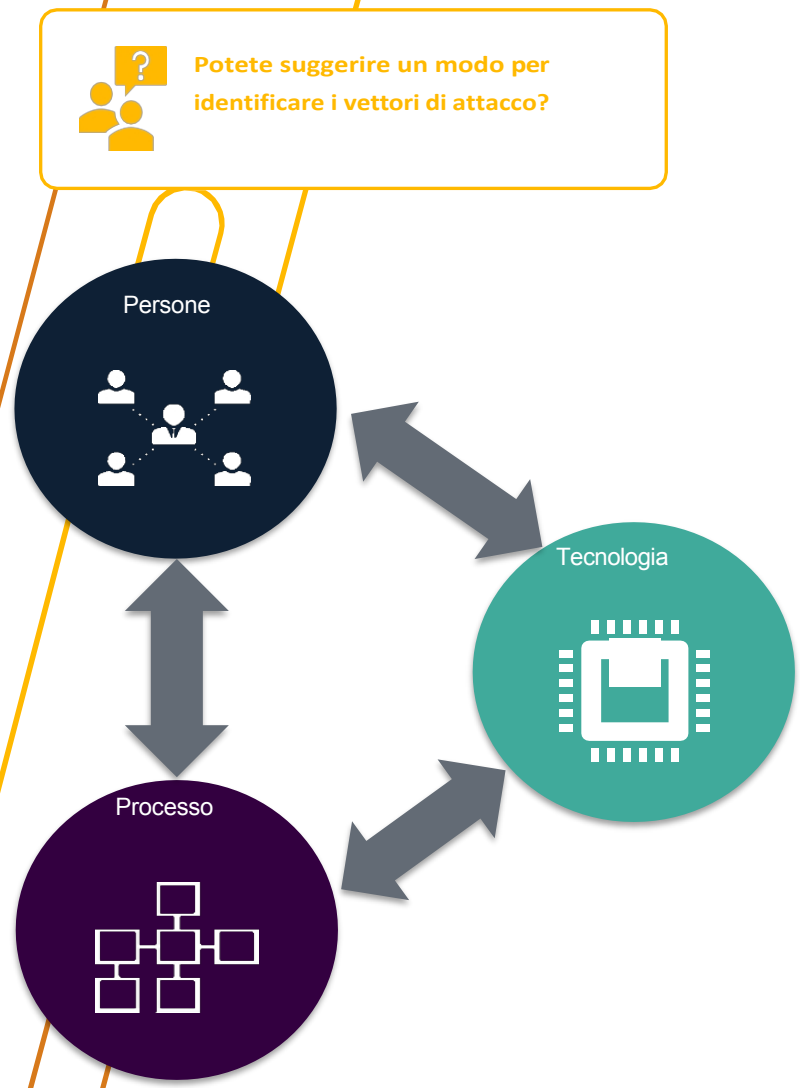
# Analisi degli attacchi informatici

- I vettori di attacco sono percorsi che una minaccia utilizza per propagarsi o infettare i sistemi.
  - Questi vettori sfruttano le persone, i processi e/o la tecnologia.

- Gli attacchi misti sono atti coordinati che utilizzano aspetti sia informatici che fisici.

- I framework per gli attacchi informatici descrivono le fasi di un attacco e aiutano a identificare le capacità che un avversario deve avere per raggiungere un obiettivo.

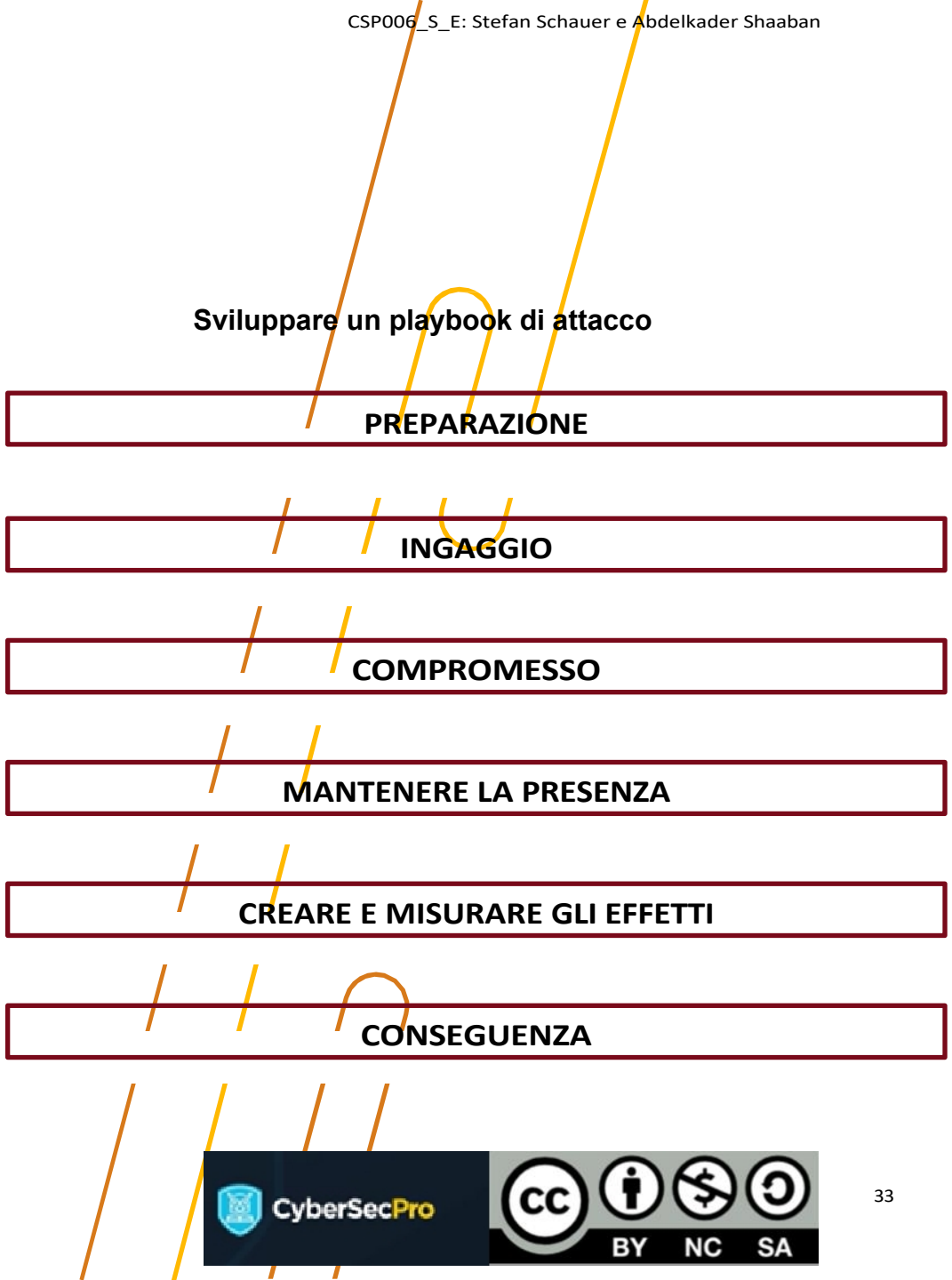
- La difesa basata sulle minacce utilizza queste fasi per offrire ai difensori maggiori opportunità di scoprire e rispondere a un attacco.



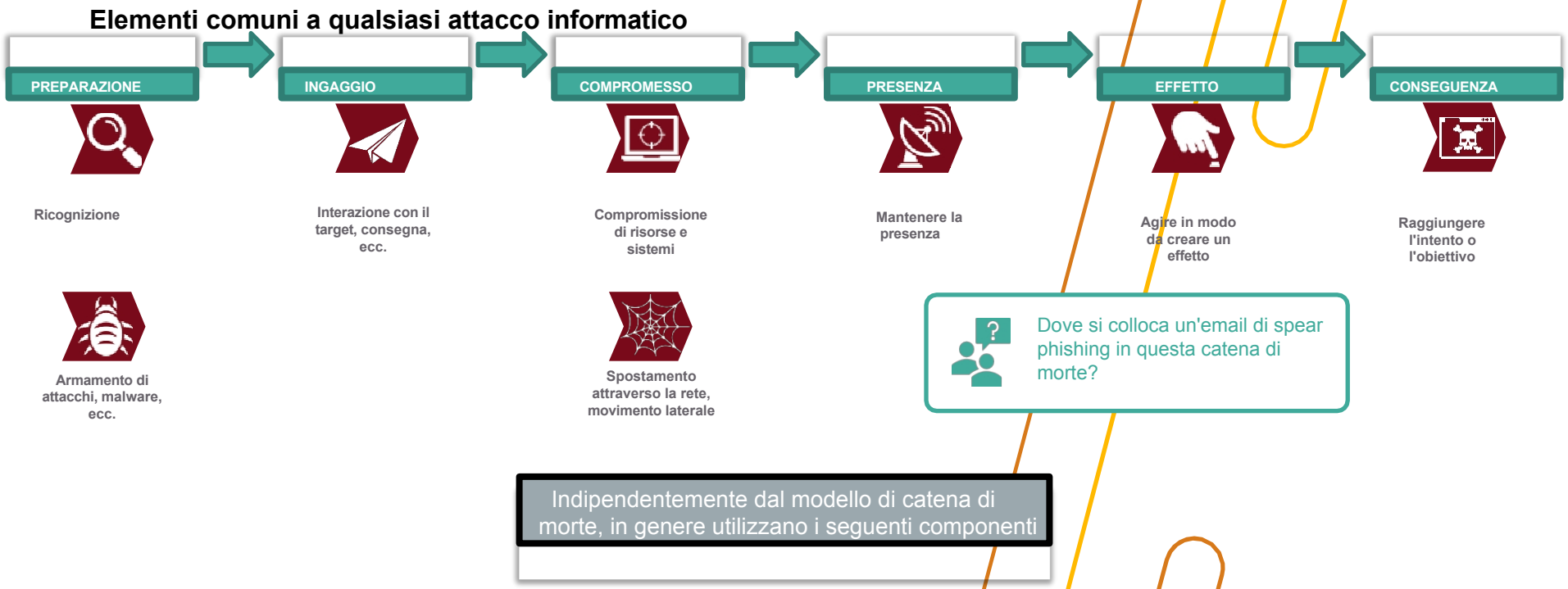
# Quadri di attacco

**Le azioni di attacco che un attore di minacce deve compiere...**

1. Scegliere un obiettivo e prepararsi all'attacco
2. Raccogliere e utilizzare l'intelligence
   - Definire i vettori
   - Convalidare l'opportunità
   - Valutare se la capacità è adeguata
3. Coinvolgere l'obiettivo
4. Compromettere l'obiettivo e ottenere l'accesso
5. Mantenere la presenza e avanzare
6. Determinare se l'attacco sta funzionando e adattarlo come richiesto (feedback)
7. Completare il proprio obiettivo



# Catena di morte



# Un esempio di modello di catena di morte: Catena di morte SANS ICS

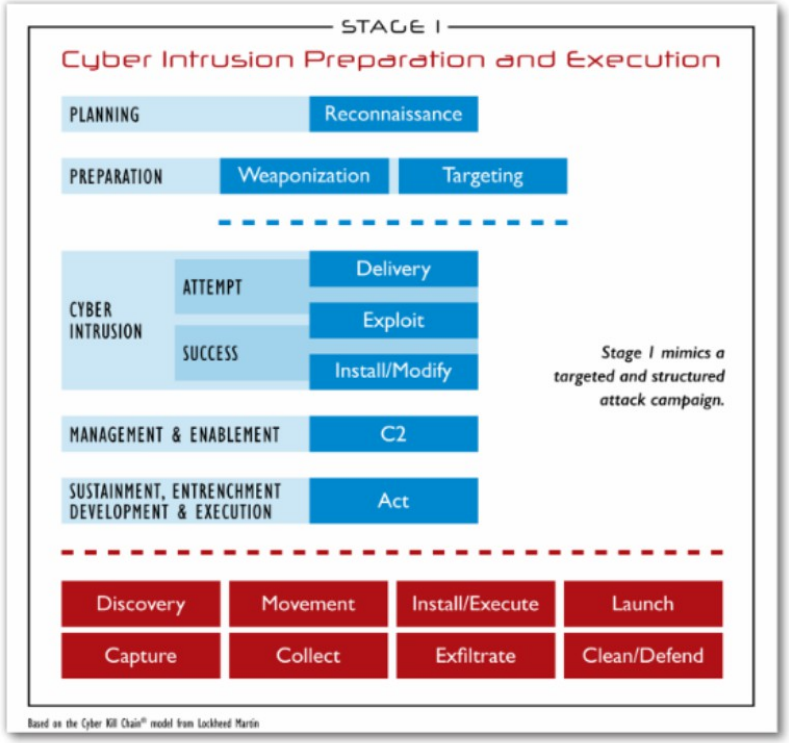



Figure 1. Stage 1: Cyber Intrusion Preparation and Execution

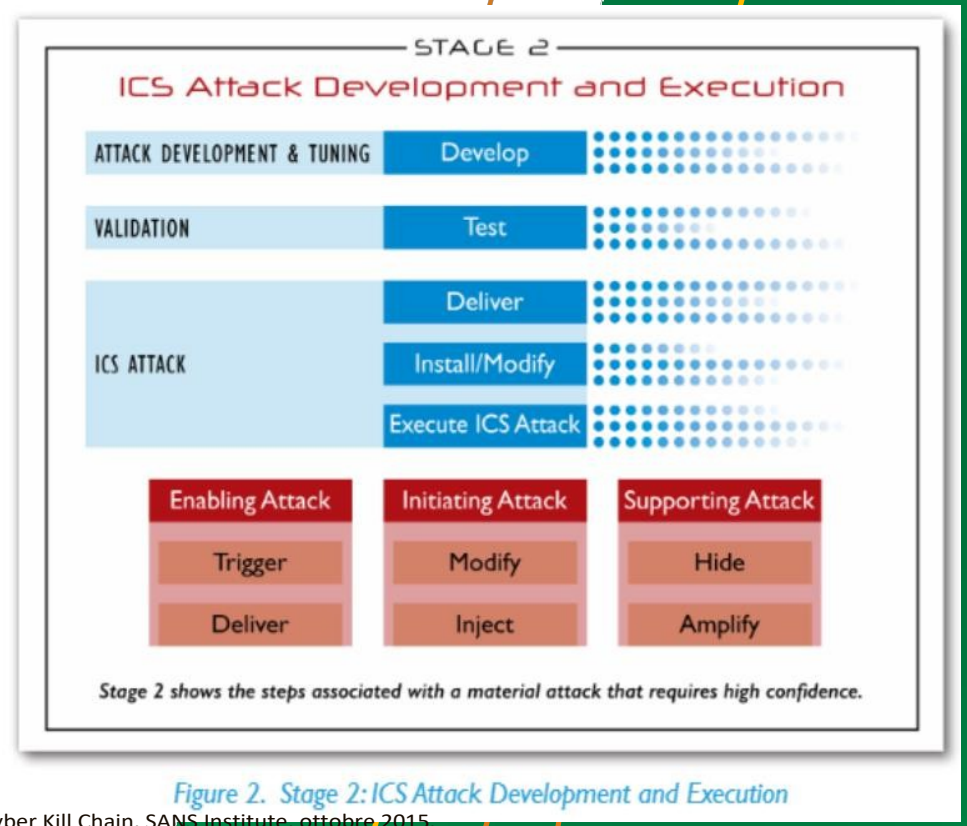



Figure 2. Stage 2: ICS Attack Development and Execution

Fonte: M.J. Assante, R.M. Lee, The Industrial Control System Cyber Kill Chain, SANS Institute, ottobre 2015.

# Analisi dell'intento e della motivazione

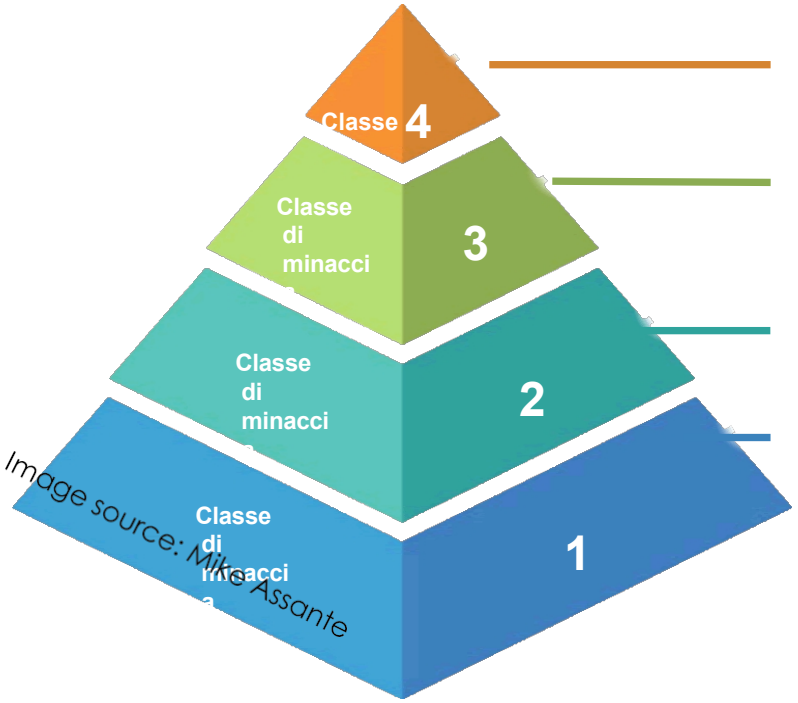
- Chiedetevi: qual è l'asset interessante su cui puntare?
- Ciò dipende dalla motivazione dell'attore della minaccia e l'intenzione

- I potenziali obiettivi potrebbero includere:
  - Dati personali
  - Sistemi finanziari (ad es. relativi ai pagamenti)
  - Sistemi operativi (sabotaggio)
  - ...

Vi vengono in mente altri obiettivi e cosa potrebbe motivare un attore di minacce a sfruttarli?

# Focus sulle capacità

Tipi di avversari in base alle loro capacità




Sviluppa l'intero spettro e inietta vulnerabilità ed exploit.

Sviluppa exploit sofisticati contro le vulnerabilità

Scopre le vulnerabilità del sistema

Sfrutta le vulnerabilità note con gli exploit pubblicati

# Relazione tra capacità e catena di morte

| No. | Descrizione | Minaccia di classe 1 | Minaccia di classe 2 | Minaccia di classe 3 | Minaccia di classe 4 |
|---|---|---|---|---|---|
| 1 | Definire l'obiettivo | X | X | X | X |
| 2. | Trovare e organizzare i complici | | | X | X |
| 3. | Costruire o acquisire strumenti | | | X | X |
| 4. | Ricerca di infrastrutture e dipendenti target | | X | X | X |
| 5. | Test di rilevamento | | | X | X |
| 6. | Distribuzione | | X | X | X |
| 7. | Intrusione iniziale | X | X | X | X |
| 8. | Connessione in uscita avviata | X | X | X | X |
| 9. | Ampliare l'accesso e ottenere le credenziali | | X | X | X |
| 10. | Rafforzare il punto d'appoggio | | | X | X |
| 11. | Esfiltrazione dei dati | X | X | X | X |
| 12. | Coprire le tracce e non farsi scoprire | | | X | X |

# Cosa rende un attacco efficace

***Pensare come un attaccante:***

- Un attacco è progettato per ottimizzare il successo e minimizzare lo sforzo.
- L'elemento "umano" deve essere sfruttato
- I dati vengono consultati, rubati e/o manipolati.
  - Raccogliere il maggior numero possibile di informazioni sull'ambiente di rete di destinazione.
  - Includere dati su persone, processi, politiche
  - Furto di credenziali e/o informazioni sensibili spesso necessarie per l'accesso
- Qualsiasi "fiducia" tra i sistemi deve essere sfruttata
  - Passare da un singolo asset/dominio a un altro, semplicemente per associazione.
  - Sfruttare l'accesso già esistente
- L'accesso deve essere mantenuto per poter misurare il successo.
- Ove possibile, utilizzare attacchi fisici per ottenere l'accesso a risorse e reti dietro le contromisure di sicurezza.

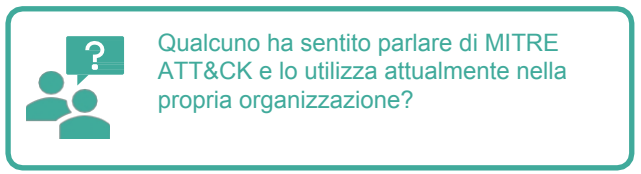
# Cosa possiamo fare?

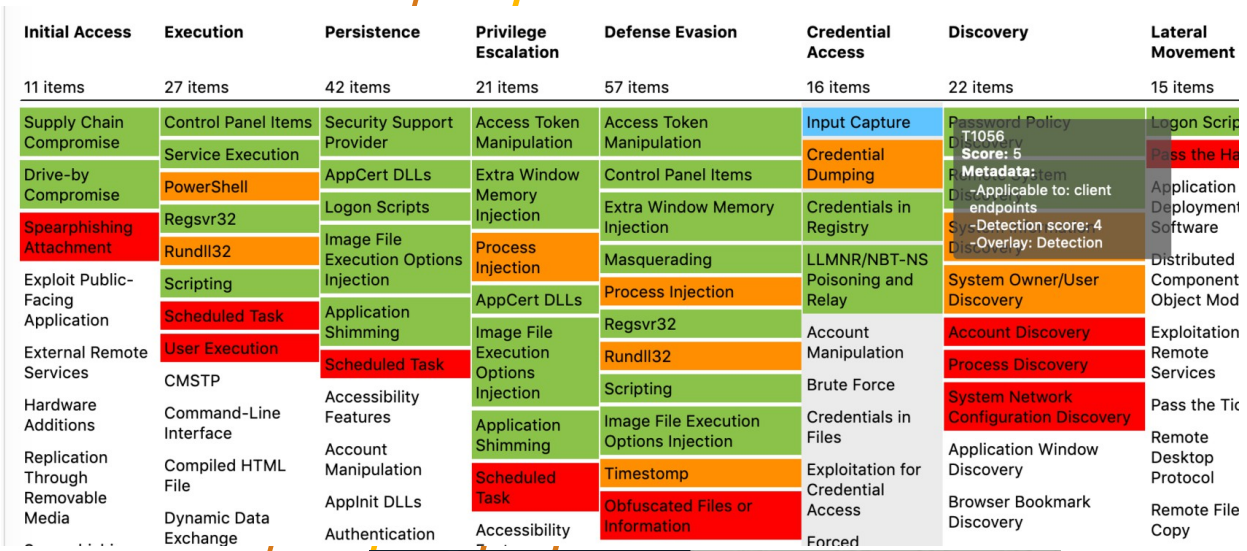
- Capire dove i nostri sistemi offrono opportunità a un aggressore.
- Determinare in modo proattivo il modo in cui un aggressore potrebbe attaccare
- Valutare come informazioni apparentemente non correlate possano informare l'avversario.
- Comprendere e gestire la nostra vulnerabilità
- Determinare quale capacità deve essere richiesta a un avversario per sfruttare una vulnerabilità.
- Difendere i nostri asset in modo da aumentare lo sforzo di lavoro di un avversario con l'obiettivo di garantire:
  - La capacità di attacco è insufficiente
  - Il panorama delle opportunità è troppo piccolo
  - La conseguenza/intento desiderato è irraggiungibile
- Mitigare gli effetti di eventi dannosi prima che si verifichino conseguenze più gravi.

Quali attività specifiche possiamo svolgere per costruire questa conoscenza e capacità?

# Il quadro MITRE ATT&CK

- Una struttura di conoscenza che descrive le TTP avversarie, organizzate in matrici.
- Esistono diverse matrici, anche per i sistemi di controllo aziendali e industriali
- Le conoscenze si basano sugli incidenti segnalati dalla comunità della cybersecurity.
- Può essere utilizzato per supportare le attività di automazione della sicurezza per valutare le minacce e l'organizzazione. disponibilità

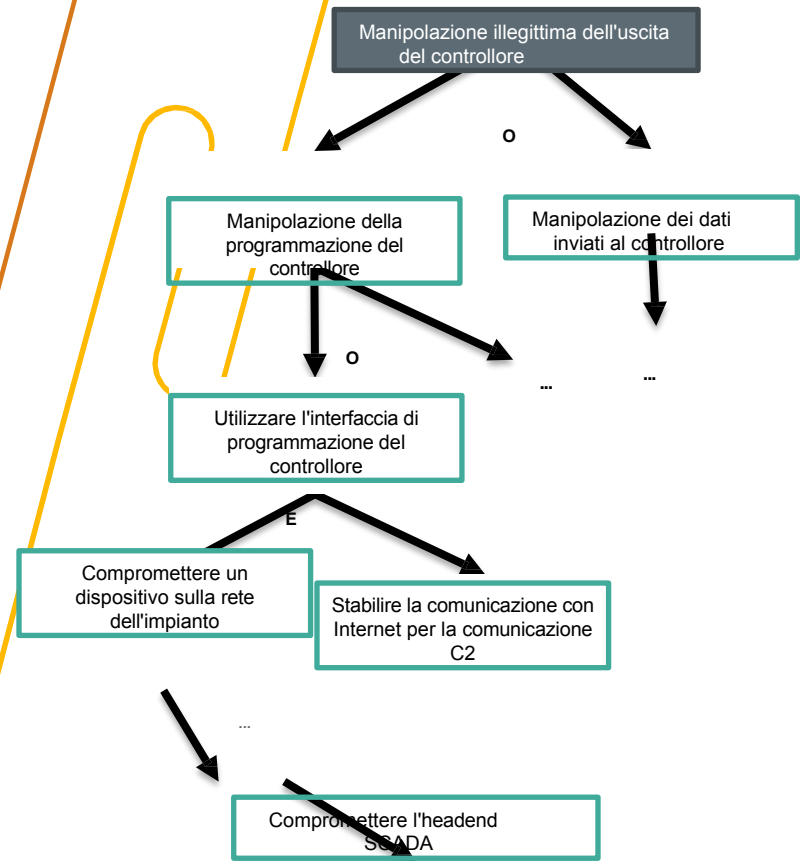


# Alberi da attacco

- Un'analisi strutturata dei vettori di attacco da un

  Prospettive dell'attaccante
  - Identificazione dell'obiettivo dell'attacco come radice dell'albero.
  - Decomposizione in sotto-obiettivi fino a raggiungere una sufficiente granularità fine (AND, OR)
  - Valutazione degli alberi di foglie in relazione alla verosimiglianza
  - Propagazione dei valori alla radice dell'albero
    - E: minimo di bambini
    - OPPURE: massimo di bambini
  - Identificazione dei principali percorsi di attacco (sottografo)



# MinacciaRaccogliete

# Modellazione delle minacce

La modellazione delle minacce è un elemento fondamentale dell'ingegneria della sicurezza:

- Rilevare potenziali punti deboli della sicurezza in un modello di sistema
- Definire le corrispondenti mitigazioni della sicurezza

https://www.theprepperjournal.com/2018/02/02/hardscaping-projects-backyard/

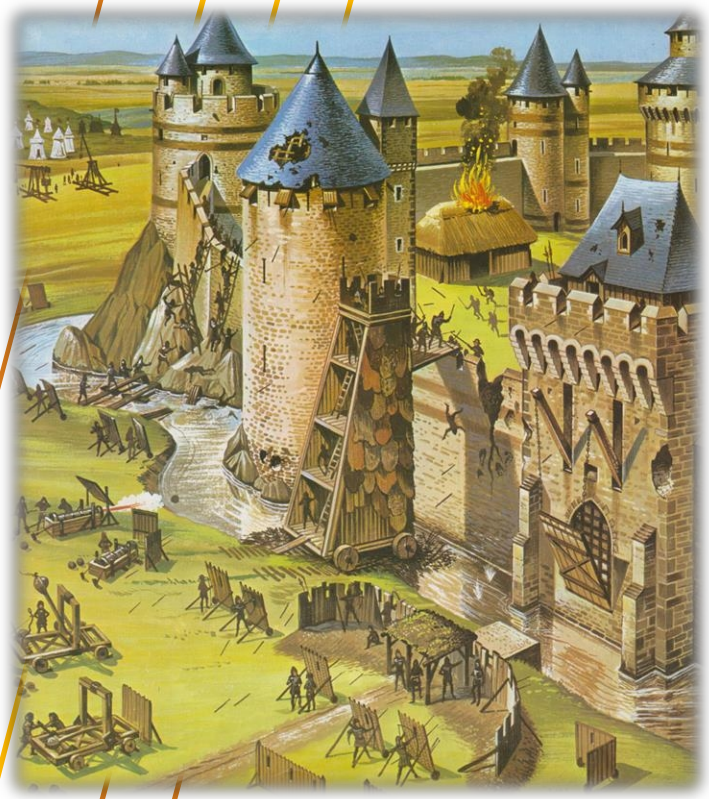
Schmittner C, Tummeltshammer P, Hofbauer D, Shaaban AM, Meidlinger M, Tauber M, Bonitz A, Hametner R, Brandstetter M.
Modellazione delle minacce nel settore ferroviario. InInternational Conference on Reliability, Safety, and Security of Railway Systems 2019 Jun 4 (pp. 261-271). Springer, Cham.

# Modellazione delle minacce

La modellazione delle minacce è un elemento fondamentale dell'ingegneria della sicurezza:

- Rilevare potenziali punti deboli della sicurezza in un modello di sistema
- Definire le corrispondenti mitigazioni della sicurezza

https://www.theprepperjournal.com/2018/02/02/hardscaping-projects-backyard/



http://history.parkfieldprimary.com/medieval/attacking-a-castle

Schmittner C, Tummeltshammer P, Hofbauer D, Shaaban AM, Meidlinger M, Tauber M, Bonitz A, Hametner R, Brandstetter M.
Modellazione delle minacce nel settore ferroviario. InInternational Conference on Reliability, Safety, and Security of Railway Systems 2019 Jun 4 (pp. 261-271). Springer, Cham.

# Perché ThreatGet?

- ThreatGet è uno strumento di analisi delle minacce sviluppato da AIT, che mira ad automatizzare l'approccio all'analisi delle minacce per identificare le potenziali minacce in un modello di sistema dovute all'esistenza di vulnerabilità di sicurezza.
- ThreatGet vi aiuta a innovare questo processo costoso e soggettivo automatizzando l'analisi e formalizzando le minacce.
  informazioni.
- I risultati delle analisi sono riutilizzabili e tutte le mitigazioni e le decisioni di progettazione sono tracciabili attraverso il processo di sviluppo.
- ThreatGet consente di risparmiare sui costi e, grazie al catalogo delle minacce aggiornabile, l'analisi rimane aggiornata automaticamente.

**AUTOMATED SECURITY ASSESSMENT**

ThreatGet automatically identifies threats and supports ongoing risk management. The tool extends the well-established Enterprise Architect modeling platform and is designed to support use cases in different domains.

**EXTENSIBLE MODEL LIBRARY**

ThreatGet contains domainspecific security-relevant elements for system modeling. Company specific model elements and threats can also be added. All model elements contain predefined security parameters to consider existing security concepts.

**AUTOMATED SUGGESTION OF MITIGATIONS**

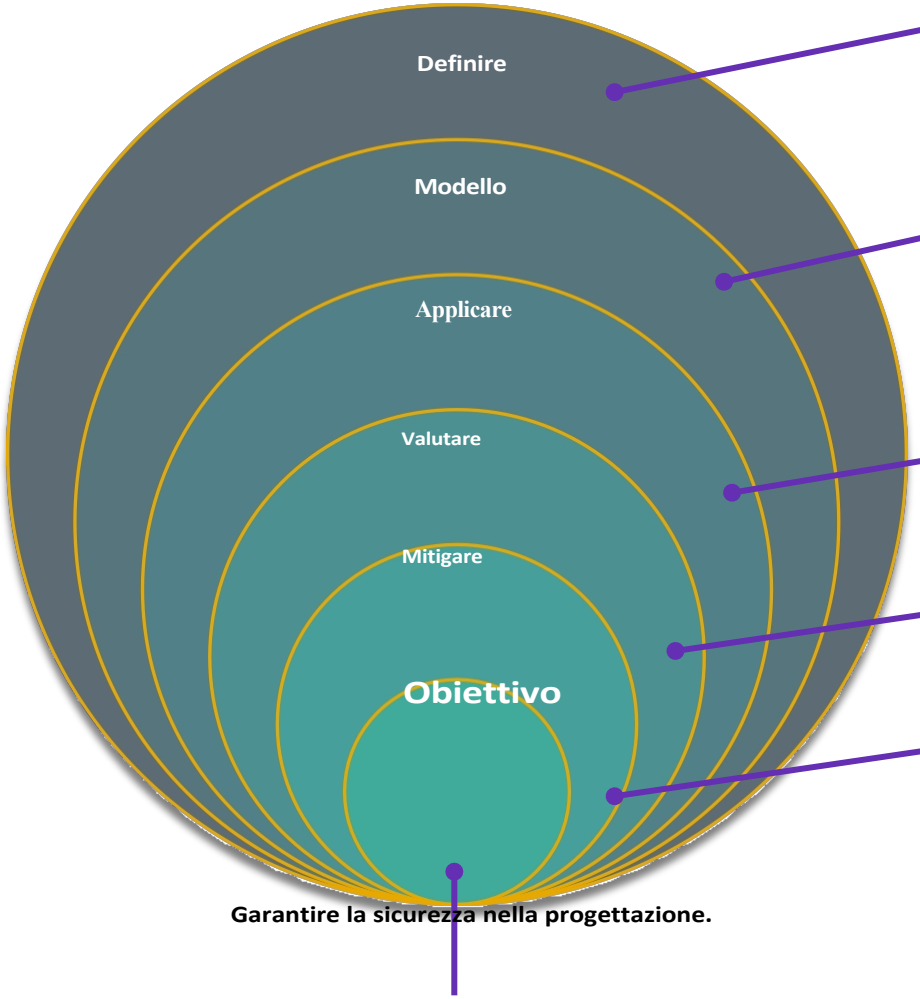
ThreatGet will automatically assess the system model to find potential security issues in the design and will also suggest mitigations.

**AUTOMATED THREAT INTELLIGENCE UPDATES**

Stay up to date with ThreatGet and receive the latest cybersecurity threats with a threat-database subscription.

CyberSecPro

# Fasi di modellazione di ThreatGet




**Garantire la sicurezza nella progettazione.**

**Fase 1**: Definire i componenti del sistema con tutte le ipotesi relative alla sicurezza e le informazioni necessarie.

**Fase 2:** creazione di un diagramma di sistema

**Fase 3**: applicare ThreatGet al modello di sistema per identificare le potenziali minacce.

**Fase 4**: valutare la gravità del rischio per ciascuna minaccia potenziale

**Fase 5**: aggiornamento del modello di sistema con le nuove ipotesi di sicurezza

# Caratteristiche di ThreatGet

**Processo di modellazione:** gli elementi e gli oggetti più comuni nel dominio automobilistico.

**Parametri di sicurezza: consente di** adattare facilmente i valori di sicurezza degli elementi del modello per mitigare la sicurezza.

**Analisi basata su regole:** Una raccolta di regole che descrivono quando una specifica minaccia è rilevante. Queste regole vengono definite utilizzando nomi e proprietà degli stencil e memorizzate in un database delle minacce.

**Categorie di minacce:** La classificazione delle minacce STRIDE è la guida per il processo di analisi e rilevamento delle minacce.

**Risultati:** le minacce rilevate vengono visualizzate in diagrammi separati in una struttura ordinata.

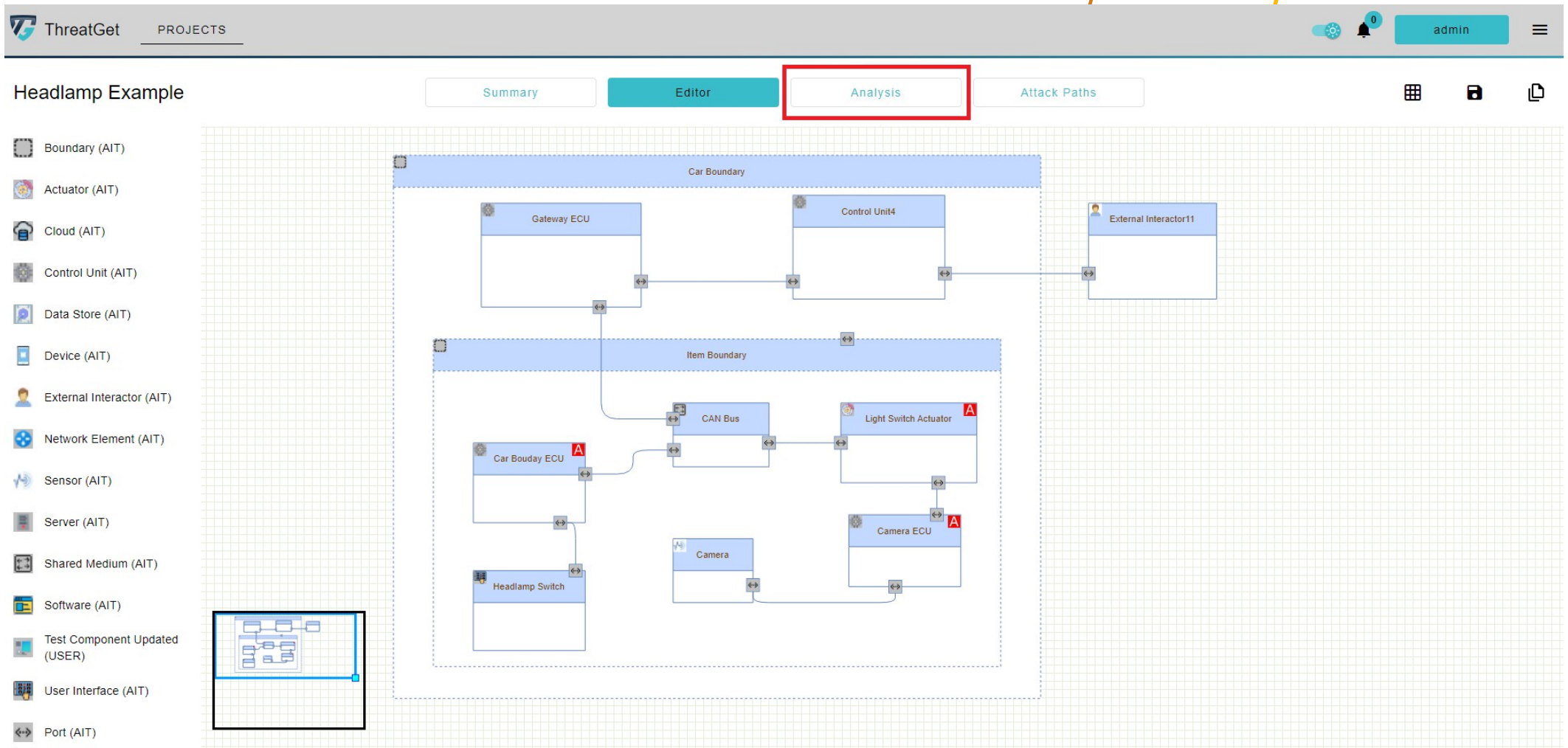
**Tracciabilità:** ThreatGet aggrega tutte le minacce generate in una tabella e ogni minaccia è riconducibile al relativo elemento (-> la tracciabilità è nel modello).

**Valutazione del rischio**: ThreatGet valuta il grado di rischio delle minacce potenziali identificate.

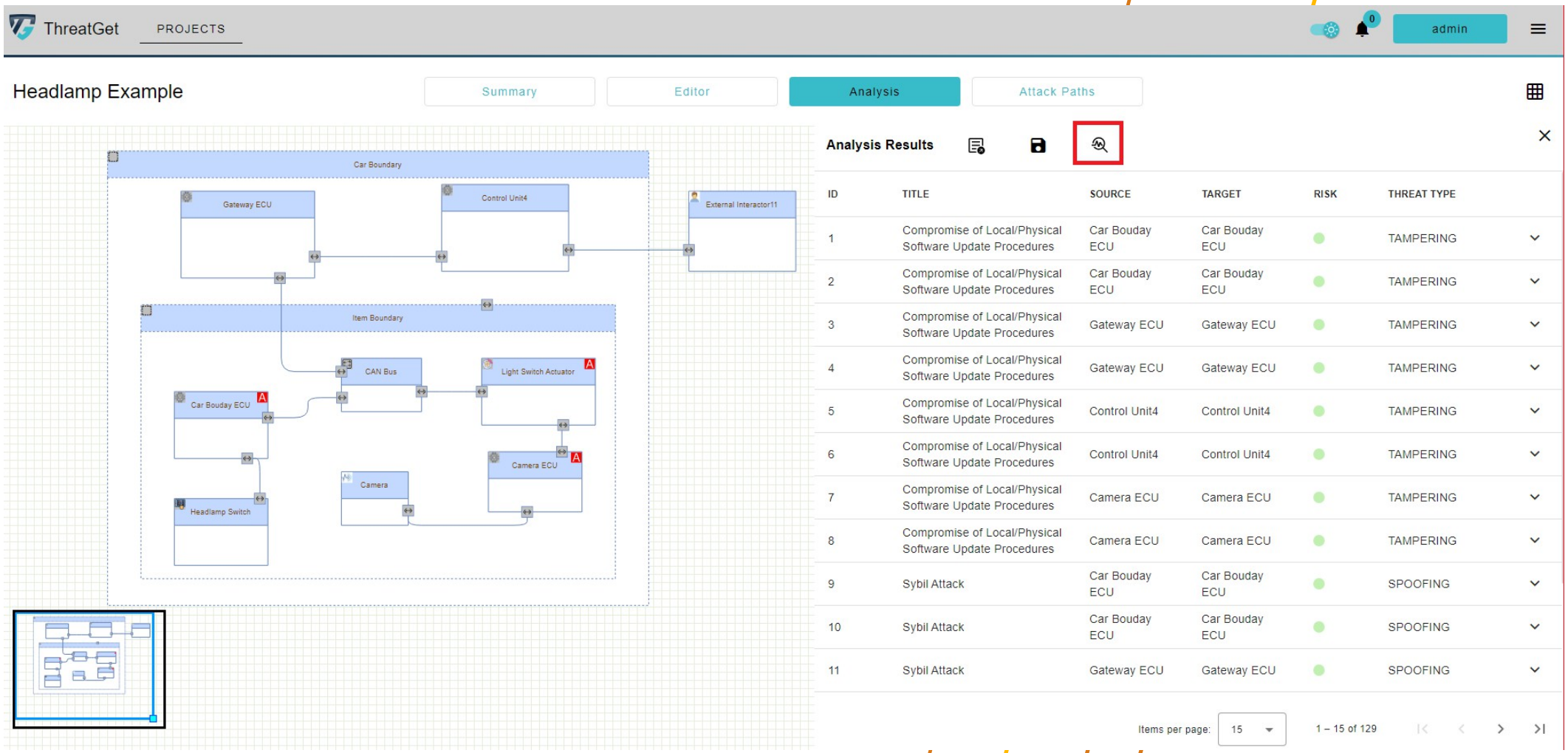
**Documentazione:** ThreatGet genera un rapporto completo di tutte le minacce identificate con un'immagine del relativo elemento del modello.

# Esempio: ThreatGet

# ThreatGet: Esempio di modellazione



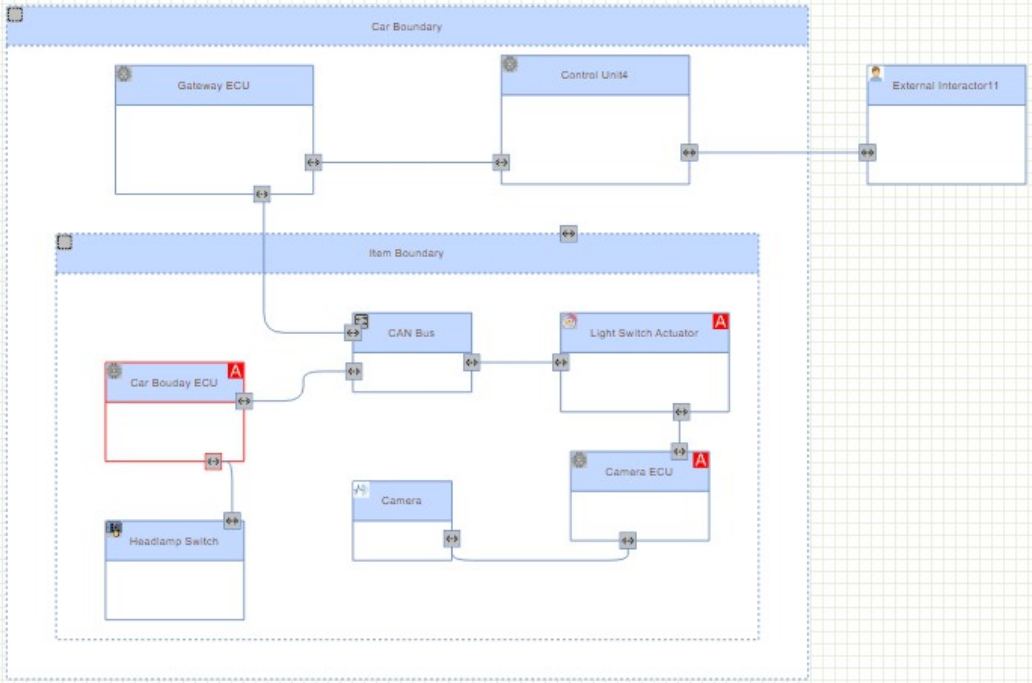
# ThreatGet: Risultati dell'analisi




| ID | TITLE | SOURCE | TARGET | RISK | THREAT TYPE |
|---|---|---|---|---|---|
| 1 | Compromise of Local/Physical Software Update Procedures | Car Bouday ECU | Car Bouday ECU | | TAMPERING |
| 2 | Compromise of Local/Physical Software Update Procedures | Car Bouday ECU | Car Bouday ECU | | TAMPERING |
| 3 | Compromise of Local/Physical Software Update Procedures | Gateway ECU | Gateway ECU | | TAMPERING |
| 4 | Compromise of Local/Physical Software Update Procedures | Gateway ECU | Gateway ECU | | TAMPERING |
| 5 | Compromise of Local/Physical Software Update Procedures | Control Unit4 | Control Unit4 | | TAMPERING |
| 6 | Compromise of Local/Physical Software Update Procedures | Control Unit4 | Control Unit4 | | TAMPERING |
| 7 | Compromise of Local/Physical Software Update Procedures | Camera ECU | Camera ECU | | TAMPERING |
| 8 | Compromise of Local/Physical Software Update Procedures | Camera ECU | Camera ECU | | TAMPERING |
| 9 | Sybil Attack | Car Bouday ECU | Car Bouday ECU | | SPOOFING |
| 10 | Sybil Attack | Car Bouday ECU | Car Bouday ECU | | SPOOFING |
| 11 | Sybil Attack | Gateway ECU | Gateway ECU | | SPOOFING |

Items per page: 15 1 – 15 of 129

# ThreatGet: Risultati dell'analisi




| 1 | Compromise of Local/Physical Software Update Procedures | Car Bouday ECU | Car Bouday ECU | | TAMPERING |
|---|---|---|---|---|---|

**Title:**
Compromise of Local/Physical Software Update Procedures

**Risk Level:** 1

**Description:**
Compromise of Local/Physical Software Update Procedures involves the physical manipulation of a software update mechanism by external or internal malicious actors. This type of cyberattack is distinct and particularly concerning because it involves direct, physical intervention in the update processes. Unlike remote cyber threats, this attack vector exploits the physical accessibility, allowing attackers with technical knowledge of software systems to alter or fabricate system update programs or firmware. The direct nature of this threat implies that the attacker might be someone with insider access, such as a service technician, or an external party who has managed to gain physical access. The implications of such an attack are severe, as they can lead to the unauthorized introduction of malicious functionalities or access capabilities within the software systems, potentially compromising safety, operational integrity, and user privacy. This threat targets the local or physical aspect of the software update mechanism, which is particularly vulnerable to manipulation when an attacker gains physical access. By modifying, replacing, or introducing harmful elements into the firmware or software updates, attackers can initiate a range of unauthorized actions. These could range from subtle system malfunctions to more overt takeovers of control systems or access to sensitive user data. To effectively counter this risk, it is crucial to implement robust physical security measures that restrict unauthorized access to the software update systems. Secure software delivery protocols are also necessary to ensure the authenticity and integrity of software and firmware updates, even when performed physically. Additionally, specific measures to detect and prevent tampering or spoofing of software updates, especially those involving physical access, are critical components of a comprehensive defense strategy.

**Likelihood:**
HIGH

Category: TAMPERING

**Impact:**

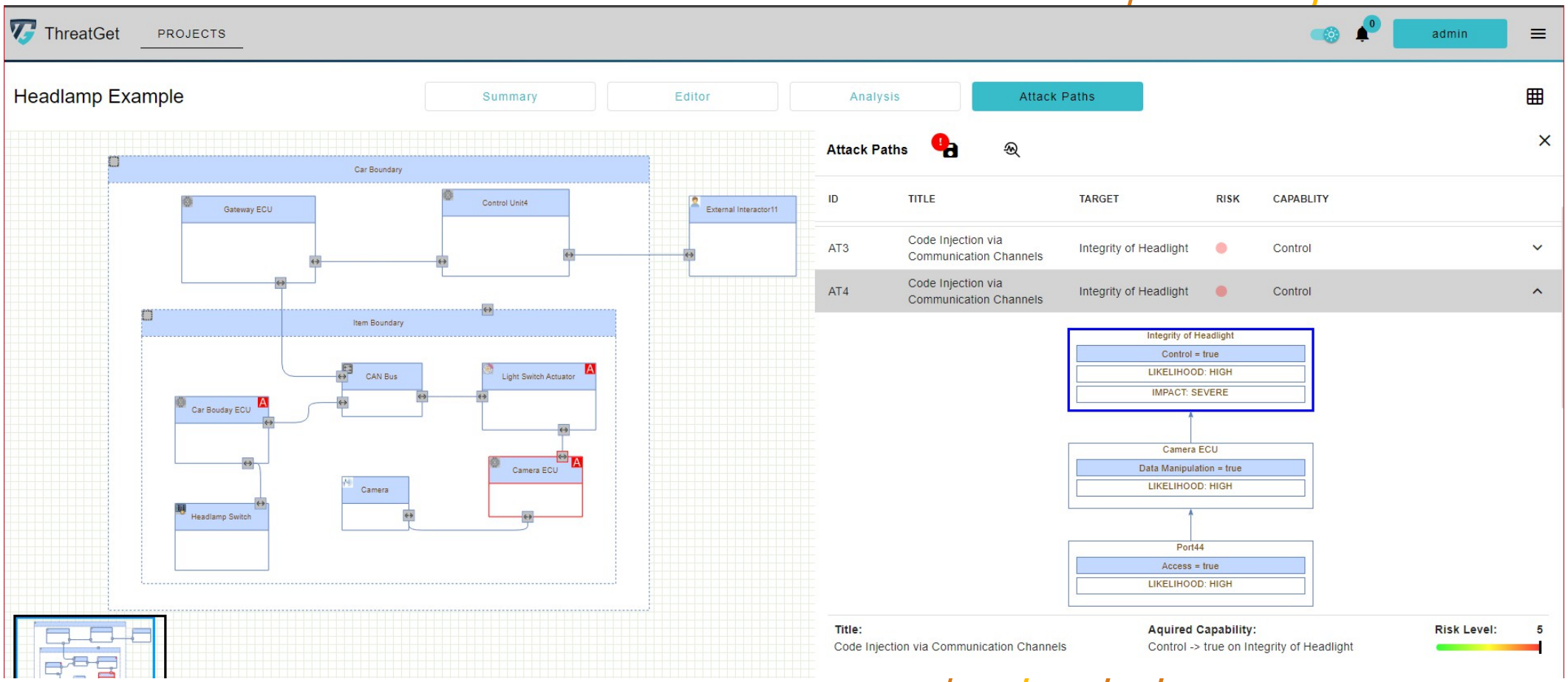
| S | F | O | P |
|---|---|---|---|
| NEG. | NEG. | NEG. | NEG. |

**Attack Feasibility:**

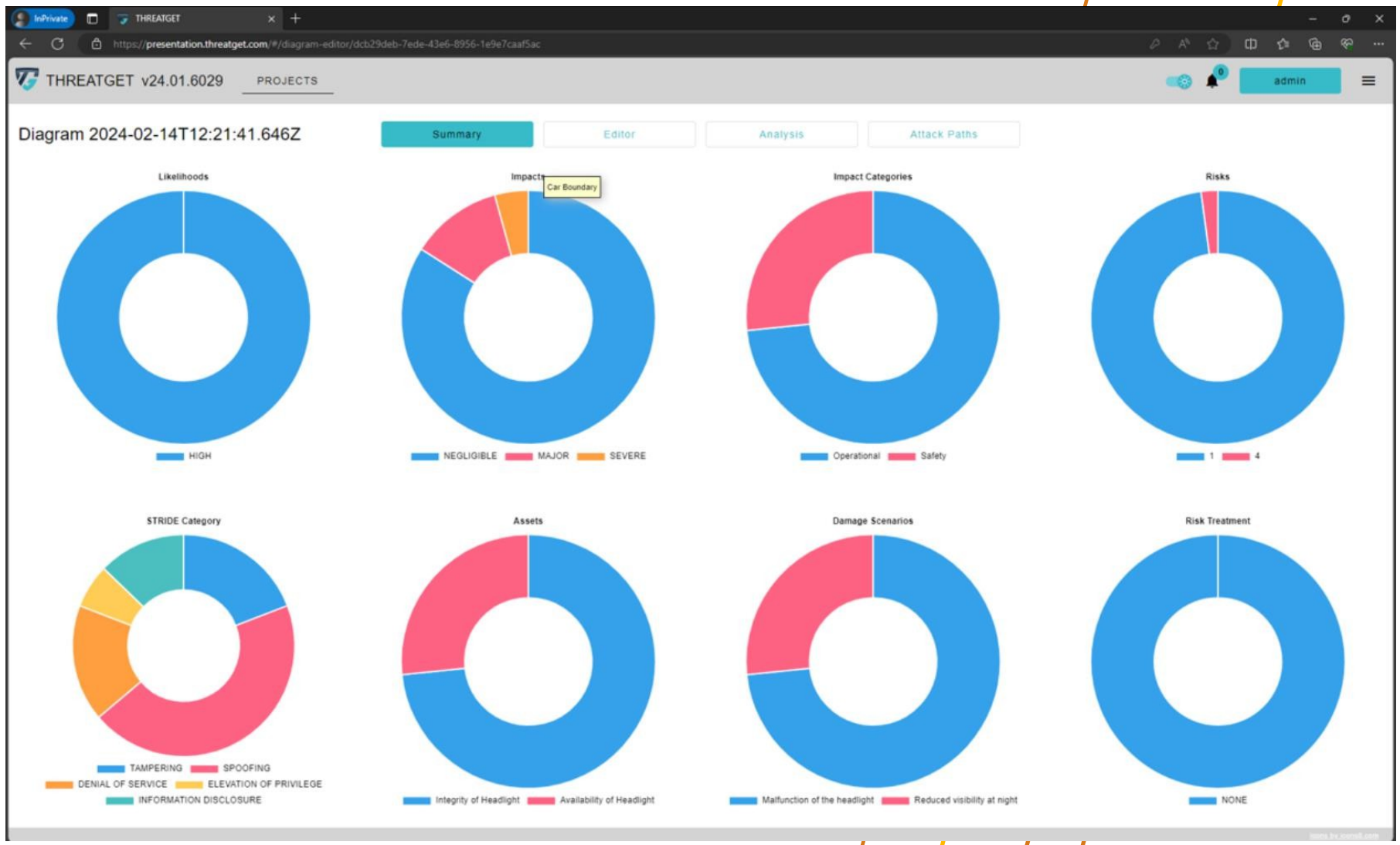
Elapsed Time: <=One Day
Expertise: Layman
Knowledge: Restricted
Window of Opportunity: Moderate
Equipment: Standard

Risk Treatment: NONE

# ThreatGet: Percorso di attacco



# ThreatGet: Sintesi dell'analisi



# Pratico: ThreatGet

# Lavoro pratico

1. **Utilizzare ThreatGet**: Sviluppare un modello di infrastruttura critica per il settore energetico utilizzando ThreatGet.

2. **Identificare i beni critici** : Definire gli asset critici e delineare tutti i danni correlati.
   scenari.

3. **Analisi iniziale delle minacce**: Eseguire un'analisi preliminare delle minacce prima di implementare qualsiasi proprietà di sicurezza nel modello del sistema.

4. **Specifica delle proprietà di sicurezza**: Identificare e definire le proprietà di sicurezza necessarie per ogni componente del sistema.

5. **Analisi delle minacce rivista**: Eseguire nuovamente l'analisi delle minacce, questa volta con le proprietà di sicurezza applicate.

6. **Relazioni e documentazione**: Riportare i risultati delle analisi iniziali e di quelle riviste. Documentare le differenze nei risultati attribuibili all'applicazione delle proprietà di sicurezza.

# Sintesi

- Le informazioni sulle minacce possono essere utilizzate per gestire il rischio di cybersecurity e informare le decisioni in materia di sicurezza.
- L'obiettivo è quello di implementare misure che costringano l'avversario a modificare tattiche, tecniche e procedure utilizzando le informazioni sulle minacce.
- È importante sapere in che modo si può essere presi di mira dagli attori delle minacce e comprendere il proprio ruolo nel riconoscere gli attributi di un attacco informatico e come le operazioni possono essere impattate

# Connettersi con CyberSecPro: come registrarsi e altre informazioni pratiche

1. Sito web: www.cybersecpro-project.eu
2. X (Twitter): https://twitter.com/CyberSecPro_eu
3. LinkedIn: https://www.linkedin.com/company/cybersecpro-euproject/



Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

# Grazie

Si prega di inviare tutte le domande a: Stefan SchauerStefan.Schauer@ait.ac.at Abdelkader Shaaban, abdelkader.Shaaban@ait.ac.at