Kraken

SOC assessment

Meet KRAKEN

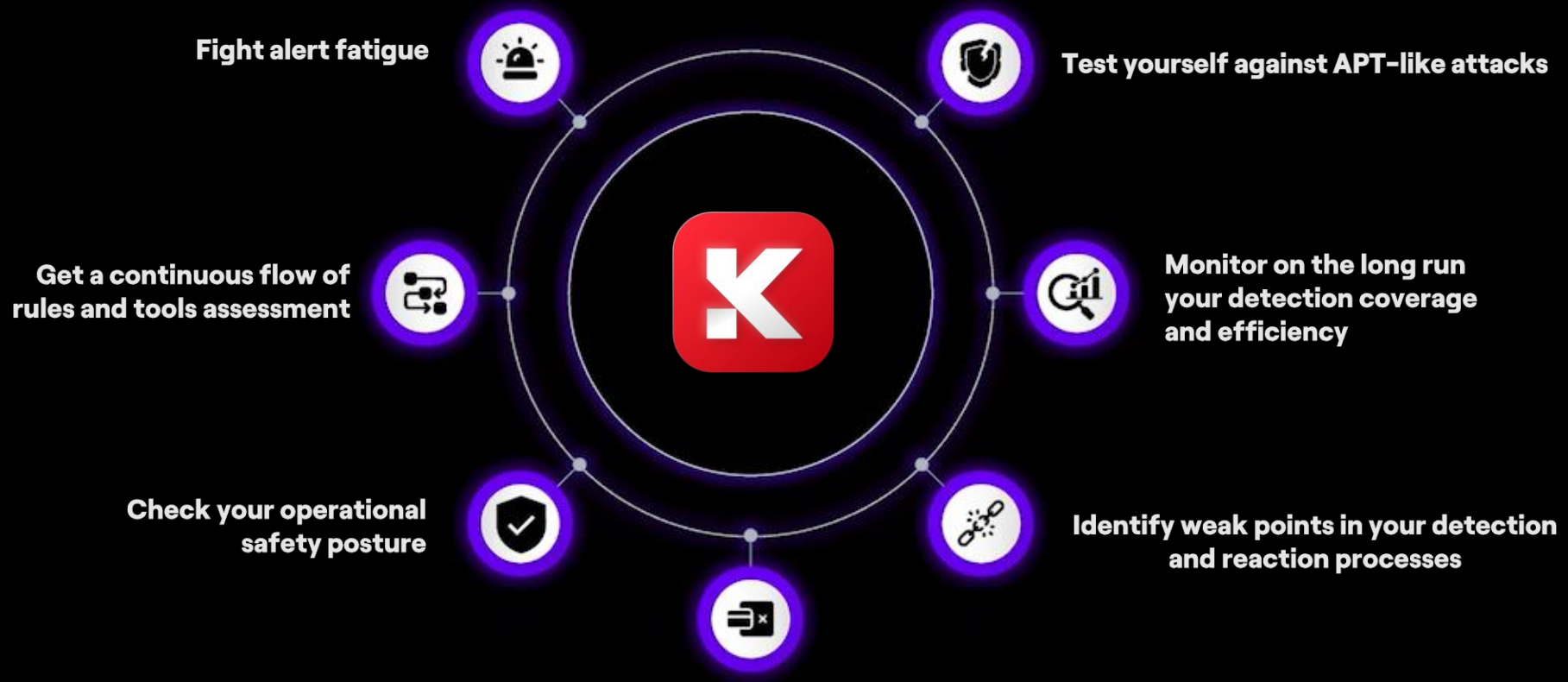
NEVERHACK

Meet KRAKEN

Faced with new challenges and cyber threats, organisations need to implement new strategies for assessing and training their Blue Teams in order to protect their assets.

Meet KRAKEN

How to assess and make your SOC viable?

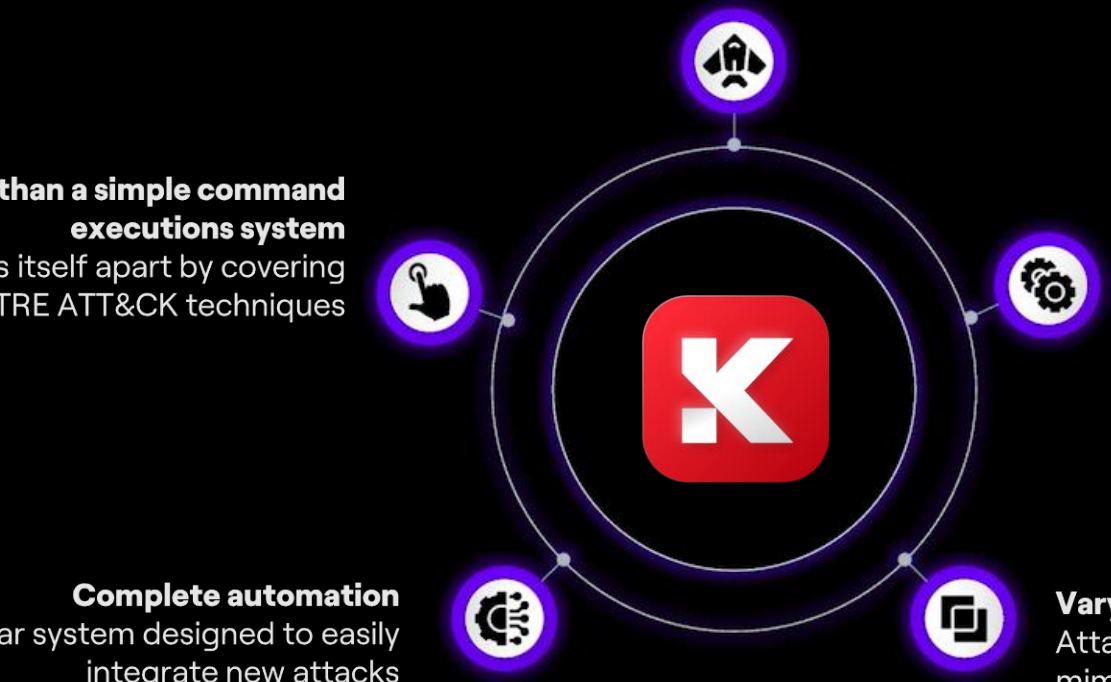


Meet KRAKEN

KRAKEN: An automatic attack engine

Sophisticated stealthy attacks
Any level of sophistication,
Most advanced APT
(files, shellcode only, ...)

For more than a simple command executions system
KRAKEN sets itself apart by covering all MITRE ATT&CK techniques



A proprietary engine
Implant, C2 and state-of-the-art proprietary module system, capable of emulating the stealthiest attacks

Complete automation
Modular system designed to easily integrate new attacks

Varying approachs
Attacks and killchains combinations to mimic a Red Team on demand and adapted for each business context

Meet KRAKEN

KRAKEN: Advanced capabilities

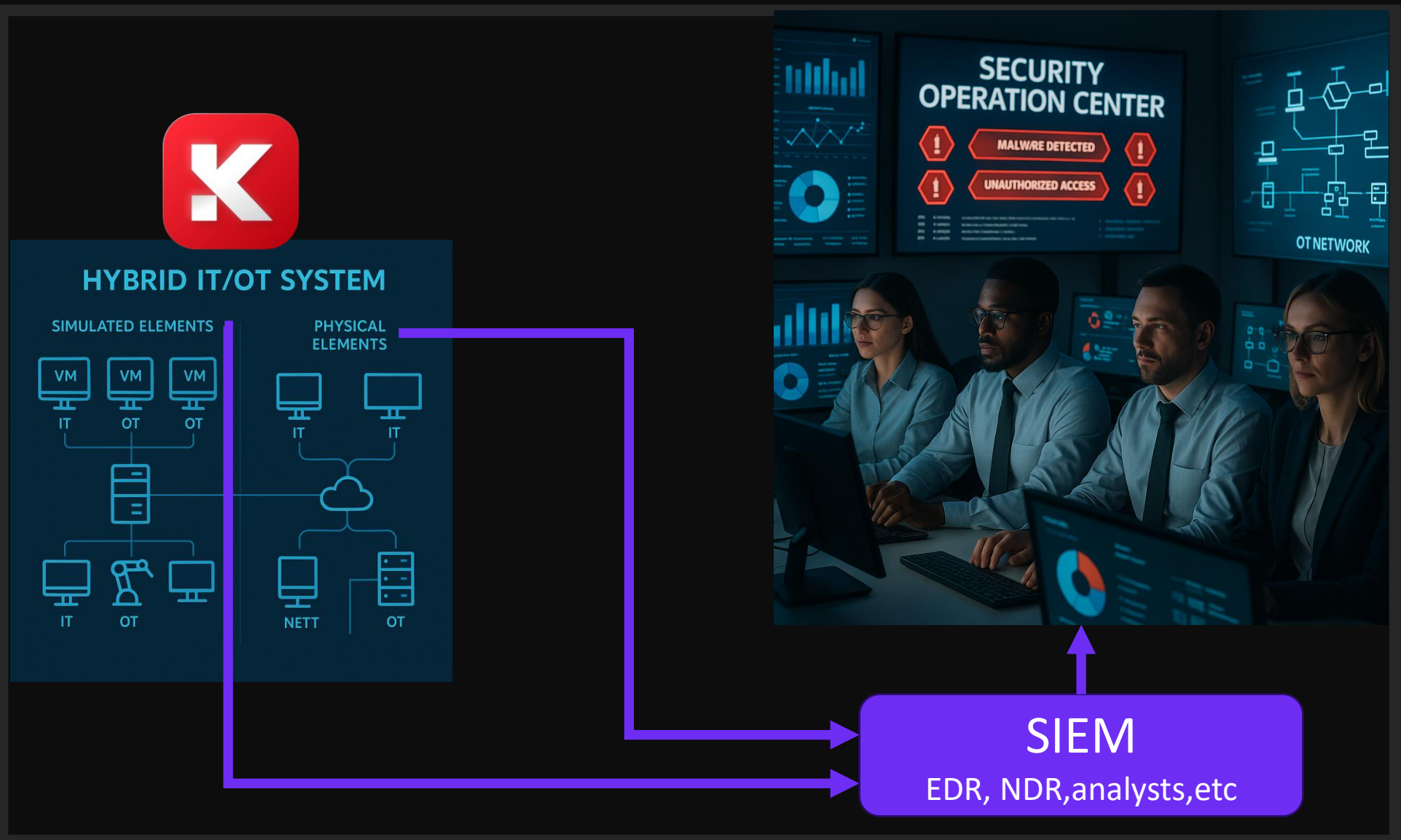
Meet KRAKEN

In the Operational Technologies (OT) sector, we are working in partnership with various Canadian companies. We began by integrating OPC UA to our system and are currently developing extensions for the Profibus and Profinet protocols. We will then look at other production line components.

Meet KRAKEN

KRAKEN evaluates the performance of SOCs (and not the Information System) to identify concrete areas for improvement thanks to a repository based on objective metrics ...

Meet KRAKEN



...and a robust attacks system involving simulated IS and/or real IS securely connected to your SOC (SIEM, EDR, NDR, etc).

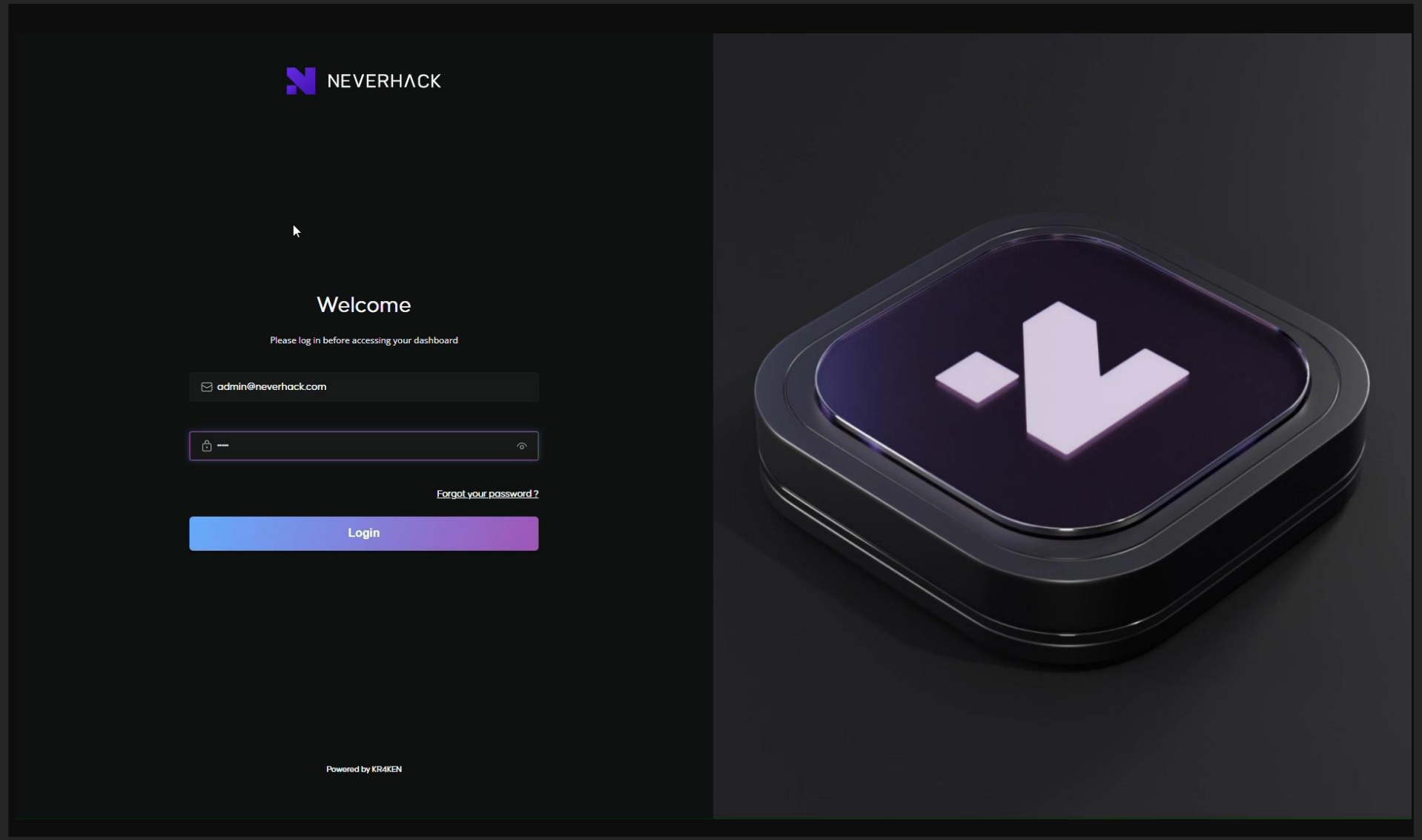
Meet KRAKEN

The interface

Demo: A SOC using KRAKEN with and advanced attack, life simulation and SIEM integration

Meet KRAKEN

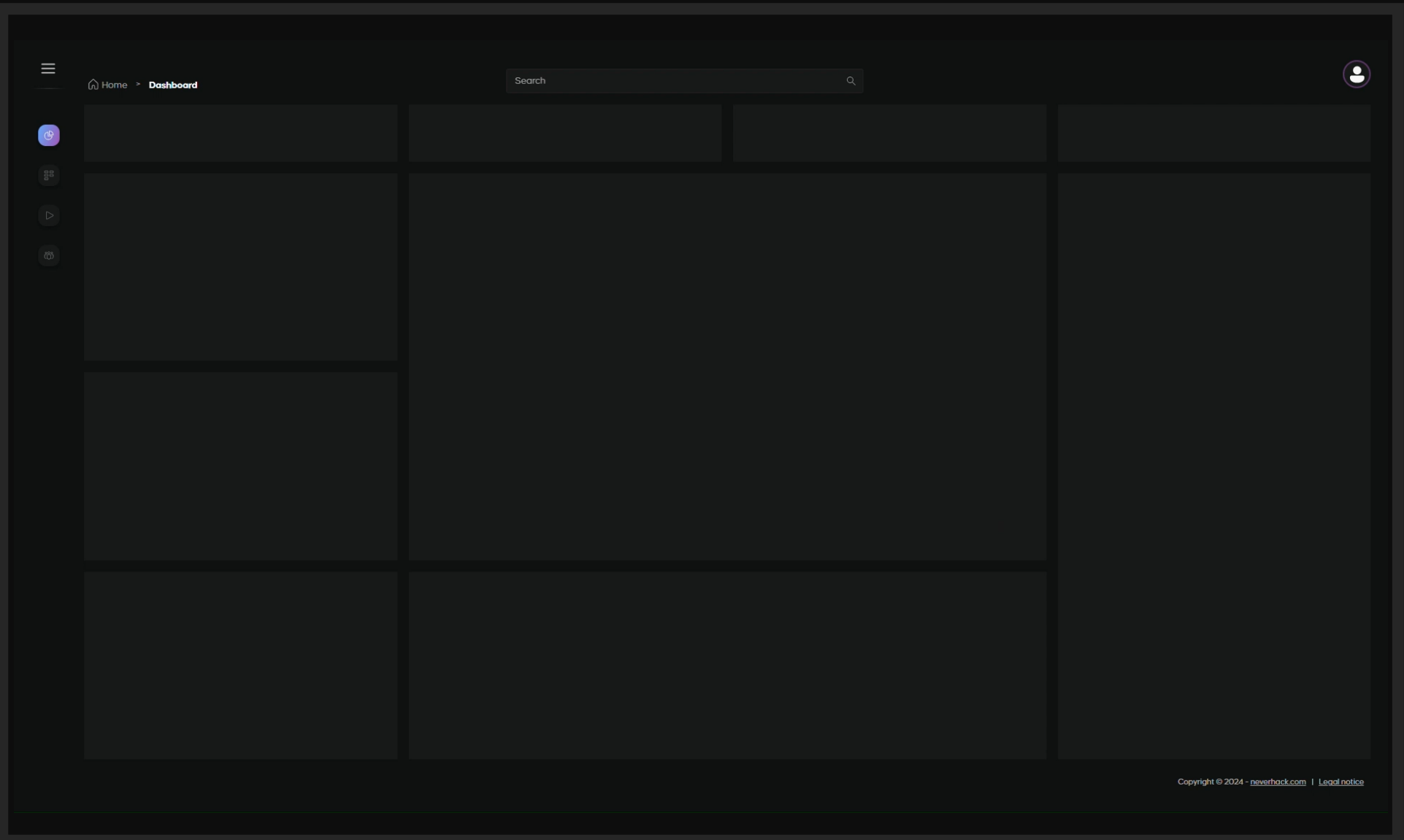
The interface



KRAKEN offers two different interfaces tailor made for both the manager and the analyst.

Meet KRAKEN

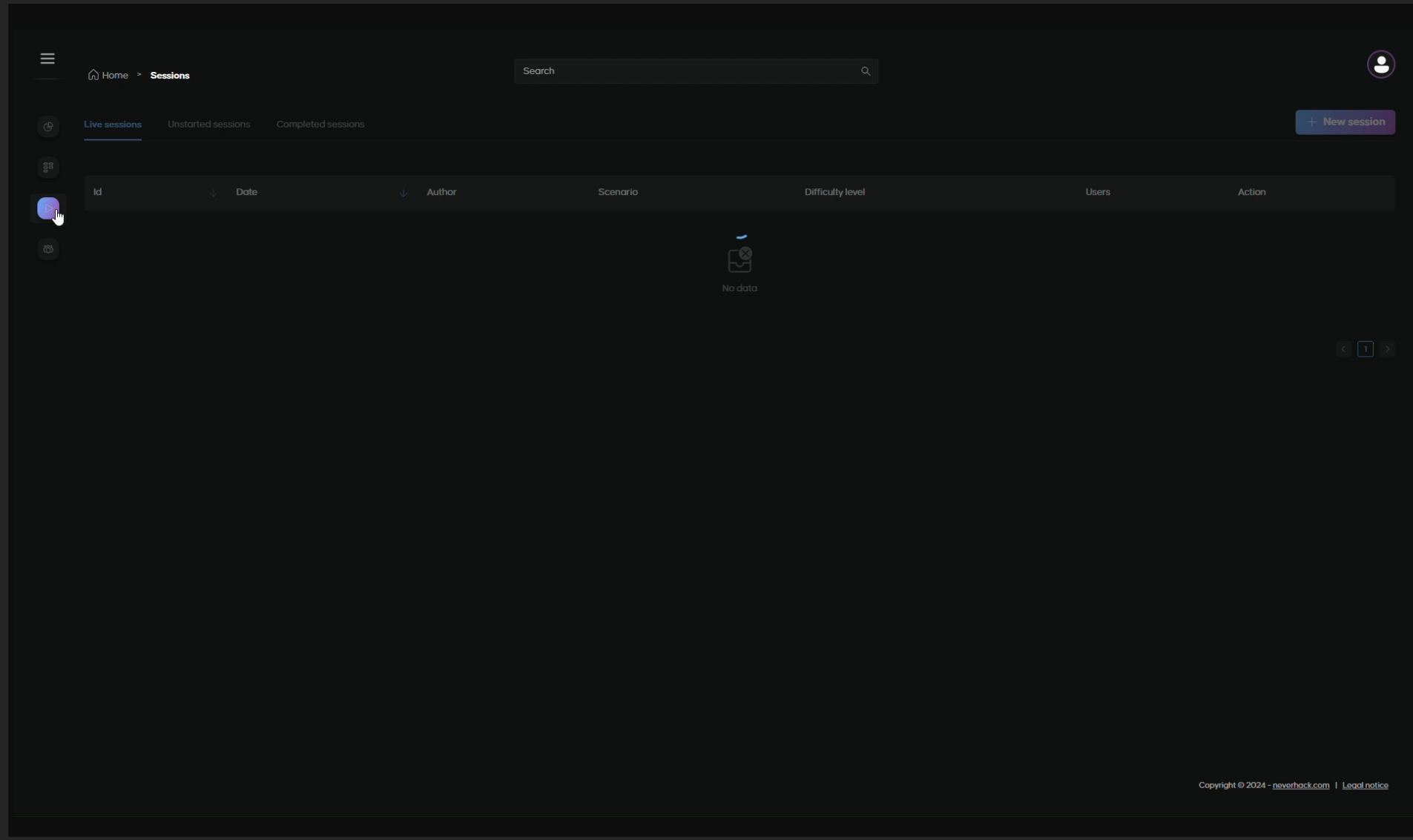
The interface



The manager interface provides an overview of session statistics, users and permissions, MITRE ATT&CK classification, and session management.

Meet KRAKEN

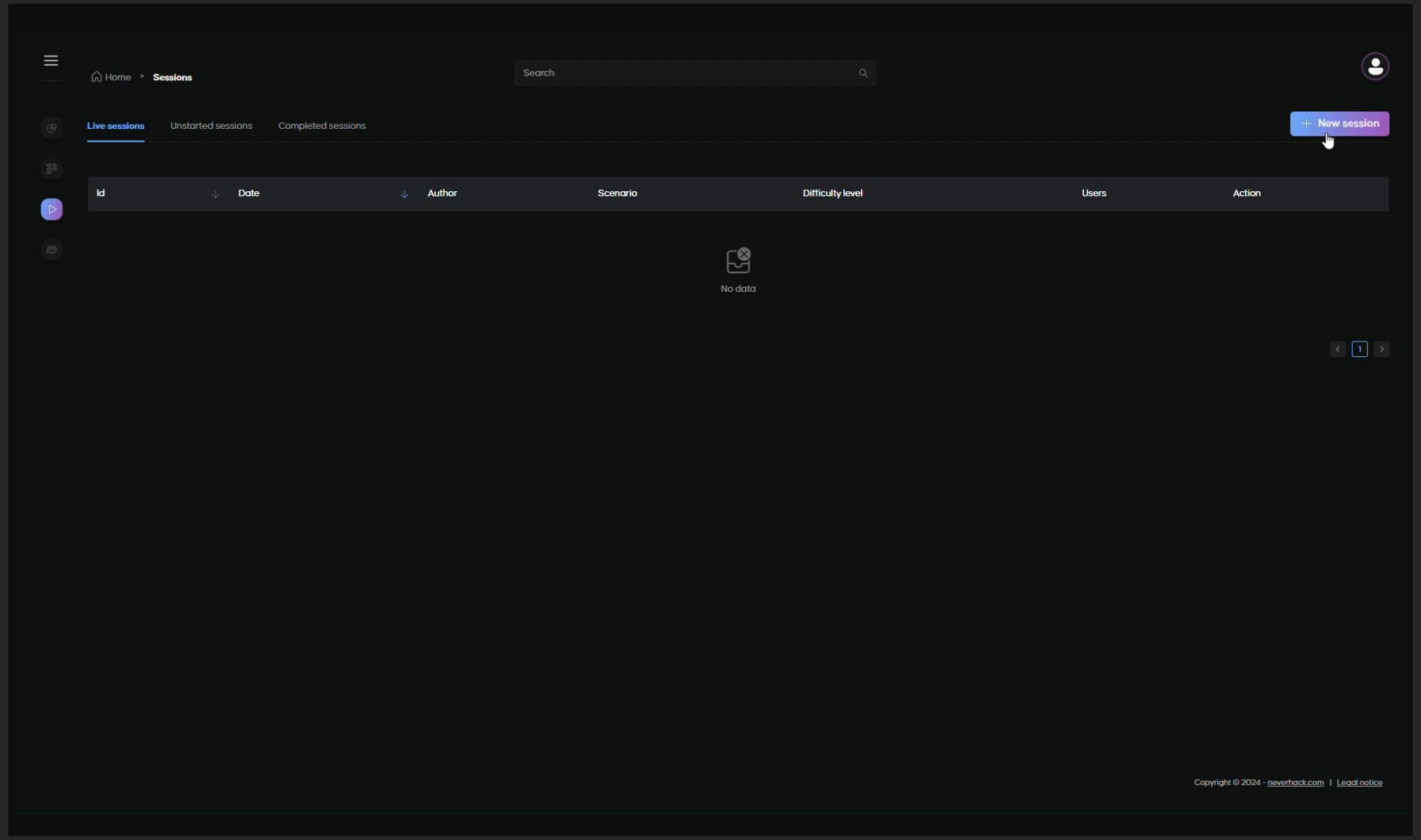
The interface



The manager creates the session.

Meet KRAKEN

The interface

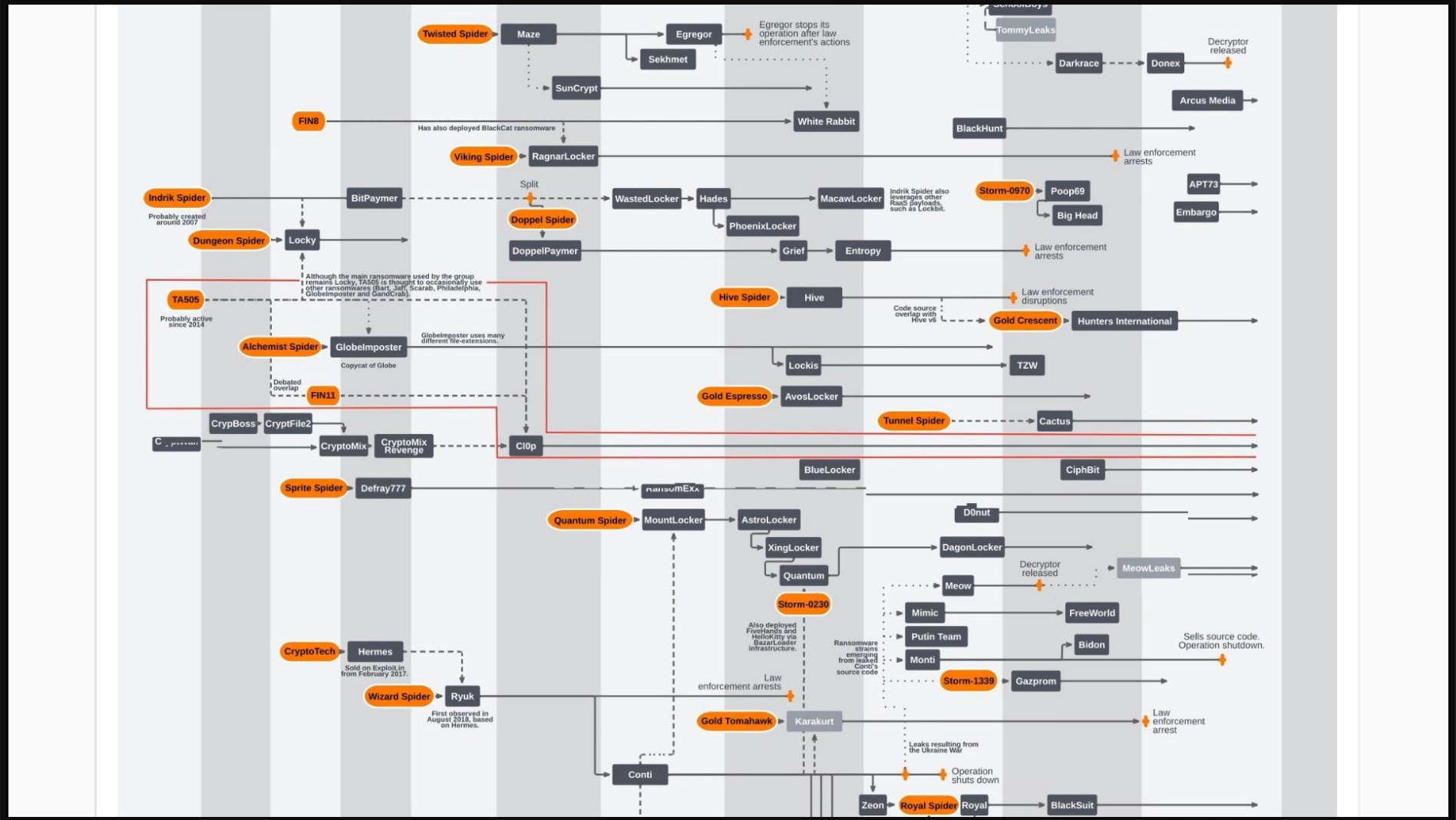


And chooses the attack scenario.

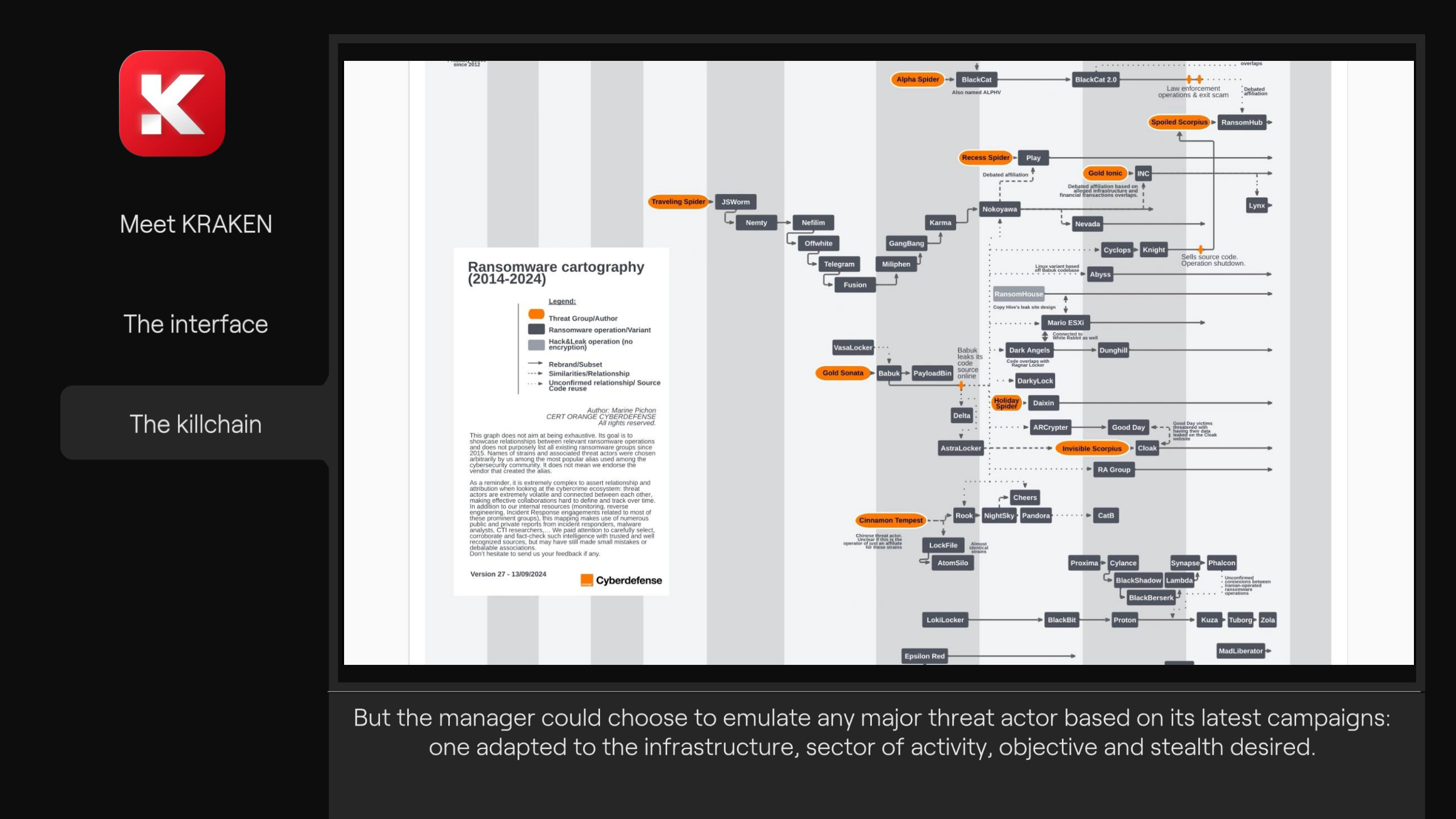
Meet KRAKEN

The interface

The killchain



As an example, we chose a real 2023 attack killchain from the well-known threat-actor FIN11.



Meet KRAKEN

The interface

The killchain

Ransomware cartography (2014-2024)

Legend:

- Threat Group/Author
- Ransomware operation/Variant
- Hack&Leak operation (no encryption)
- Rebrand/Subset
- Similarities/Relationship
- Unconfirmed relationship/ Source Code reuse

Author: Marine Pichon
CERT ORANGE CYBERDEFENSE
All rights reserved.

This graph does not aim at being exhaustive. Its goal is to showcase relationships between relevant ransomware operations and does not purposely list all existing ransomware groups since 2015. Names of strains and associated threat actors were chosen arbitrarily by us among the most popular alias used among the cybersecurity community. It does not mean we endorse the vendor that created the alias.

As a reminder, it is extremely complex to assert relationship and attribution when looking at the cybercrime ecosystem: threat actors are extremely volatile and connected between each other, making effective collaborations hard to define and track over time. In addition to our internal resources (monitoring, reverse engineering, Incident Response engagements related to most of these prominent groups), this mapping makes use of numerous public and private reports from incident responders, malware analysts, CTI researchers,... We paid attention to carefully select, corroborate and fact-check such intelligence with trusted and well recognized sources, but may have still made small mistakes or debatable associations.
Don't hesitate to send us your feedback if any.

Version 27 - 13/09/2024

Cyberdefense

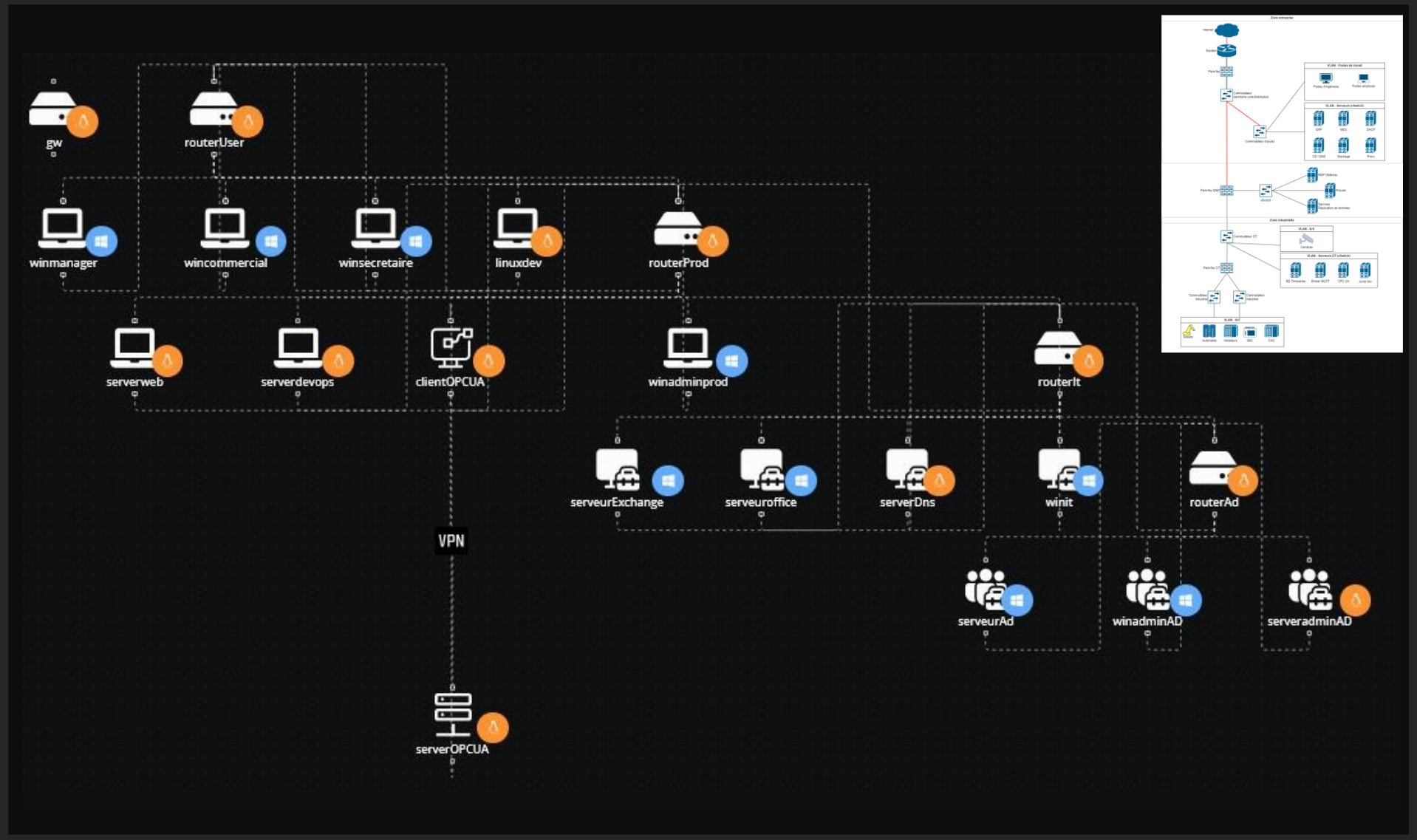
Alpha Spider
BlackCat
Also named ALPHV
BlackCat 2.0
Law enforcement operations & exit scam
Debated affiliation
Spoiled Scorpius
RansomHub
Recess Spider
Play
Debated affiliation
Gold Ionic
INC
Debated affiliation based on alleged infrastructure and financial transactions overlaps.
Lynx
Traveling Spider
JSWorm
Nemty
Nefilim
Offwhite
Telegram
Fusion
Miliphen
GangBang
Karma
Nokoyawa
Nevada
Cyclops
Knight
Sells source code. Operation shutdown.
Linux variant based off Babuk codebase
Abyss
RansomHouse
Copy Hive's leak site design
Mario ESXi
Connected to White Rabbit as well
VasaLocker
Gold Sonata
Babuk
PayloadBin
Babuk leaks its code source online
Dark Angels
Code overlaps with Ragnar Locker
Dunghill
DarkyLock
Holiday Spider
Daixin
Delta
ARCrypter
Good Day
Good Day victims threatened with having their data leaked on the Cloak website
AstraLocker
Invisible Scorpius
Cloak
RA Group
Cheers
Cinnamon Tempest
Rook
NightSky
Pandora
CatB
Chinese threat actor. Unclear if this is the operator of just an affiliate for these strains
LockFile
Almost identical strains
AtomSilo
Proxima
Cylance
Synapse
Phalcon
BlackShadow
Lambda
BlackBerserk
Unconfirmed connexions between Iranian-operated ransomware operations
LokiLocker
BlackBit
Proton
Kuza
Tuborg
Zola
Epsilon Red
MadLiberator

But the manager could choose to emulate any major threat actor based on its latest campaigns: one adapted to the infrastructure, sector of activity, objective and stealth desired.

Meet KRAKEN

The interface

The killchain



Thanks to Kraken automated and customizable infrastructure system, we can deploy a topology adapted to the chosen FIN11 OT killchain.

Meet KRAKEN

The interface

The killchain

Life trafic

File View Server Document Settings Help

Project

Project
Servers
toto@10.10.10.2
Documents
Data Access View

Data Access View

CurrentTime: 2025-04-22 07:28:44.452033

Attributes

Attribute	Value
NodeId	i=11492 [Serv
NamespaceIndex	0
IdentifierType	Numeric
Identifier	11492 [Server
NodeClass	Method
BrowseName	0, "GetMonitor
DisplayName	"", "GetMonito
Description	BadAttributeId
Executable	true

Address Space

No Highlight

Server
Auditing
Dictionaries
EstimatedReturnTime
GetMonitoredItems
LocalTime
NamespaceArray
Namespaces
PublishSubscribe

References

Forward

Reference	Target DisplayName
HasProperty	InputArguments
HasProperty	OutputArguments

Log

Timestamp	Source	Server	Message
22 Apr 2025 07:25:47.713	Attribute Plugin	toto@10.10.10.2	Read attributes of node 'NS0|Numeric|17594' succeeded [ret = Good].
22 Apr 2025 07:25:47.724	Reference Plugin	toto@10.10.10.2	Browse succeeded.
22 Apr 2025 07:25:48.611	Attribute Plugin	toto@10.10.10.2	Read attributes of node 'NS0|Numeric|2255' succeeded [ret = Good].
22 Apr 2025 07:25:48.614	Reference Plugin	toto@10.10.10.2	Browse succeeded.
22 Apr 2025 07:25:49.028	Attribute Plugin	toto@10.10.10.2	Read attributes of node 'NS0|Numeric|17634' succeeded [ret = Good].
22 Apr 2025 07:25:49.030	Reference Plugin	toto@10.10.10.2	Browse succeeded.
22 Apr 2025 07:25:49.524	Attribute Plugin	toto@10.10.10.2	Read attributes of node 'NS0|Numeric|12885' succeeded [ret = Good].
22 Apr 2025 07:25:49.525	Reference Plugin	toto@10.10.10.2	Browse succeeded.
22 Apr 2025 07:25:50.083	Attribute Plugin	toto@10.10.10.2	Read attributes of node 'NS0|Numeric|2994' succeeded [ret = Good].
22 Apr 2025 07:25:50.084	Reference Plugin	toto@10.10.10.2	Browse succeeded.
22 Apr 2025 07:25:50.650	Attribute Plugin	toto@10.10.10.2	Read attributes of node 'NS0|Numeric|11492' succeeded [ret = Good].
22 Apr 2025 07:25:50.650	Reference Plugin	toto@10.10.10.2	Browse succeeded.

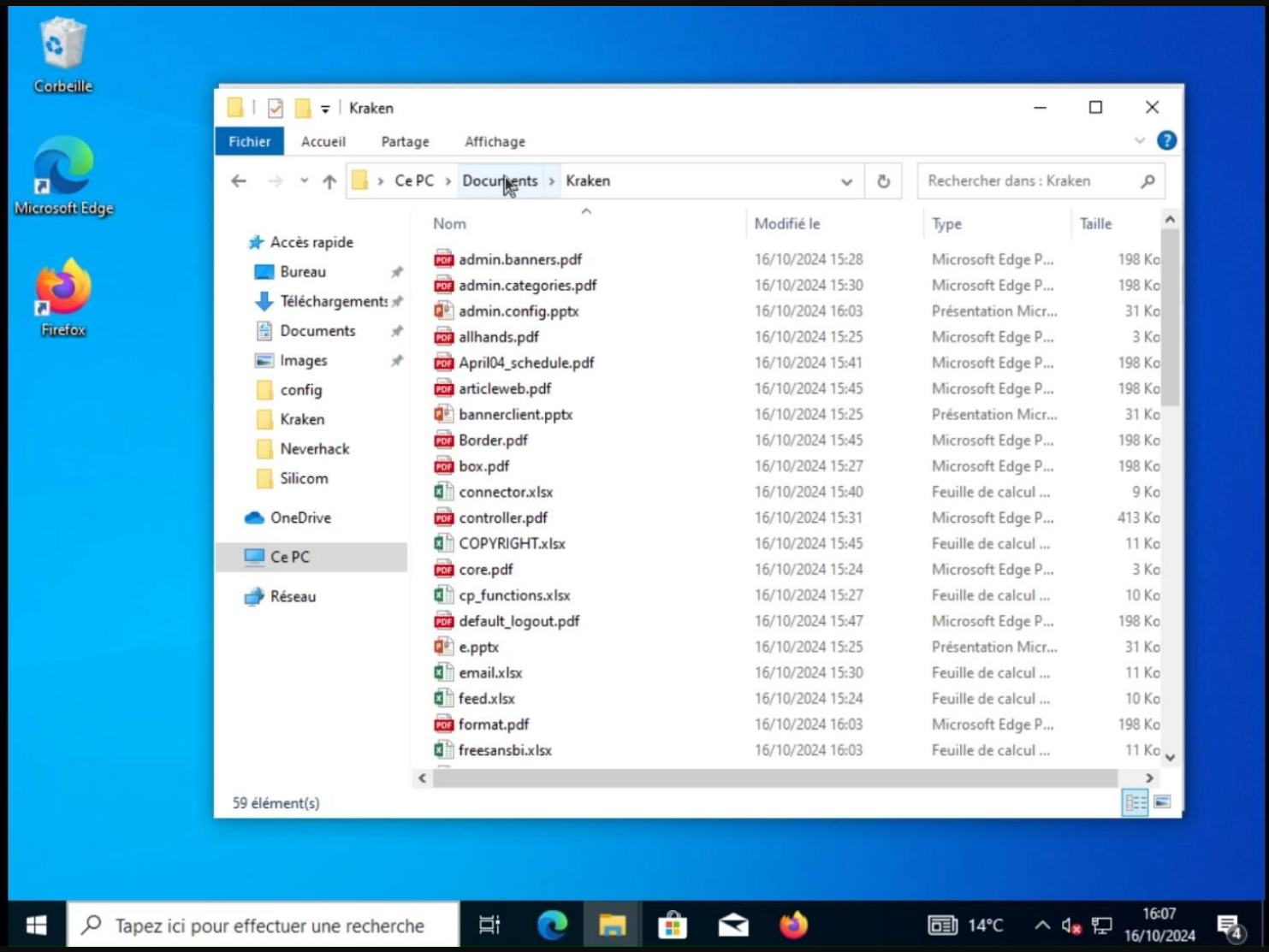
The chosen infrastructure is also animated with a life simulation OT system (OPC UA for example).

Meet KRAKEN

The interface

The killchain

Life trafic



And also the life simulation IT part of SCADA network to make it even more real for the SOC.

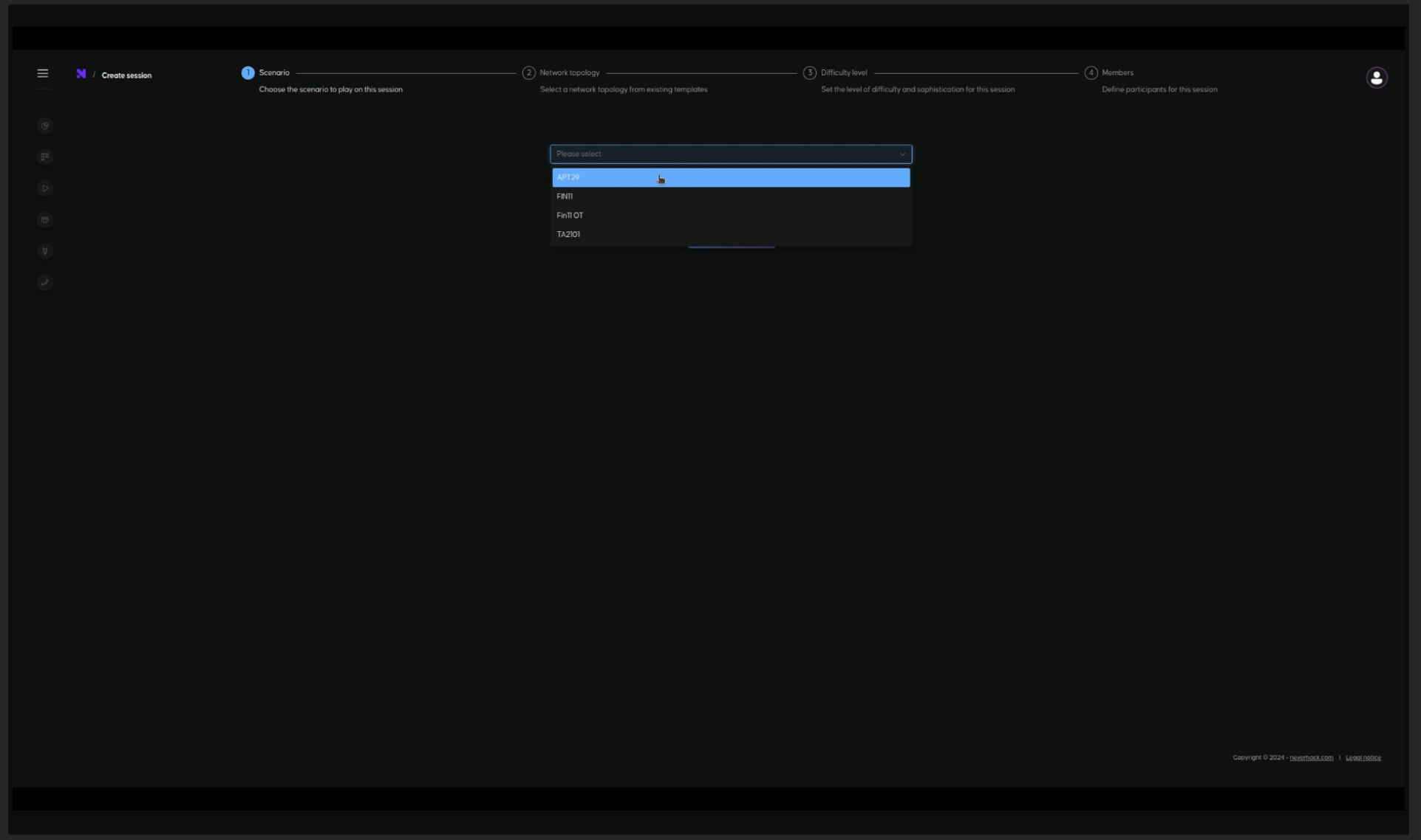
Meet KRAKEN

The interface

The killchain

Life trafic

Attack session



Let’s go back to the session creation by the manager. He chooses the attacker type then the adapted target network topology. The manager picks a level of difficulty for the killchain. Kraken will then adapt accordingly its attacks’ sophistication level. Finally, the manager selects the session participants.

Meet KRAKEN

The interface

The killchain

Life trafic

Attack session

```
Summary
WaitImplant: Implant 1 has connected

ListImplants
Summary
ListImplants: [1]

GetImplant
Summary
GetImplant: {'id': {'inner': '81e03a27-8f5c-4849-9dde-d862fb2e67b2'}, 'interfaces': [{'name': 'Ethernet 2', 'macAddr': 'BC:24:11:BE:61:67', 'v6': {'ip': 'fe80::fa7d:186b:cb0d:27d1'}}, {'name': 'Et
hernet 2', 'macAddr': 'BC:24:11:BE:61:67', 'v4': {'ip': '192.168.10.5', 'broadcast': '192.168.10.255', 'netmask': '255.255.255.0'}}]}

Initialising the environment with the initial target : 192.168.10.5
-------- Env Init----------
{'sub_networks': [SubNetwork(ip_network=None, machines=[Machine(os=None, usage=None, ip_addresses=[IPv4Address('192.168.10.5')], implants=[Implant(privileges=ImplantPrivilege(), id=1)], credential
s={}, hostname='', ports=[])])], 'credentials': defaultdict(<class 'dict'>, {}), 'dns_ips': [], 'hashes': []}
--------------------------
Adding scenarios/LISI_DEMO_OT/windows_secretary_sequence.yaml
ExecuteModule intern/credential_access/mimikatz;
  parameters: {'args': '"privilege::debug" "lsadump::lsa /inject" exit'};
  payloads: {}

[*]
  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # privilege::debug
ERROR kuhl_m_privilege_simple ; RtlAdjustPrivilege (20) c0000061

mimikatz(commandline) # lsadump::lsa /inject
ERROR kuhl_m_lsadump_lsa_getHandle ; OpenProcess (0x00000005)
ERROR kuhl_m_lsadump_lsa ; SamConnect c0000022

mimikatz(commandline) # exit
Bye!

hostname silicom

Getting info for module_name: "intern/credential_access/mimikatz"

Sending stats to the OrchClient : hostname: "silicom\n"
result: "Success"
technique: "T1003"
tactic: "TA0006"
tactic_name: "CredentialAccess"
timestamp: "2025-05-07T07:46:29.189858+00:00"
targets: "192.168.10.5"
source: "192.168.10.5"

Summary
[SUCCESS]: {'result': 'Exe has terminated'}

ExecuteModule intern/discovery/port_scan;
  parameters: {'ip': '192.168.10.3'};
  payloads: {}
```

Once all the participants are connected to the session, the session can start. Under the hood, this will trigger the initial access inside the target network and the attack starts.

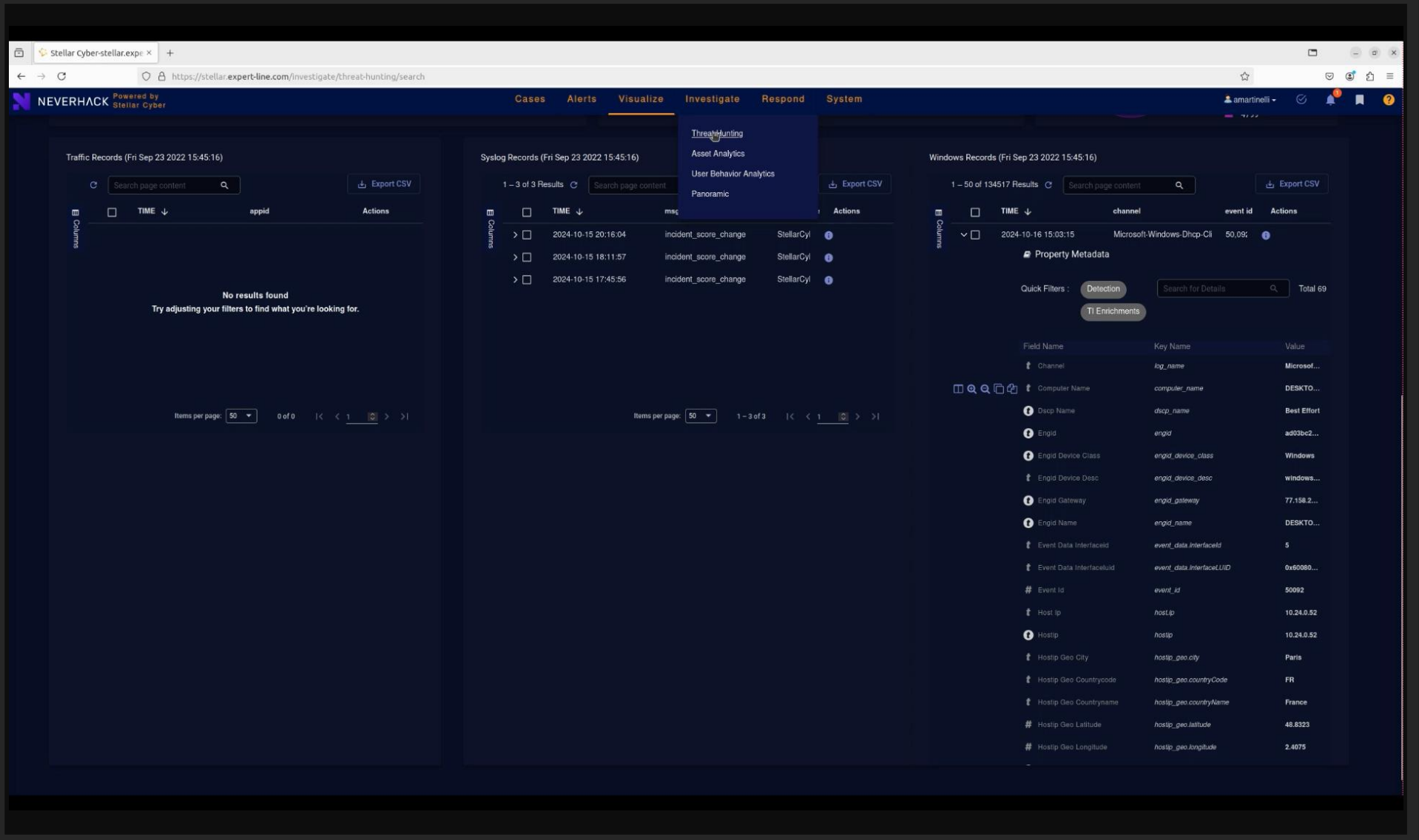
Meet KRAKEN

The interface

The killchain

Life trafic

Attack session



The resulting alerts within the SIEM will vary according to the level of difficulty chosen for the session. Here is a summary of all the detected attacks in the SIEM.

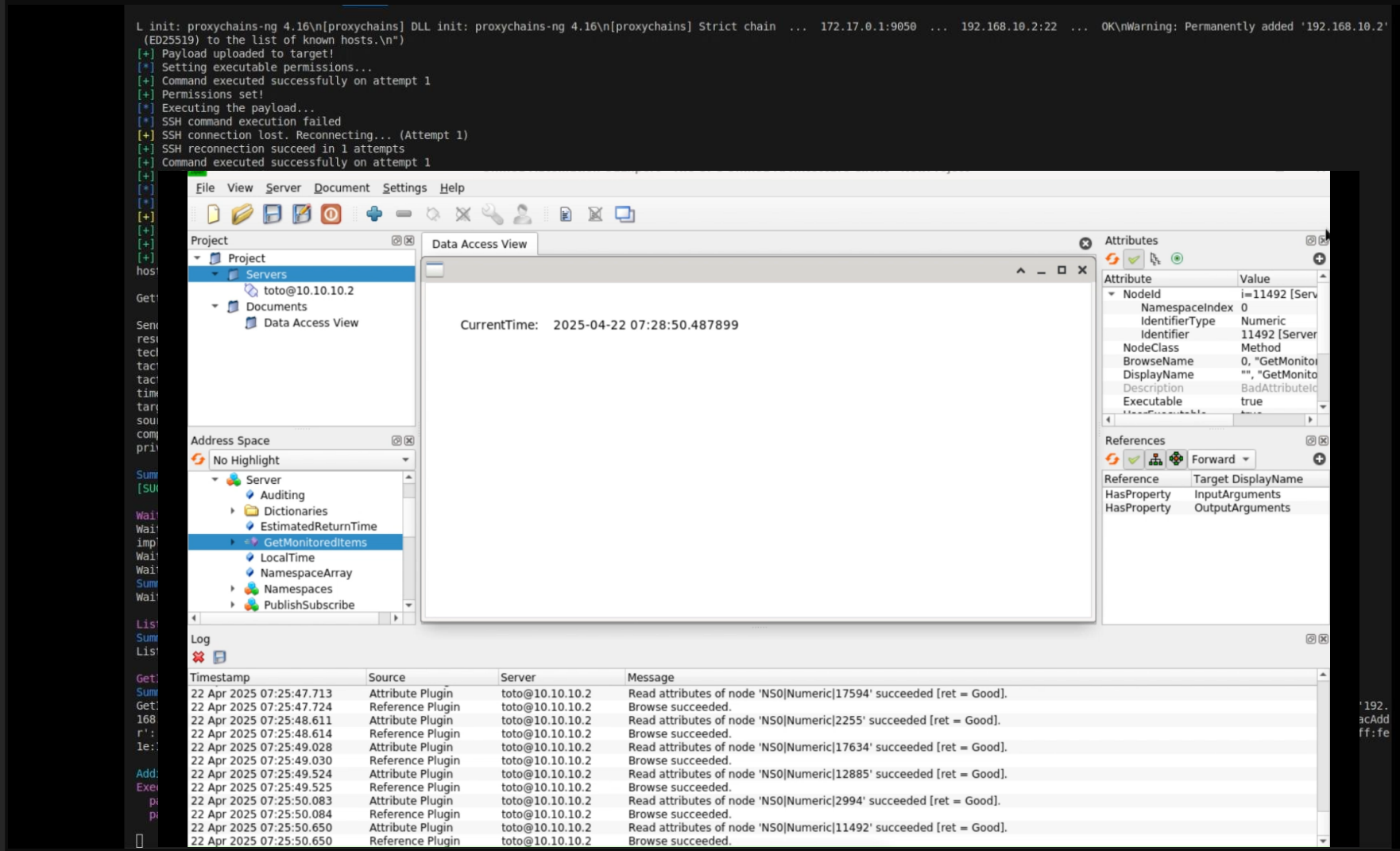
Meet KRAKEN

The interface

The killchain

Life trafic

Attack session



When the attack ends (in our case, when the OPC UA server goes down), the KRAKEN session remains active and the analysts can still access the KRAKEN session interface.

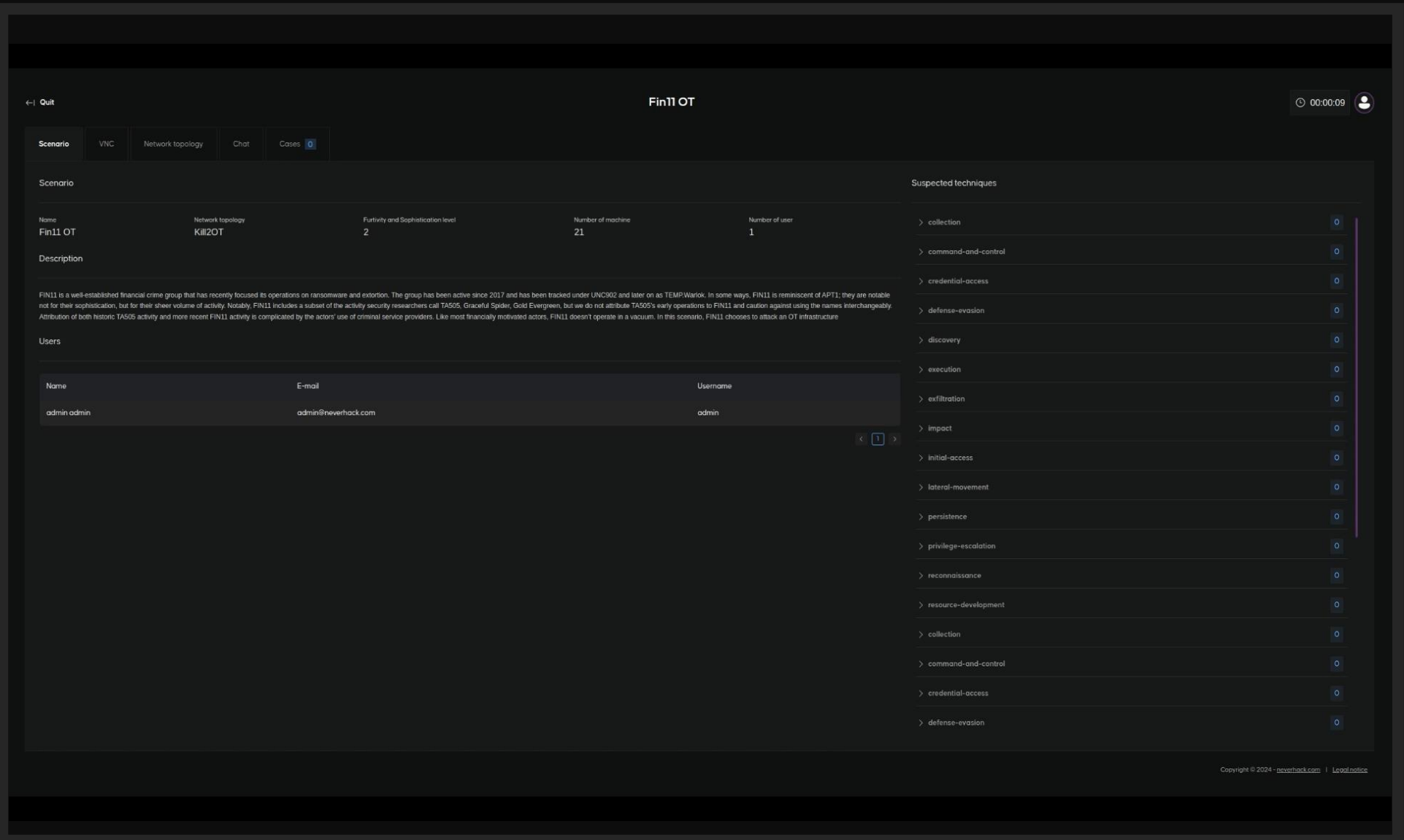
Meet KRAKEN

The interface

The killchain

Life trafic

Attack session



The SIEM alerts help the analysts detect attacks meant to be reported as cases of detection within Kraken. They specify the compromised machine, the technique detected and a description. The entire analyst team can report any detected malicious behaviour by creating Kraken cases during the session.

Meet KRAKEN

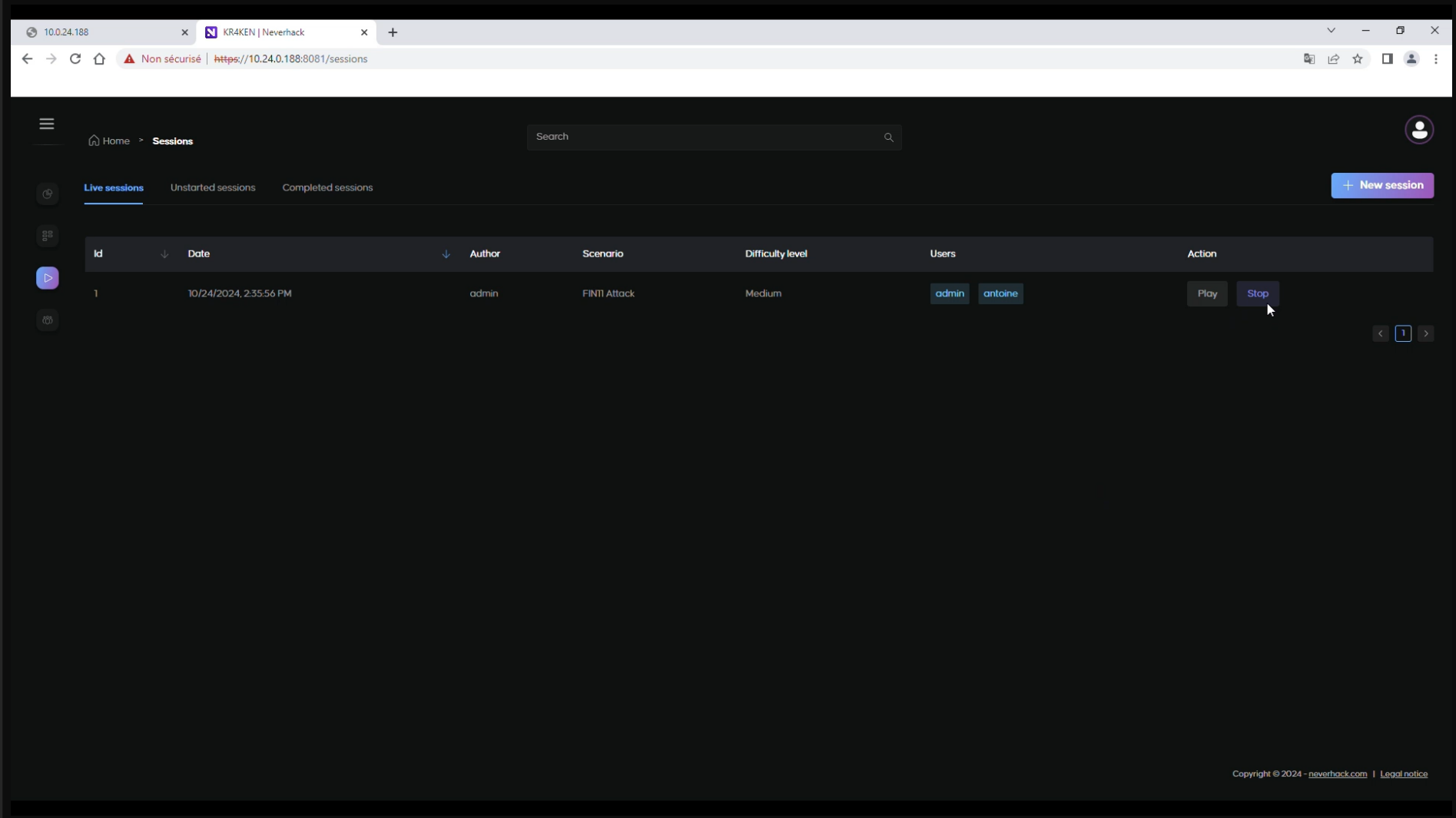
The interface

The killchain

Life trafic

Attack session

End session



When the analyst considers that he has covered as many attacks as possible with his cases, he stops the session.

Meet KRAKEN

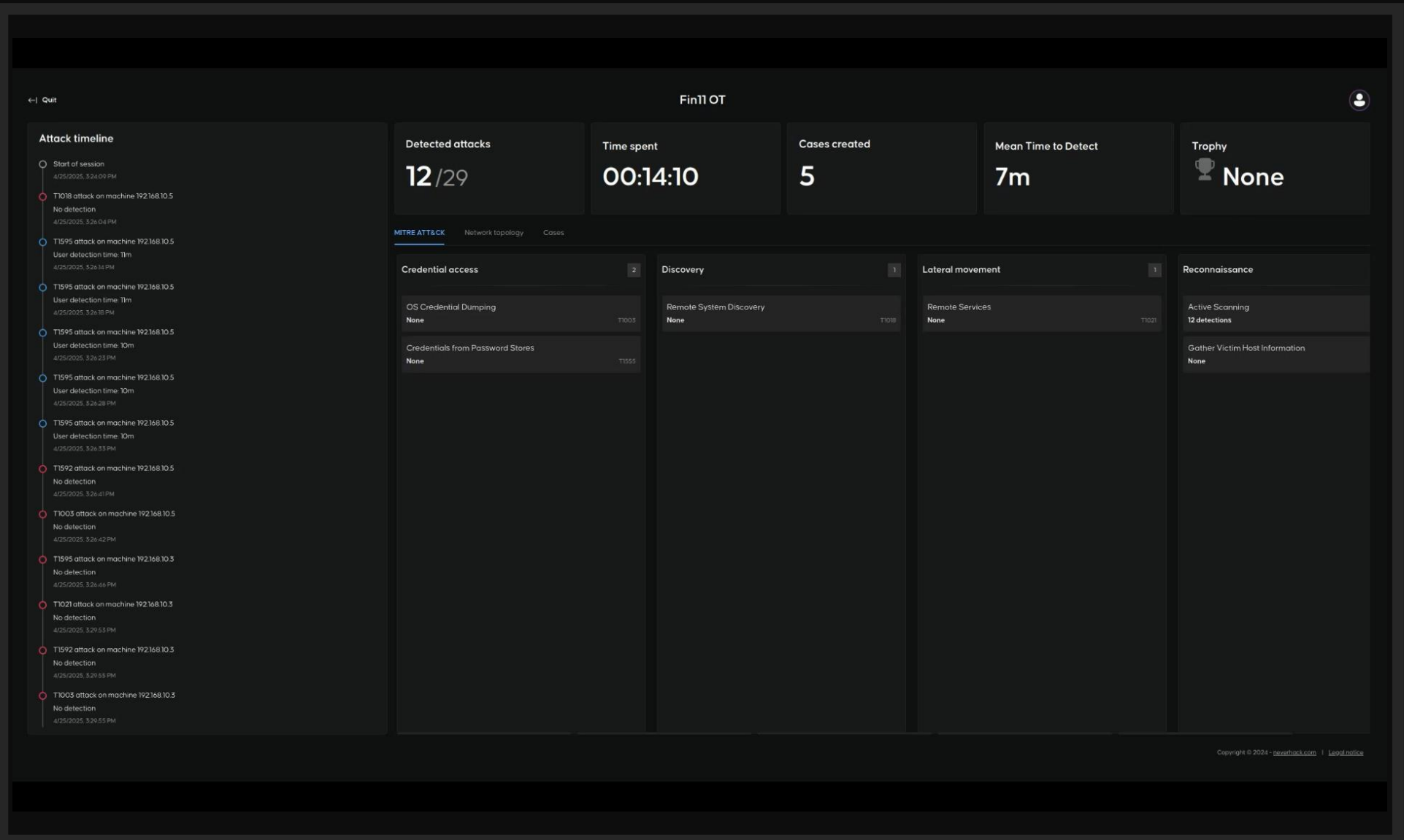
The interface

The killchain

Life trafic

Attack session

End session



The summary gives access to the entire attack timeline, the detection rate and the created cases (classified with MITRE ATT&CK). The analyst can observe step-by-step the attacks that went through, both to improve himself and its tools.

Meet KRAKEN

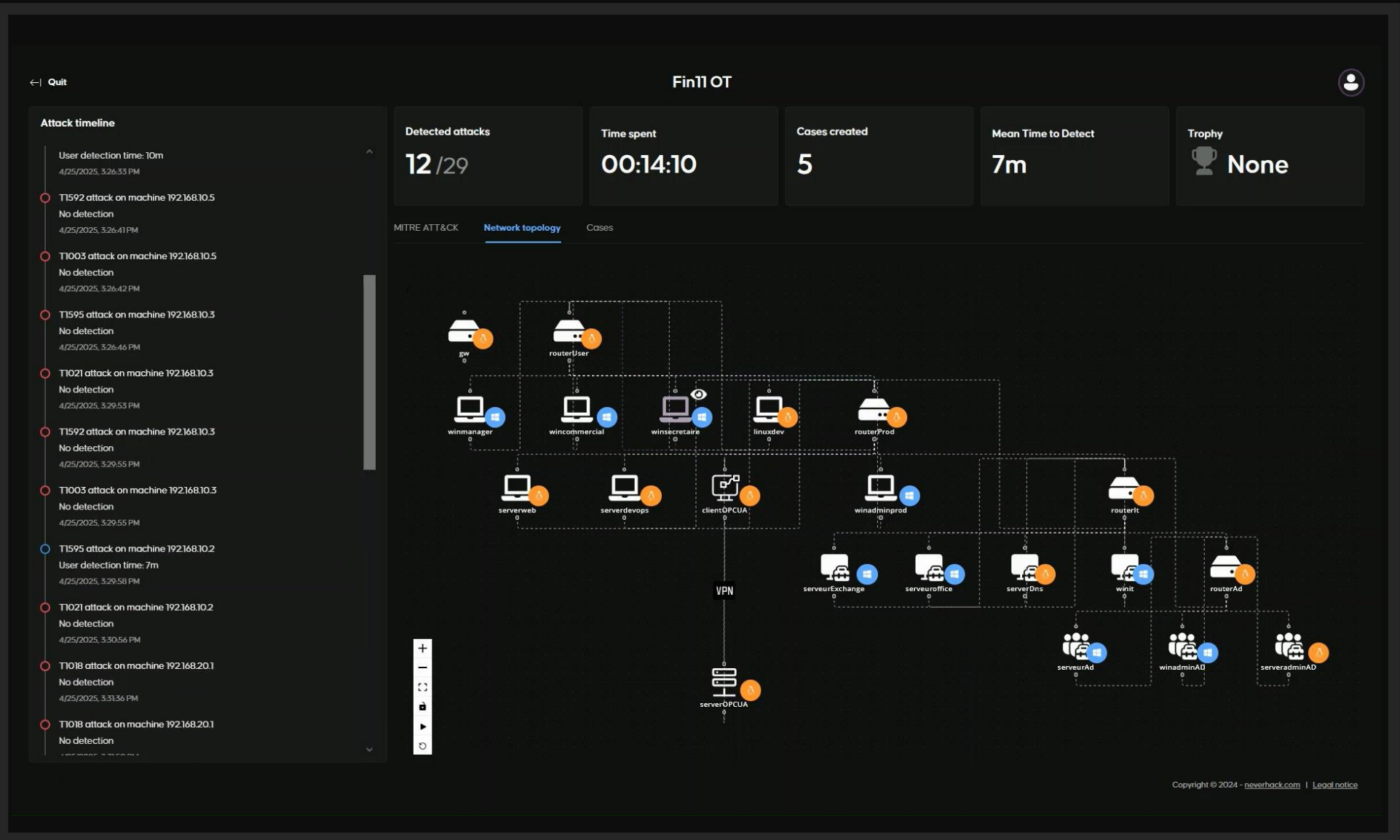
The interface

The killchain

Life trafic

Attack session

End session



A graphic animation over the topology is also available to better display the compromised paths and machines.

Meet KRAKEN

The interface

The killchain

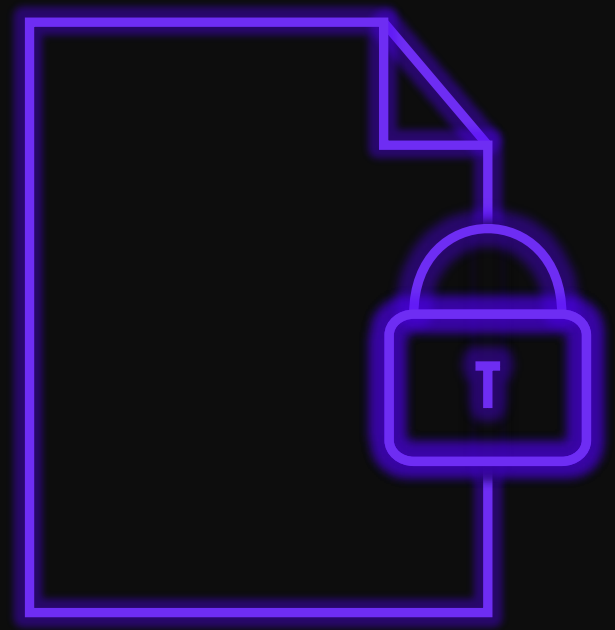
Life trafic

Attack session

End session

The dashboard provides Key Performance Indicators for all sessions, enabling managers to make informed decisions.

Kraken can be integrated into any SIEM.



And constantly offers up-to-date killchains to provide analysts with a high-quality context in which they can test their posture on an ongoing basis.

Kraken can be configured entirely. The scenarios, target topologies and difficulties can meet the exact needs of each SOC.


NEVERHACK