

# Forefuture - Intelligence Based Attack Simulations

---

Staffan Truvé, Co-founder/CTO Recorded Future  
January 2023

[truve@recordedfuture.com](mailto:truve@recordedfuture.com)

# Partners

 Recorded Future®



Swedavia  
Airports

(  foresee*ti* )

# Idea

Cyber security requires both an understanding of the current global threat picture and insight into how these threats can affect the actual systems of a company or organization.

Recorded Future performs global collection and analysis of threat, actor and vulnerability data. KTH tailors threat modeling and attack simulations of organizations' actual systems according to the current threat picture. By combining these capabilities, in a completely unique way, the relevant threat picture can be assessed in real time and measures taken to reduce the real risk from cyber attacks. Results will be validated together with Swedavia.









Who has the keys?

Is someone asking for the keys?

Is someone selling my property?

Are the blueprints out there?

Is someone talking about attacking places like this?

What places like this one have been attacked recently?

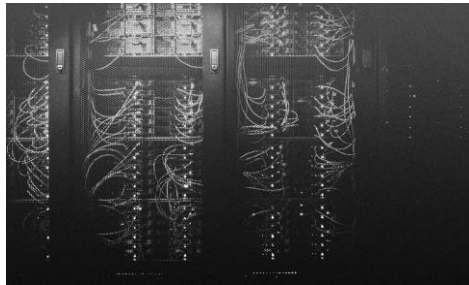
# Internet → Intelligence



## Unstructured/content sources

### 28 FBI, DHS, HHS Warn of Imminent, Credible Ransomware Threat Against U.S. Hospitals

On Monday, Oct. 26, KrebsOnSecurity began following up on a tip from a reliable source that an aggressive Russian cybercriminal gang known for deploying ransomware was preparing to disrupt information technology systems at hundreds of hospitals, clinics and medical care facilities across the United States. Today, officials from the FBI and the U.S. Department of Homeland Security hastily assembled a conference call with healthcare industry executives warning about an "imminent cybercrime threat to U.S. hospitals and healthcare providers."



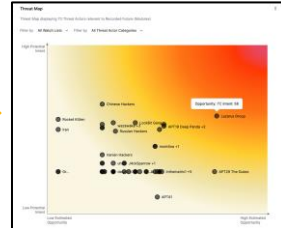
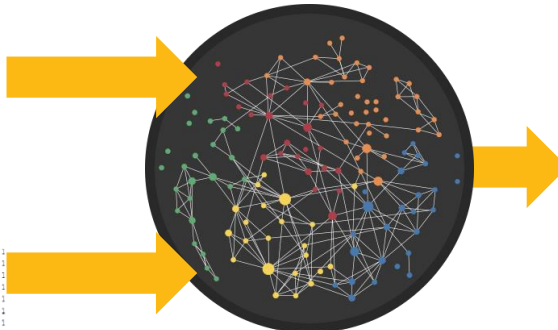
```
2012-12-27 16:58:23.000 0.000 TCP    66.249.132.103    80 → 132.161.254.100 80 [RST] Seq=1228231872 Win=0 Len=0
2012-12-27 16:58:24.000 0.000 TCP    172.16.0.100     80 → 66.249.132.103 80 [RST] Seq=1228231872 Win=0 Len=0
2012-12-27 16:58:25.000 0.000 TCP    192.168.1.100    80 → 66.249.132.103 80 [RST] Seq=1228231872 Win=0 Len=0
2012-12-27 16:58:26.000 0.000 TCP    66.249.132.103    80 → 192.168.1.100 80 [RST] Seq=1228231872 Win=0 Len=0
2012-12-27 16:58:27.000 0.000 TCP    66.249.132.103    80 → 192.168.1.100 80 [RST] Seq=1228231872 Win=0 Len=0
```



```
{(($_.InnerText -> #)
    |> getParameter('name'));
    |> getParameter('user');
    |> getParameter('pass');
    |> getParameter('email');
    |> getParameter('username');
    |> getParameter('password');
    |> getParameter('email');
    |> getParameter('username');
    |> getParameter('password');
    |> getParameter('email');
    |> getParameter('username');
    |> getParameter('password');
    |> getParameter('email');
    |> getParameter('username');
    |> getParameter('password');
    |> getParameter('email');
    |> getParameter('username');
    |> getParameter('password');
```



устранило две 0-day уязвимости  
В минувшие выходные разработчики Mozilla выпустили экстренное обновление безопасности для Firefox. Срочные патчи устранили в браузере две уязвимости нулевого дня, которые уже использовались хакерами в атаках. Два исправленные уязвимости получили идентификаторы CVE-2022-26485 (<https://www.mozilla.org/en-US/security/advisories/mfsa2022-09/>) CVE-2022-26485 и обе оцениваются как критические. Проблемы относятся к типу use-after-free (программа пытается использовать ранее очищенную память) и обе были обнаружены и исследователями из компании Qihoo 360. Сообщает, что первая из уязвимостей связана удалением параметров Extensible Stylesheet Language Transformations (XSLT) во время обработки, а вторая ошибка может быть вызвана неожиданным сообщением во фреймворке WebGPU (IPC). Хотя разработчики не сообщают каких-либо деталей о наблюдаемых попытках эксплуатации этих уязвимостей, баги такого типа обычно позволяют злоумышленникам выполнять произвольный код на целевых системах. Обе проблемы были решены в релизе Firefox 97.0.2, Firefox ESR 91.6.1, Firefox для Android 97.3.0 и Focus 97.3.0, сообщает Mozilla. Технические подробности об уязвимости пока тоже не разглашаются. Скорее всего, дополнительная информация будет опубликована после того, как большая часть пользователей установит исправления.



Structured data from technical/code sources





## Adversaries And Intent

Nation-State &  
Criminal Groups  
Hacktivists

Intent, TTPs,  
Vulns



## Infrastructure They Build

DNS  
Certificates  
Network Traffic  
Malware Detonations  
IP/Domain Infrastructure  
C2



## Organizations They Target

Corporate Networks  
Endpoints  
Intellectual Property  
Identities  
Physical world



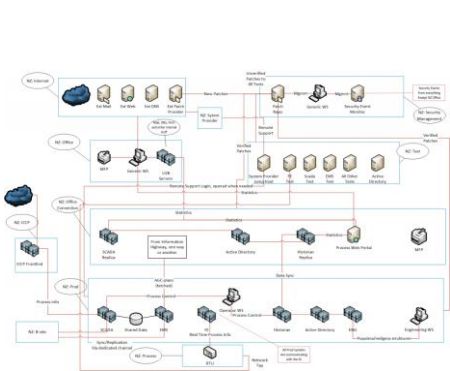
# Threat Modelling and Attack Simulations

- Attack simulations can evaluate the risks affecting your system
  - Manual system specification
  - AWS or Azure environment
    - Scans your environment and builds a digital copy
    - As granular as you allow it to be
- Probabilistic simulation

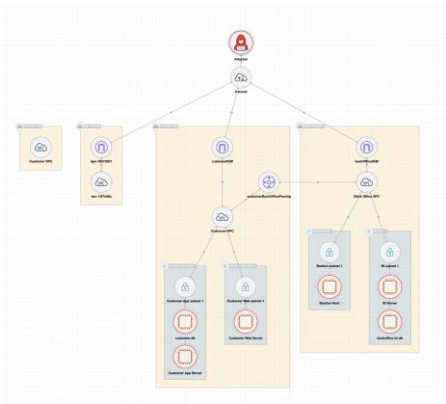




# SecuriCAD, how it looks/ works



Environment



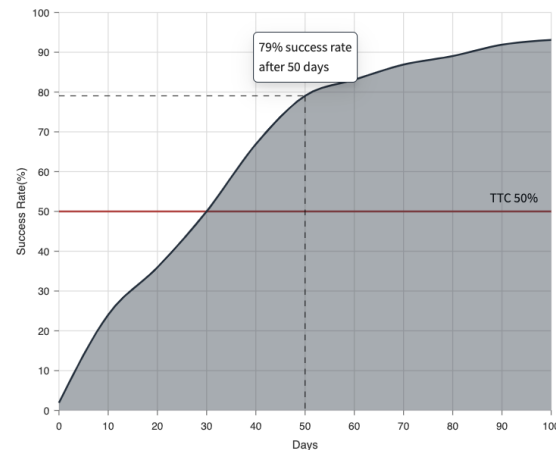
SecuriCAD



Simulation

# Areas of improvement

- Lacks access to current real world data
  - Assumptions based of research
  - Pulls data from “static” lists
  - Slow to react to changes in threat levels
- Manual setting alterations needed to update
  - Reacts to alterations from inside, not outside

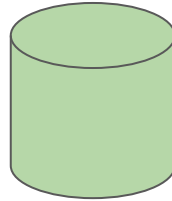




API



E-mails  
AWS keys  
CVE  
Trends  
C2



Ingestion  
Simulation enrichment



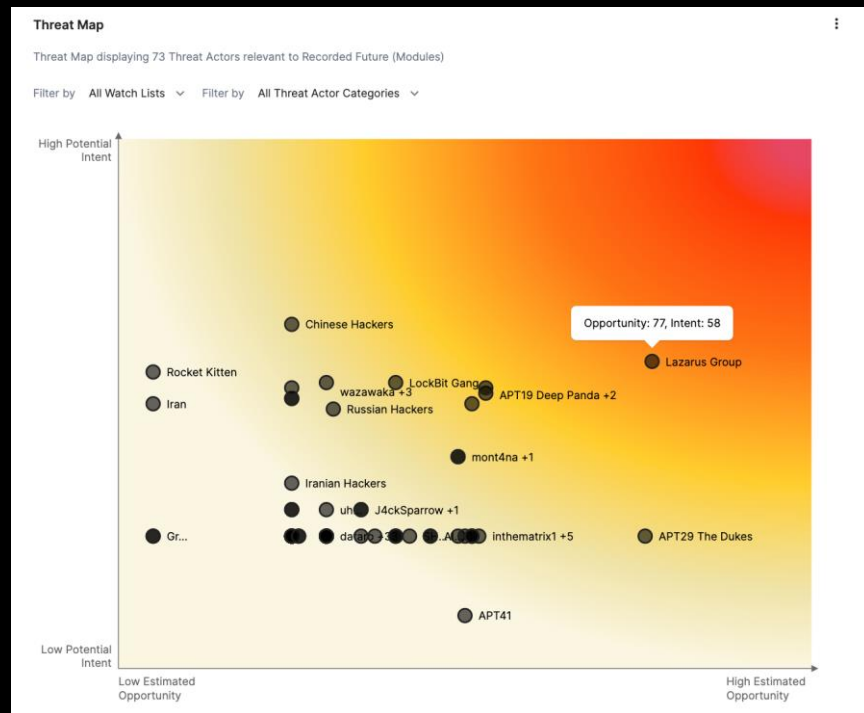


# The data

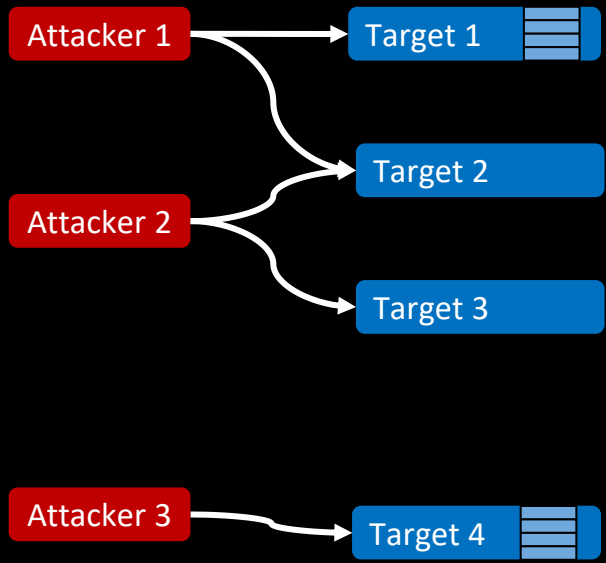
- Credential leaks + AWS keys
  - Parameters that have a powerful impact on simulations.
  - Natural connection between our systems
- CVEs + C2s
- Trends
  - Industry , Geo, Threat Actors, Attack Vectors

# Putting the Intelligence Graph to work: Threat Map

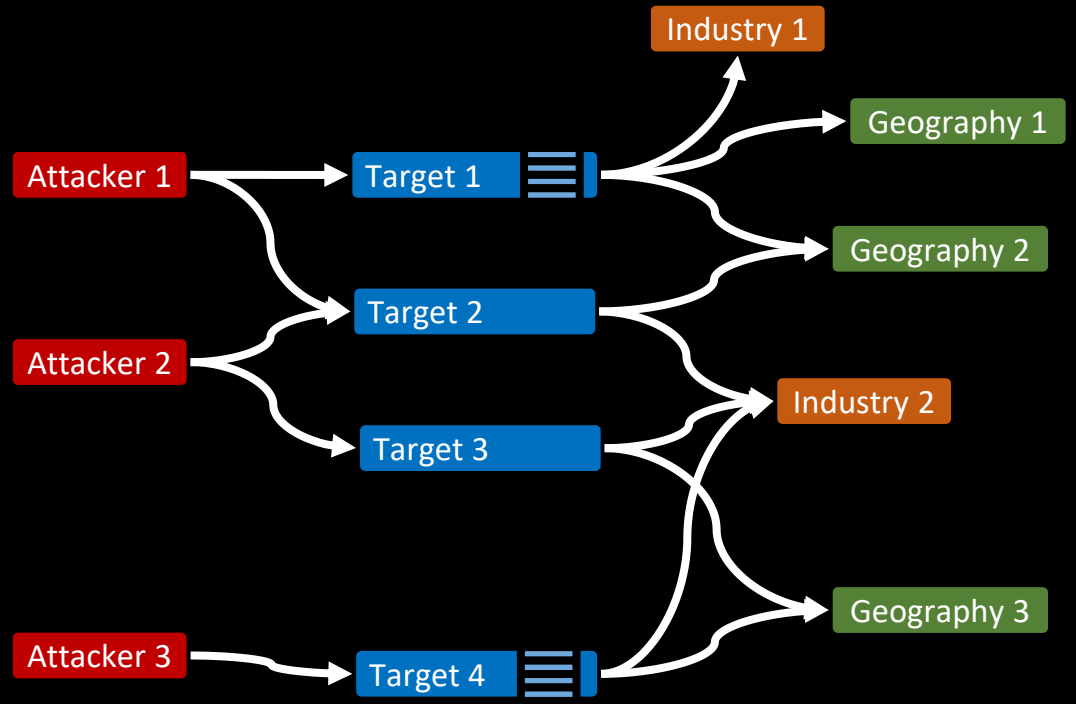
Intent

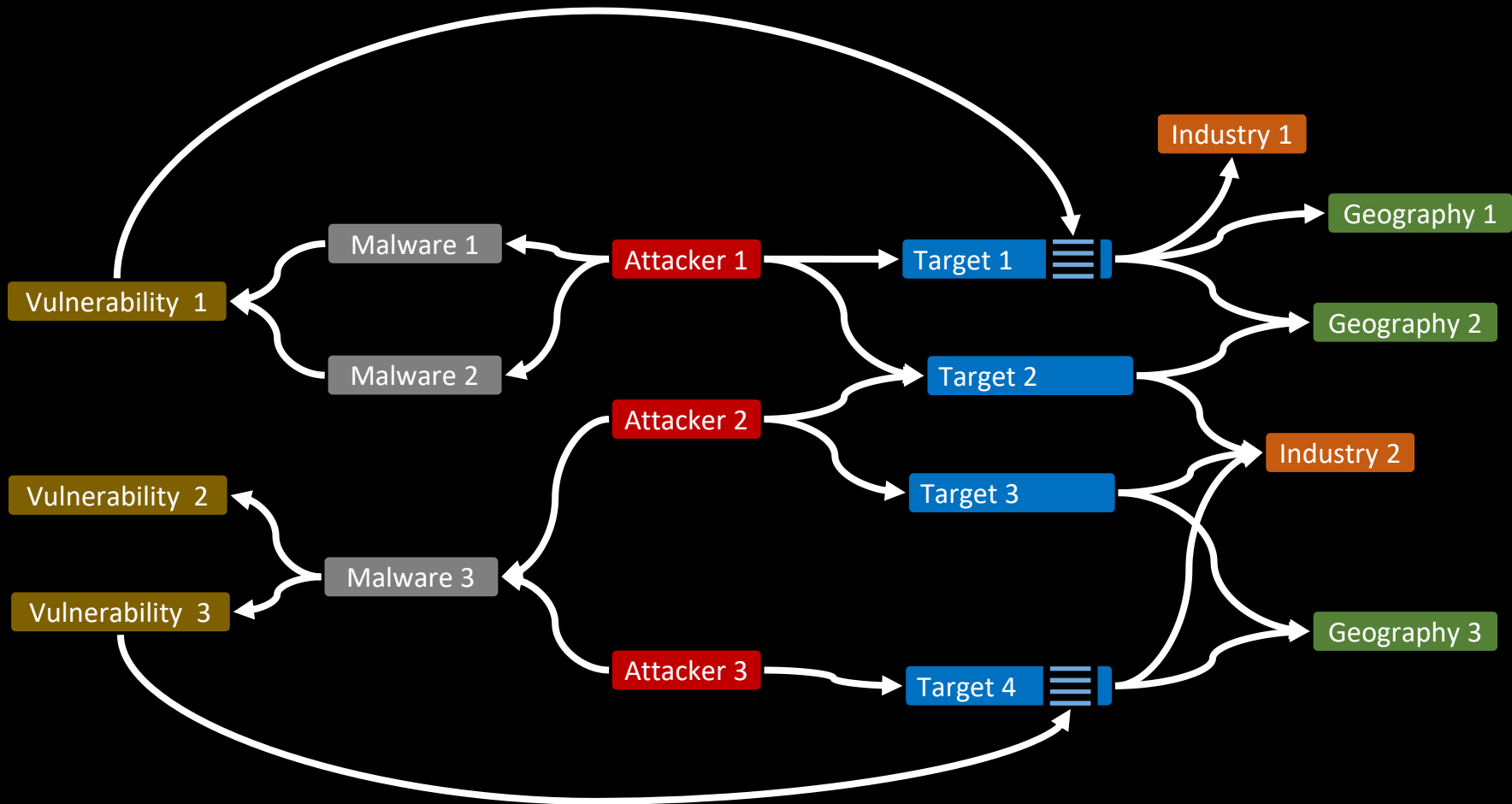


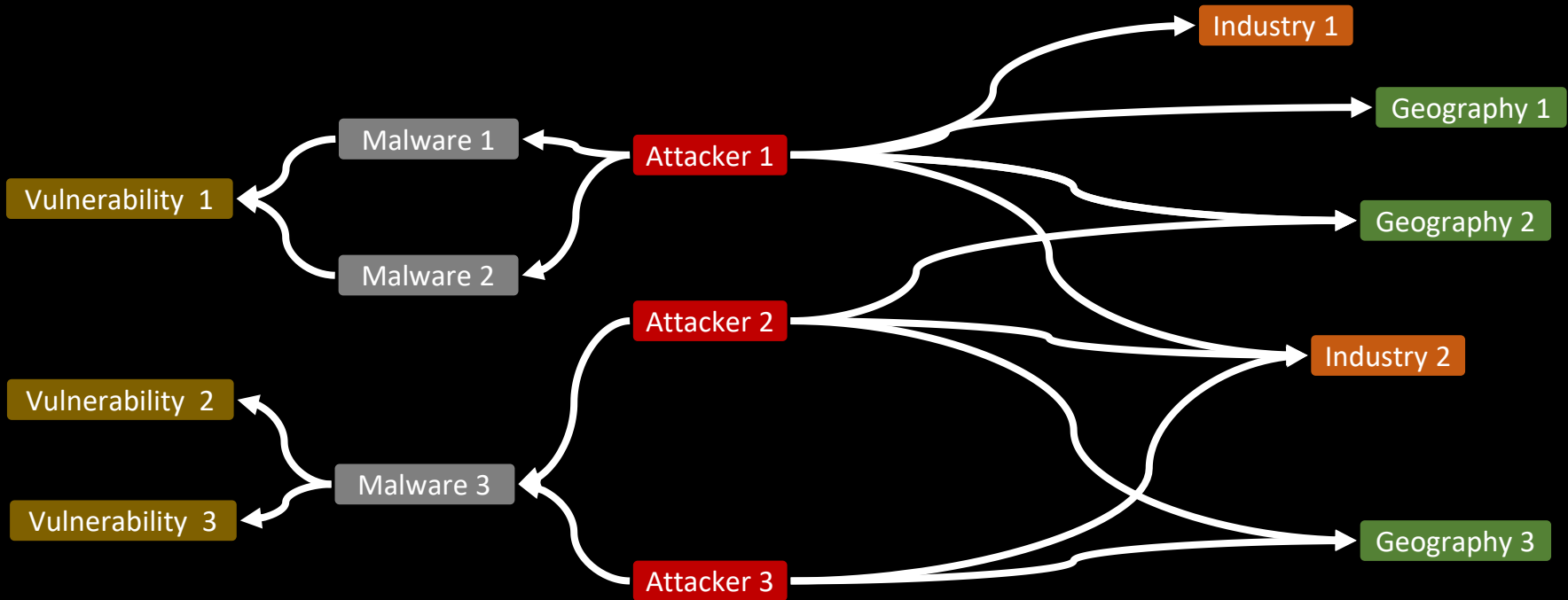
Opportunity



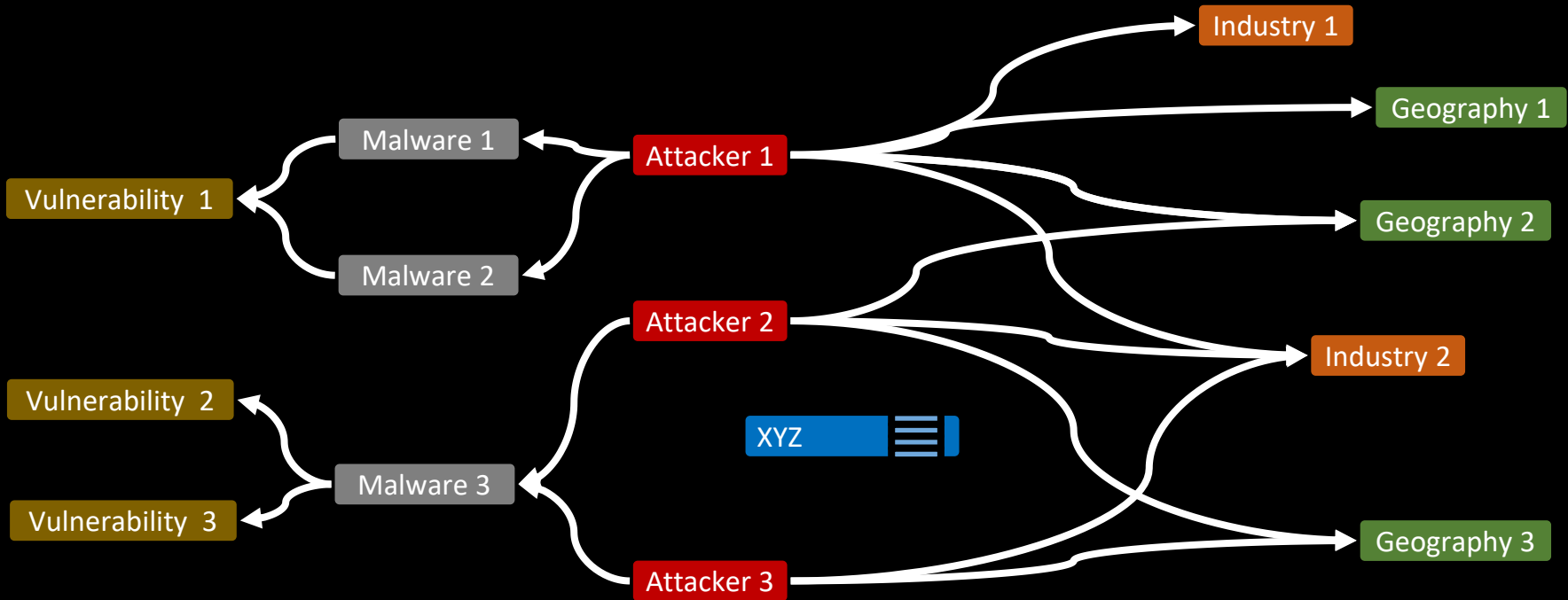


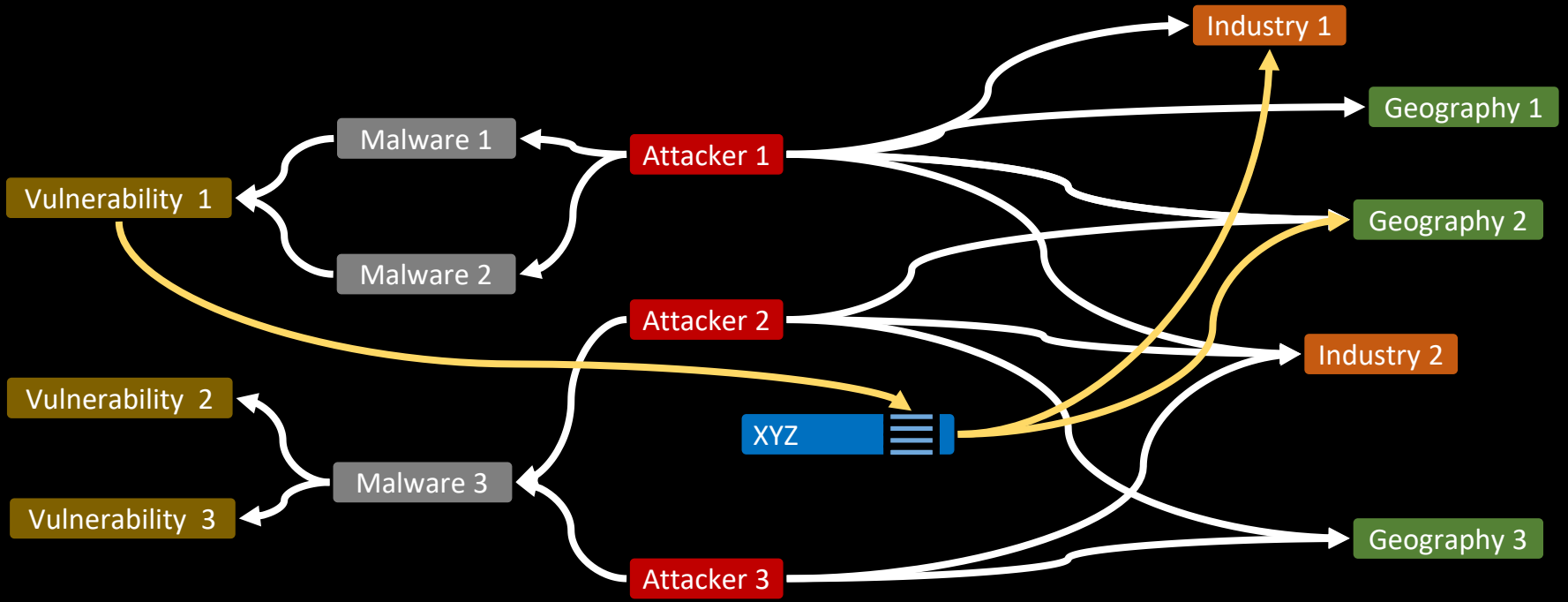


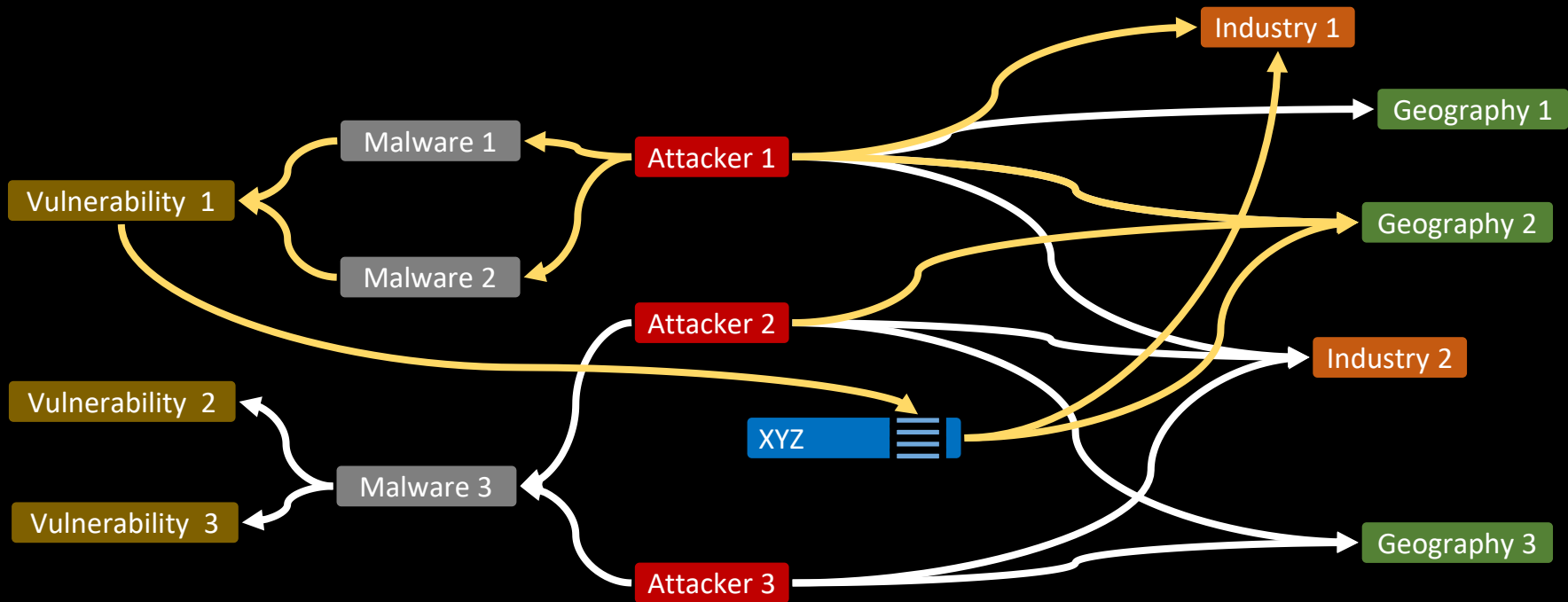




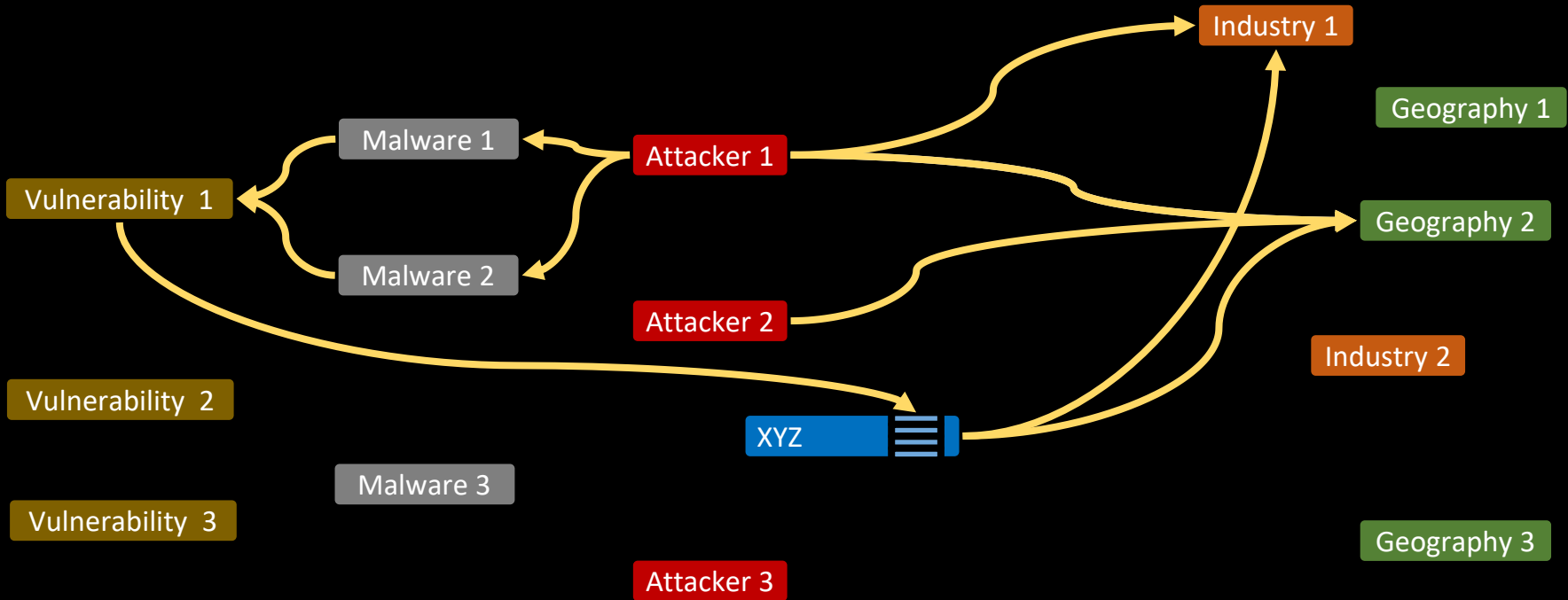




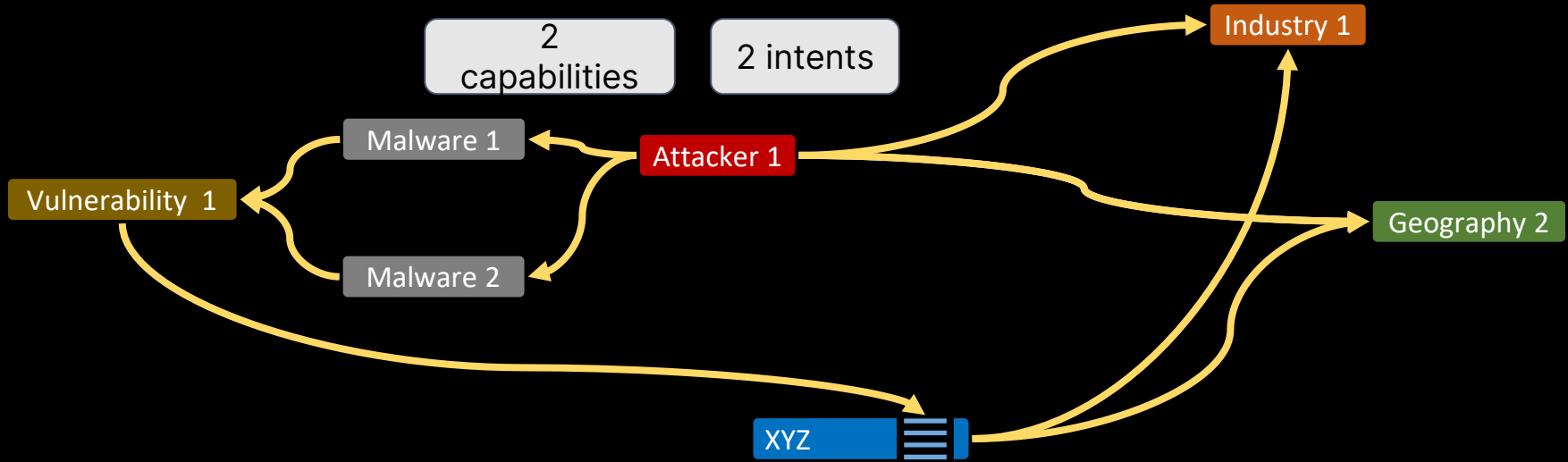




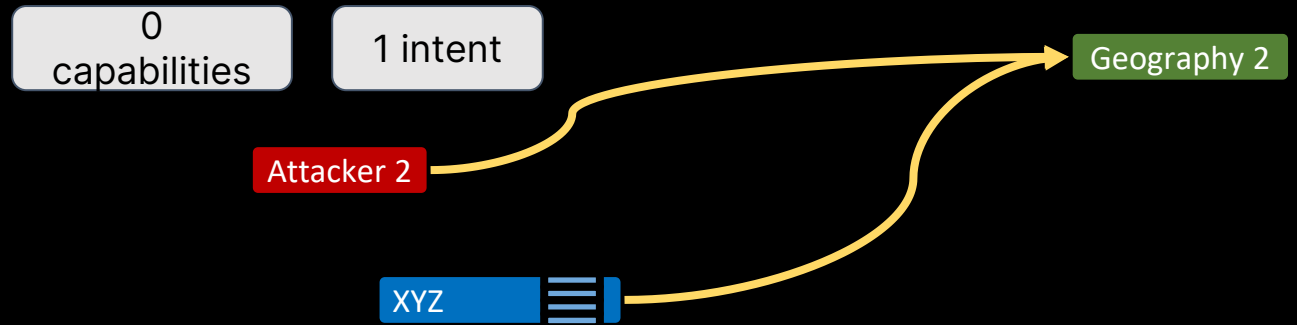




# Two Matching Intents, Two Matching Capabilities



# One Matching Intent, Zero Matching Capabilities



# No Connection!

XYZ 

Attacker 3

0  
capabilities

0 intents

2  
capabilities

2 intents

Attacker 1

0  
capabilities

1 intent

Attacker 2

Attacker 3

0  
capabilities

0 intents

2 capabilities

2 intents

Attacker 1

0  
capabilities

1 intent

Attacker 2

Attacker 3

0  
capabilities

0 intents



2  
capabilities

2 intents

Attacker 1

0  
capabilities

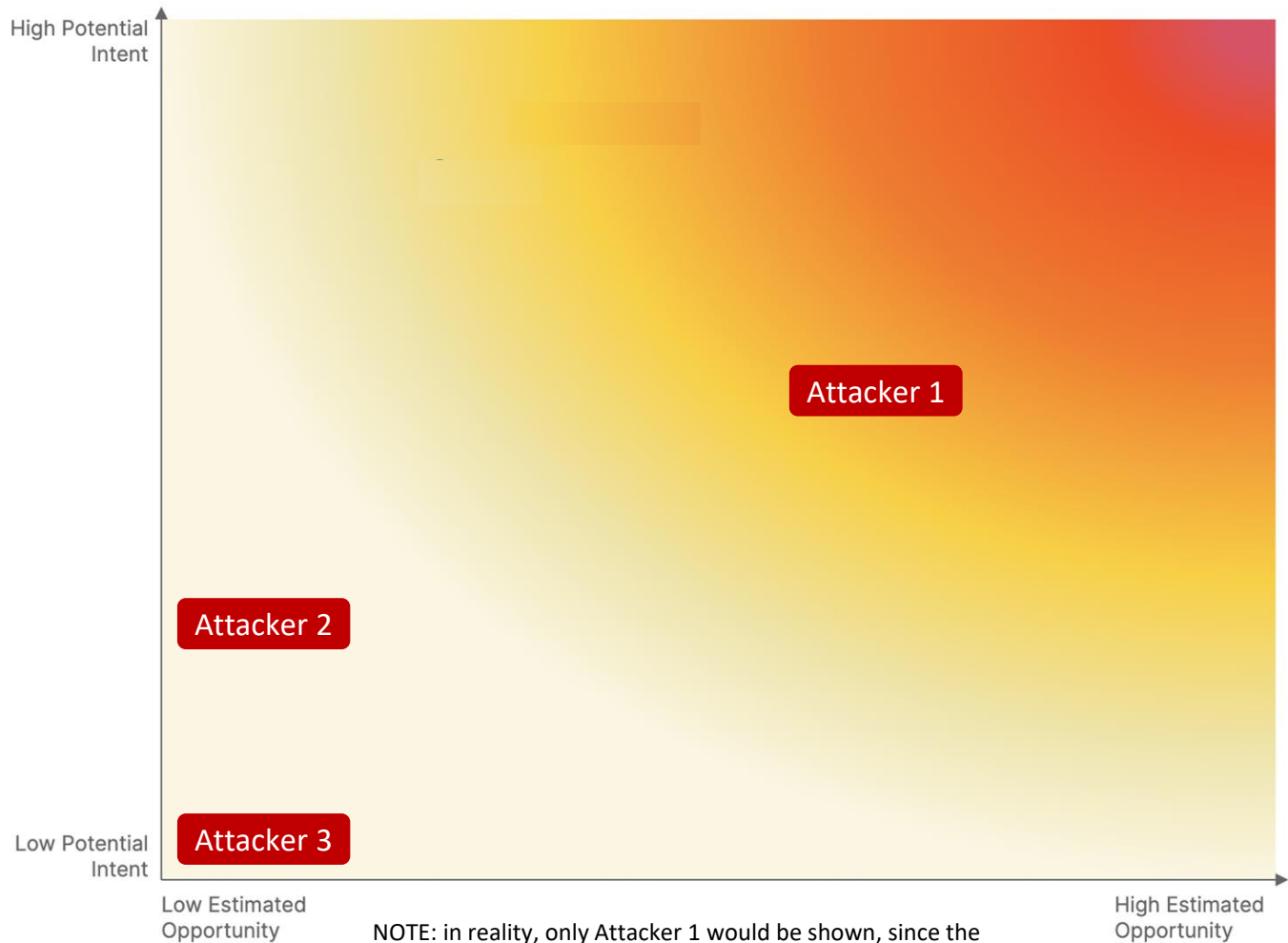
1 intent

Attacker 2

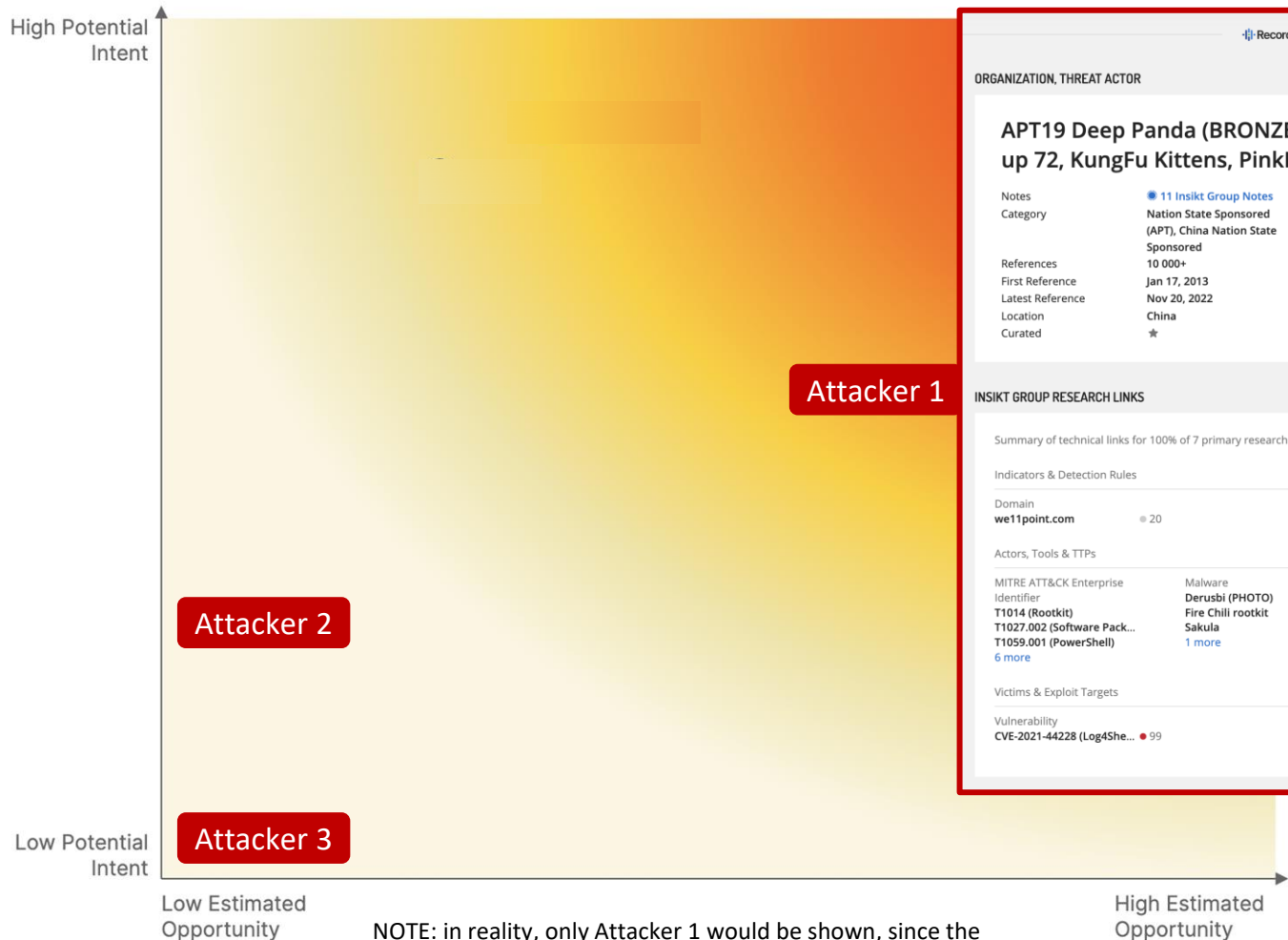
Attacker 3

0  
capabilities

0 intents



NOTE: in reality, only Attacker 1 would be shown, since the map requires some intent AND capability



Attacker 1

Attacker 2

Attacker 3

Recorded Future

ORGANIZATION, THREAT ACTOR

### APT19 Deep Panda (BRONZE FIRESTONE, Black Vine, Group 72, KungFu Kittens, PinkPanther, Shell Crew)

Notes 11 Insikt Group Notes Show recent events or cyber events

Category **Nation State Sponsored (APT), China Nation State Sponsored**

References **10 000+**

First Reference **Jan 17, 2013**

Latest Reference **Nov 20, 2022**

Location **China**

Curated **★**

---

INSIKT GROUP RESEARCH LINKS Learn More

Summary of technical links for 100% of 7 primary research notes between Nov 1, 2014 – Apr 5, 2022 Show in Table

Indicators & Detection Rules

---

Domain

**we11point.com** 20

---

Actors, Tools & TTPs

MITRE ATT&CK Enterprise Identifier	Malware
<b>T1014 (Rootkit)</b>	<b>Derusbi (PHOTO)</b>
<b>T1027.002 (Software Pack...)</b>	<b>Fire Chili rootkit</b>
<b>T1059.001 (PowerShell)</b>	<b>Sakula</b>
<a href="#">6 more</a>	<a href="#">1 more</a>

---

Victims & Exploit Targets

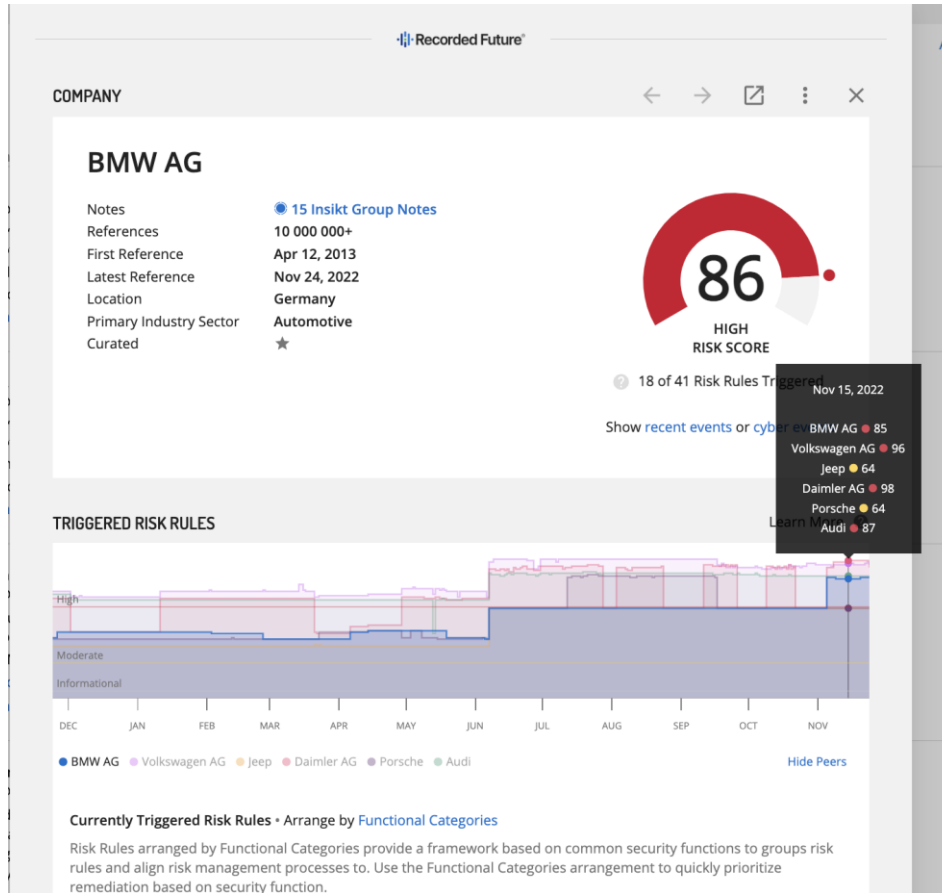
---

Vulnerability

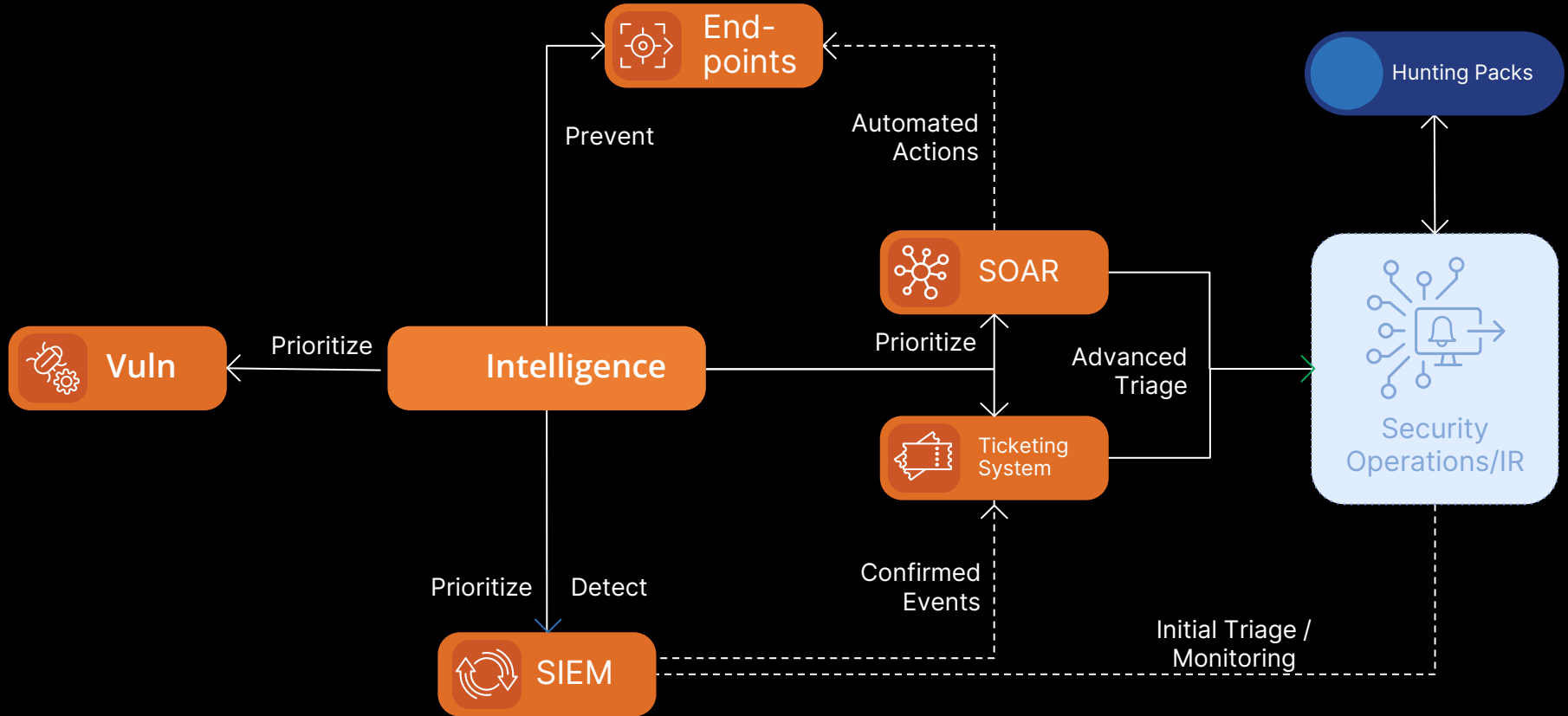
**CVE-2021-44228 (Log4She...)** 99

NOTE: in reality, only Attacker 1 would be shown, since the map requires some intent AND capability

# Automated Risk Scoring - A Measure of Resilience!



# The Modern Security Stack is Automated



# Thank you!

Staffan Truvé PhD  
*CTO & Co-Founder*  
[truve@recordedfuture.com](mailto:truve@recordedfuture.com)  
[@truve](https://twitter.com/truve)

