



Kraken

SOC assessment



Meet KRAKEN

NEVERHACK



Meet KRAKEN

Cyber criminals
Activists
APT
Ransomware
Exfiltration
Denial of Service



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?

Fight alert fatigue



Get a continuous flow of
rules and tools assessment



Check your operational
safety posture



Avoid buying tools without testing
them first

Test yourself against APT-like attacks



Monitor on the long run
your detection coverage
and efficiency



Identify weak points in your detection
and reaction processes





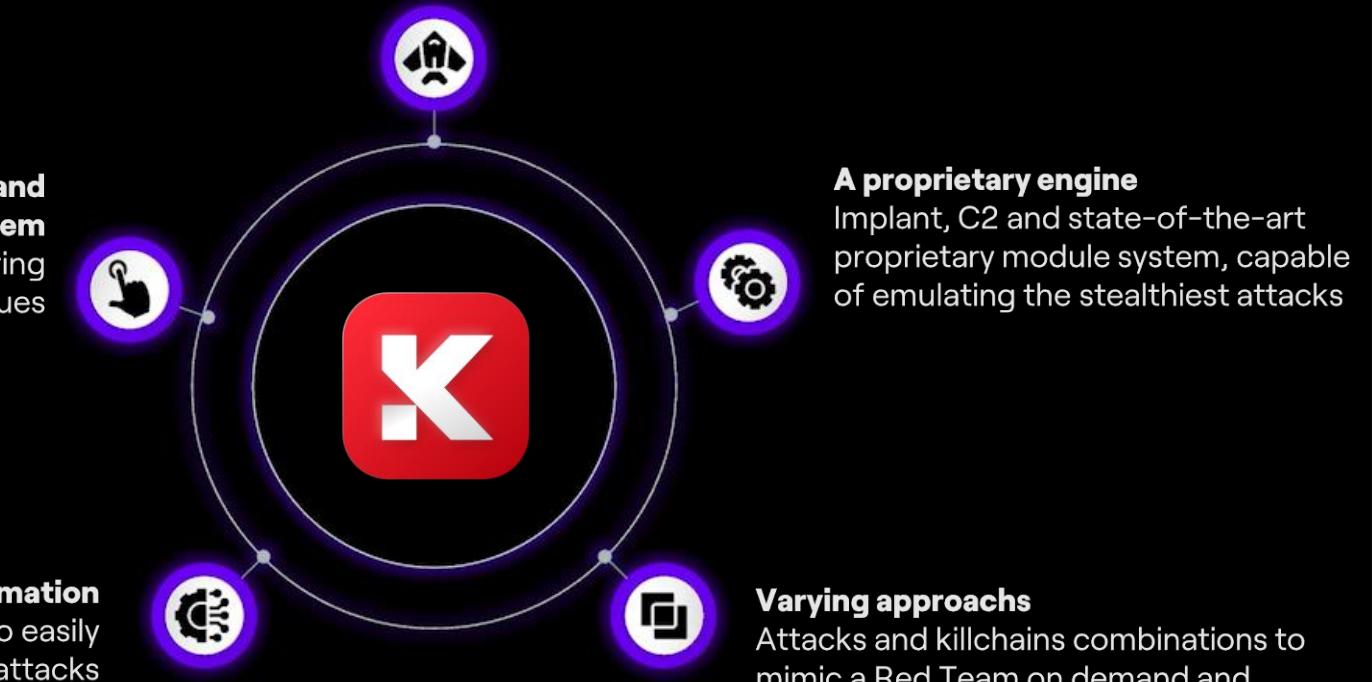
Meet KRAKEN

For more than a simple command executions system

KRAKEN sets itself apart by covering all MITRE ATT&CK techniques

Complete automation

Modular system designed to easily integrate new attacks



KRAKEN: An automatic attack engine

Sophisticated stealthy attacks

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

A proprietary engine

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

Varying approaches

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



Meet KRAKEN

KRAKEN: Advanced capabilities

Deterministic or procedural scenario system



Advanced escape capabilities



Passive and active scans, application exploitation, lateralization, privilege escalation, process injection, etc



A library of advanced, customizable attacks





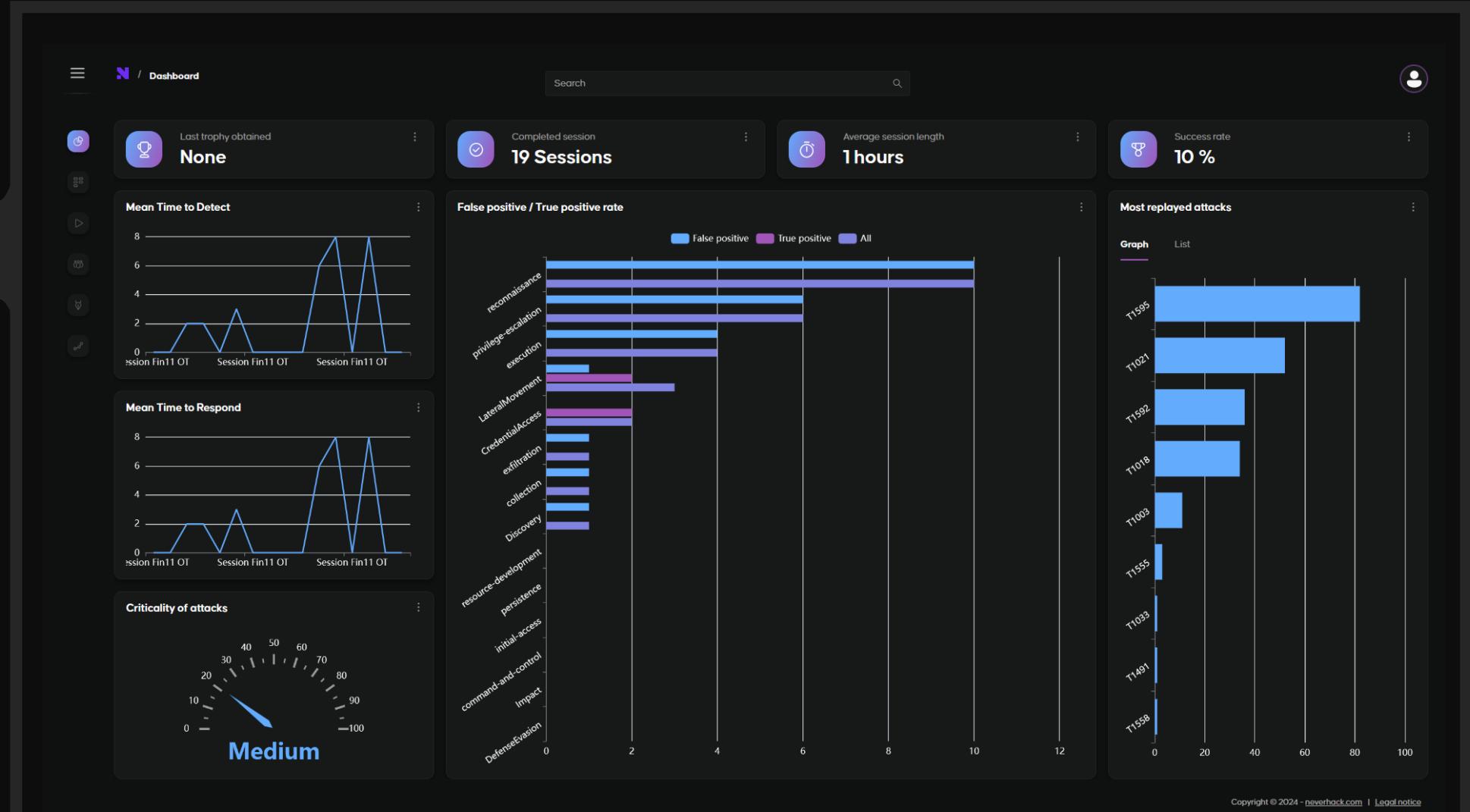
Meet KRAKEN



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.



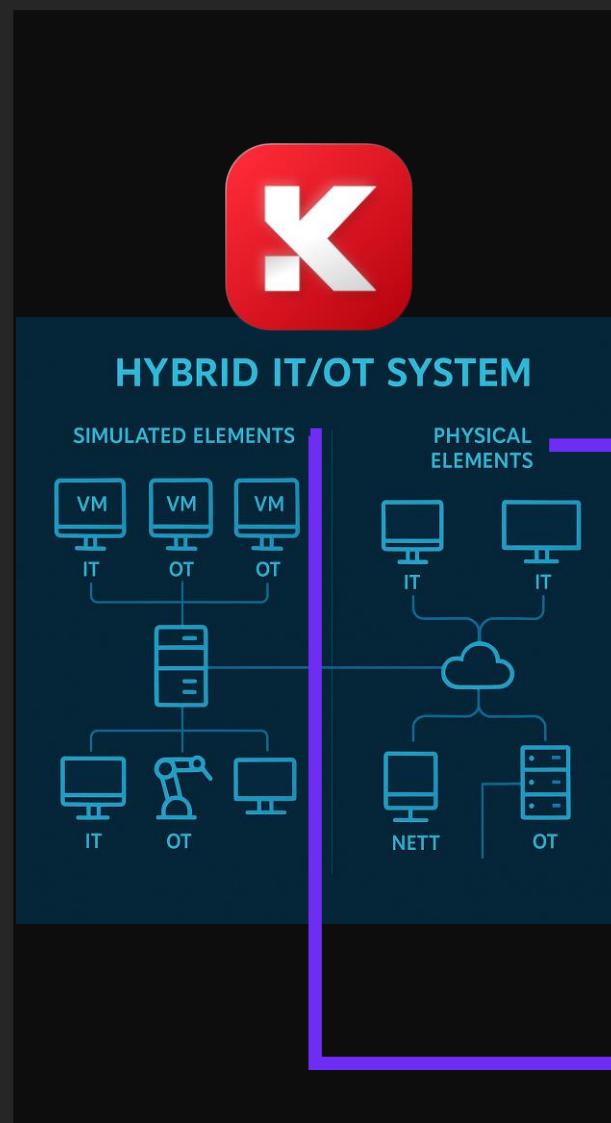
Meet KRAKEN



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



SIEM
EDR, NDR, analysts, etc

...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

NEVERHACK

Welcome

Please log in before accessing your dashboard

admin@neverhack.com

Forgot your password ?

Login

Powered by KRAKEN



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



Meet KRAKEN

The interface

A screenshot of the KRAKEN manager interface. The top navigation bar includes a home icon, 'Home' (selected), and 'Dashboard'. A search bar with a magnifying glass icon is positioned above a grid of four large, dark rectangular cards. On the far left, a vertical sidebar features a menu icon and four circular icons with symbols: a person, a gear, a right-pointing arrow, and a left-pointing arrow. In the top right corner, there is a user profile icon. The bottom right corner of the screenshot contains the text 'Copyright © 2024 - neverhack.com | Legal notice'.

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



Meet KRAKEN

The interface

The screenshot shows the KRAKEN session management interface. At the top, there's a navigation bar with a home icon, the text "Home > Sessions", a search bar with a magnifying glass icon, and a user profile icon. Below the navigation is a toolbar with icons for "Live sessions" (highlighted), "Unstarted sessions", and "Completed sessions". A large button labeled "+ New session" is on the right. The main area is a table with columns: Id, Date, Author, Scenario, Difficulty level, Users, and Action. The "Id" column has a sorting arrow. The "Users" column has a sorting arrow. The "Action" column has a sorting arrow. The table currently displays the message "No data". At the bottom right, there are navigation arrows and a page number indicator "1".

The manager creates the session.



Meet KRAKEN

The interface

The screenshot shows the KRAKEN web application's session management interface. At the top, there is a navigation bar with a home icon, the word "Sessions", a search bar, and a user profile icon. Below the navigation is a header with tabs: "Live sessions" (which is active), "Unstarted sessions", and "Completed sessions". To the right of the tabs is a blue button labeled "+ New session" with a cursor hovering over it. The main area features a table with columns: Id, Date, Author, Scenario, Difficulty level, Users, and Action. The table currently displays the message "No data". At the bottom right of the interface, there are navigation icons for back, forward, and search.

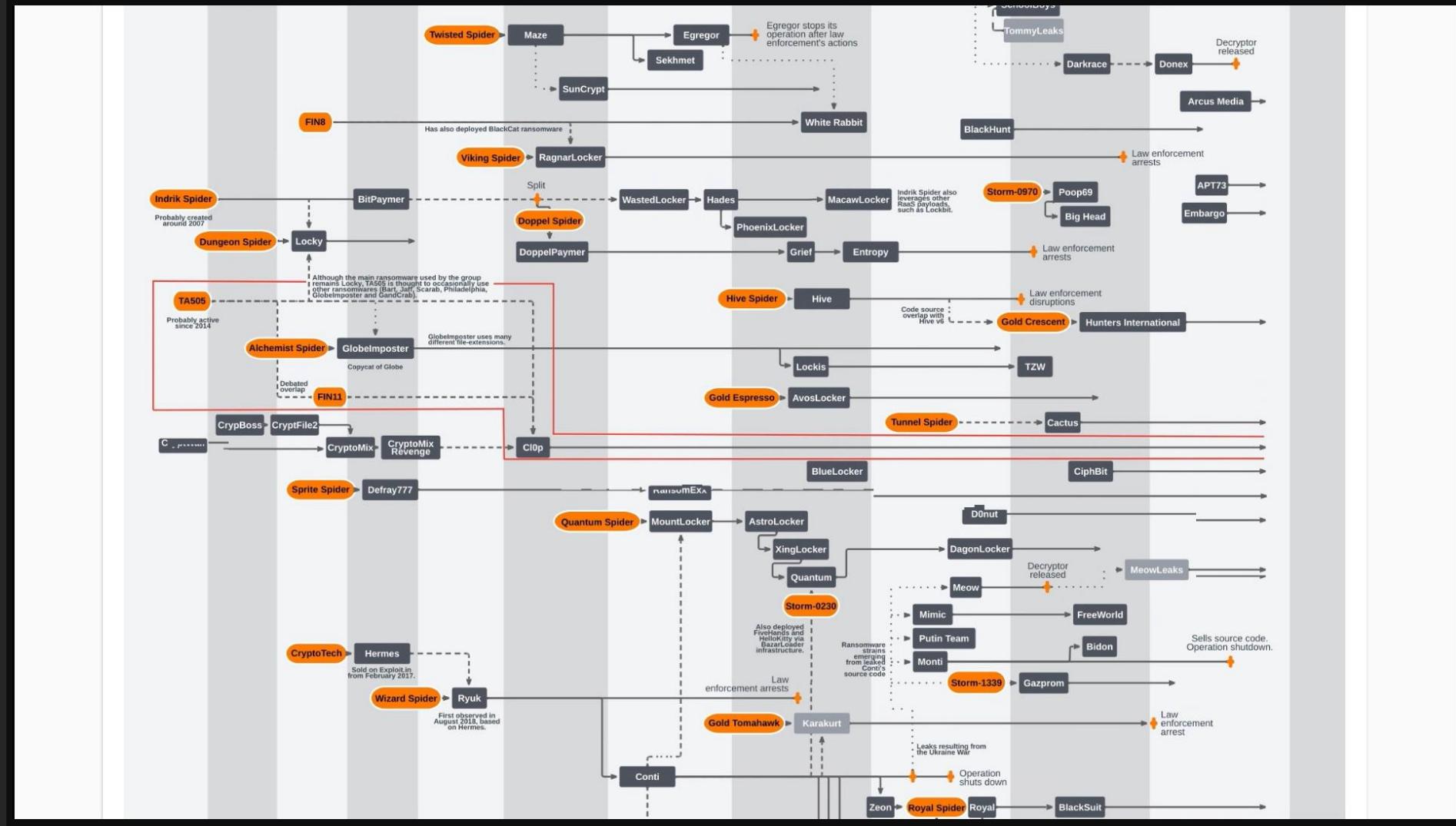
And chooses the attack scenario.



Meet KRAKEN

The interface

The killchain



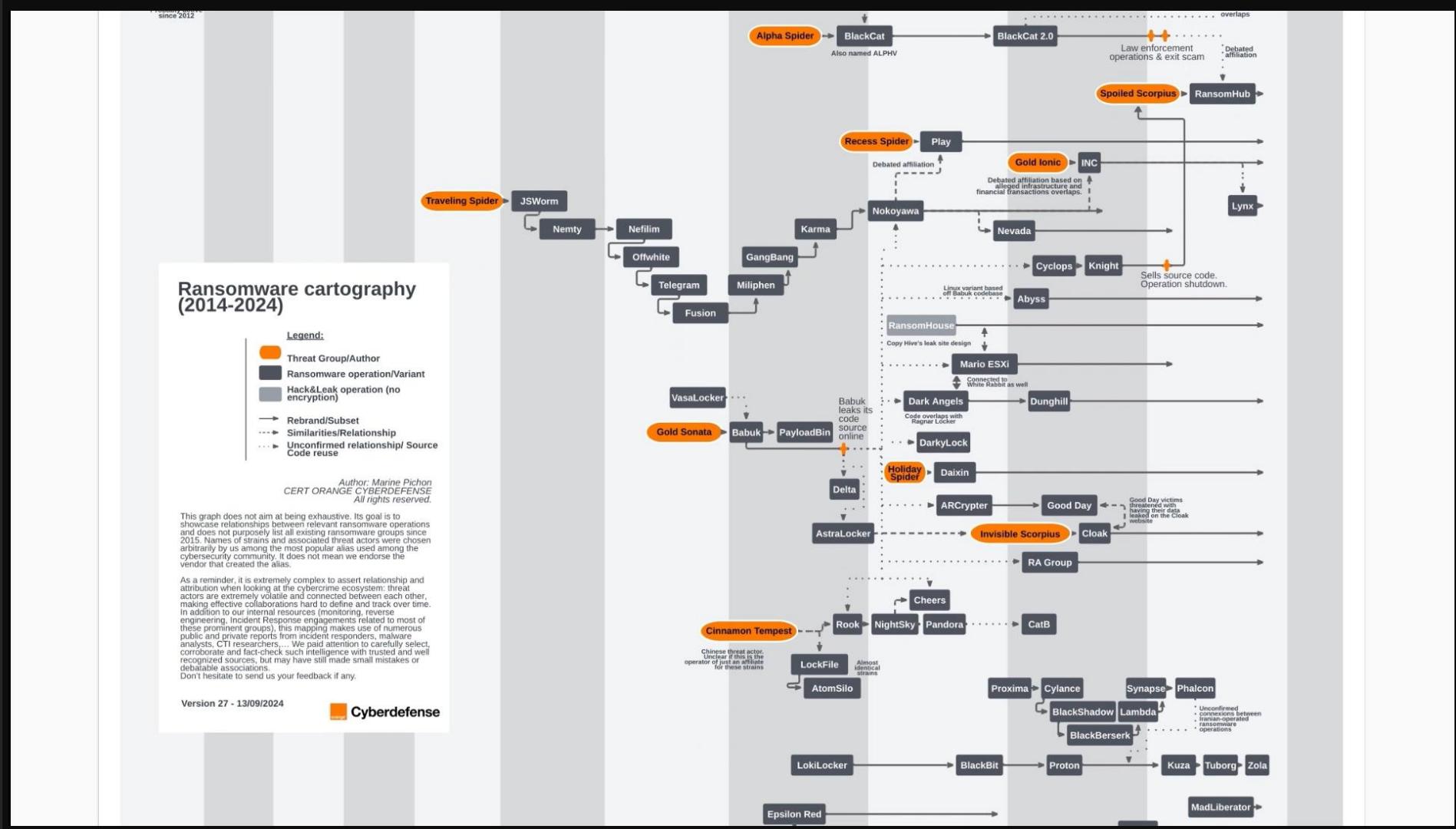
As an example, we chose a real 2023 attack killchain from the well-known threat-actor FIN11.



Meet KRAKEN

The interface

The killchain



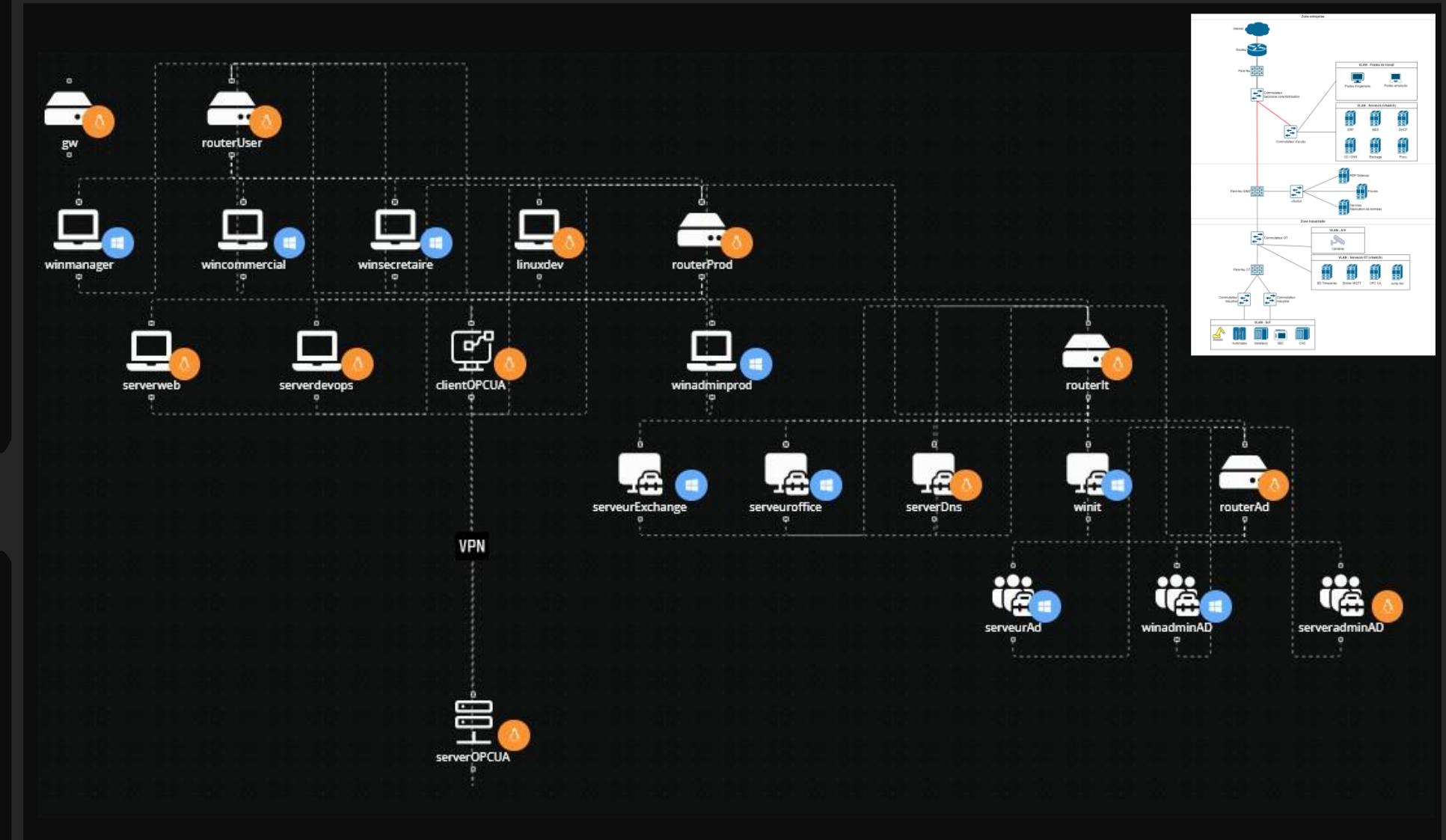
But the manager could choose to emulate any major threat actor based on its latest campaigns: one adapted to the infrastructure, sector of activity, objective and stealth desired.



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 traffic

The screenshot shows the KRAKEN software interface. At the top, there's a menu bar with File, View, Server, Document, Settings, and Help. Below the menu is a toolbar with various icons. The main window has a Project tree on the left containing a Project node, which has Servers, Documents, and Data Access View children. Under Servers, there's a connection to 'toto@10.10.10.2'. The central area is titled 'Data Access View' and displays the message 'CurrentTime: 2025-04-22 07:28:44.452033'. On the right, there are two panes: 'Attributes' and 'References'. The 'Attributes' pane lists properties for a selected node, including NodeId (i=11492), NamespaceIndex (0), IdentifierType (Numeric), Identifier (11492), NodeClass (Method), BrowseName (0, "GetMonitor"), DisplayName ("", "GetMonitor"), Description (BadAttributel), and Executable (true). The 'References' pane shows HasProperty entries for InputArguments and OutputArguments. At the bottom, the 'Log' panel displays a table of log entries:

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).

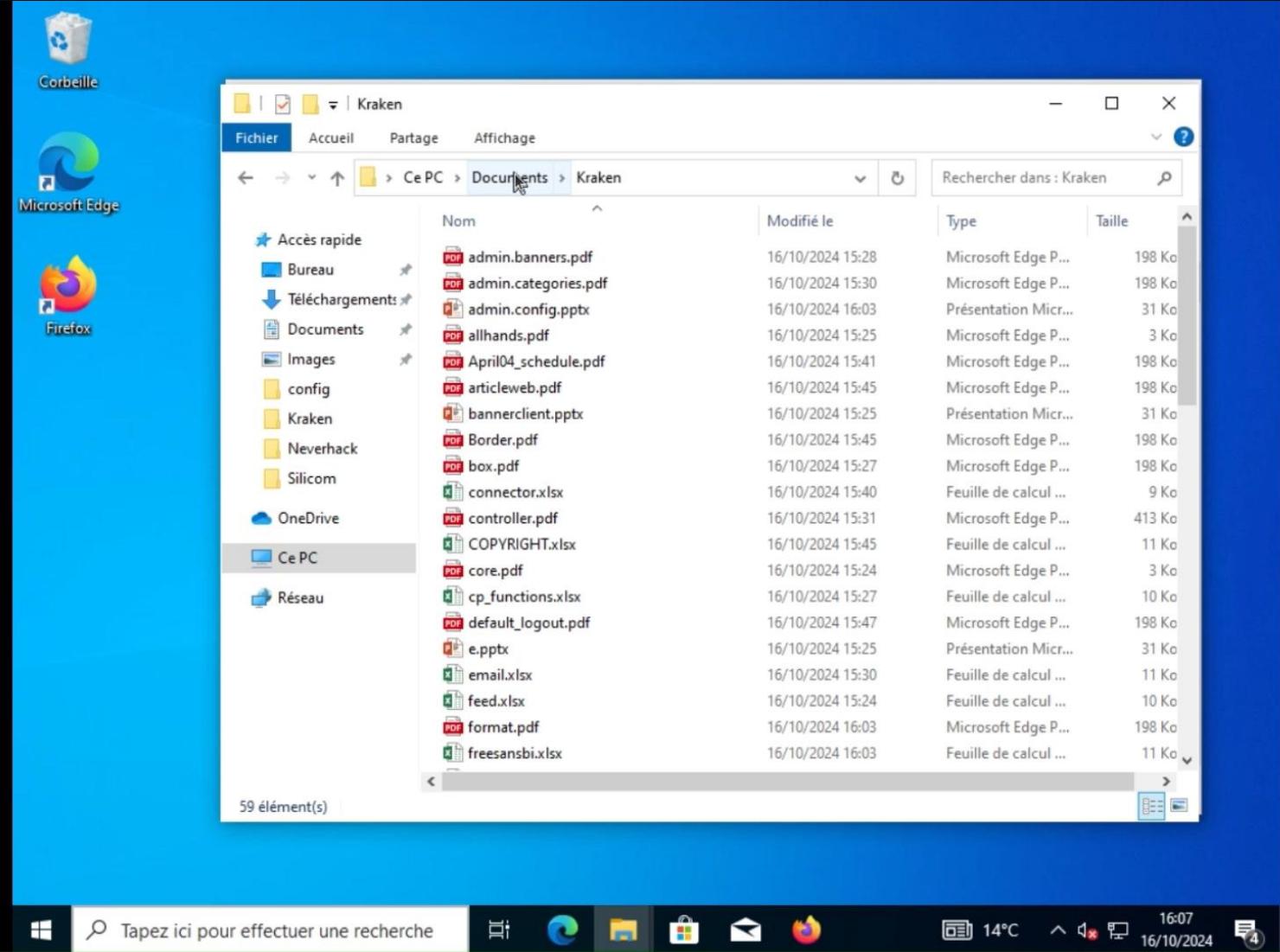


Meet KRAKEN

The interface

The killchain

Life traffic



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 traffic

Attack session

The screenshot shows the Kraken interface for creating a session. The top navigation bar includes a back arrow, a search bar with placeholder 'Search', and a user profile icon. Below the header, a progress bar indicates four steps: 1. Scenario (selected), 2. Network topology, 3. Difficulty level, and 4. Members. The 'Scenario' step is titled 'Choose the scenario to play on this session' and features a dropdown menu with options: 'Please select', 'APT29' (which is selected and highlighted in blue), 'FIN11', 'Fin11 OT', and 'TA2101'. On the left side, there's a vertical sidebar with several small circular icons representing different tools or modules.

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 traffic

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': 'Ethernet 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)], credentials={}, 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
ERROROR kuhl_m_privilege_simple ; RtlAdjustPrivilege (20) c0000061

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

mimikatz(commandline) # exit
Bye!

hostname silicon

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 traffic

Attack session

The screenshot displays the Stellar SIEM interface with the following sections:

- Threat Hunting:** Shows 1 - 3 of 3 Results. One entry is visible: "2024-10-15 20:16:04 incident_score_change StellarCyl".
- Traffic Records (Fri Sep 23 2022 15:45:16):** Shows 0 results found. Filter: appid. Items per page: 50.
- Syslog Records (Fri Sep 23 2022 15:45:16):** Shows 1 - 3 of 3 Results. One entry is visible: "2024-10-15 18:11:57 incident_score_change StellarCyl". Filter: msc. Items per page: 50.
- Windows Records (Fri Sep 23 2022 15:45:16):** Shows 1 - 50 of 134517 Results. One entry is visible: "2024-10-16 15:03:15 Microsoft.Windows-Dhcp-Cli 50.09%". Filter: channel, event id. Items per page: 50.

On the right side, there is a detailed table of detected attack properties:

Field Name	Key Name	Value
Channel	ing_name	Microsoft...
Computer Name	computer_name	DESKTOP...
Dspc Name	dspc_name	Best Effort
Engid	engid	ad03bc2...
Engid Device Class	engid_device_class	Windows
Engid Device Desc	engid_device_desc	windows...
Engid Gateway	engid_gateway	77.198.2...
Engid Name	engid_name	DESKTOP...
Event Data InterfaceId	event_data_interfaceId	5
Event Data InterfaceUUID	event_data_interfaceUUID	0x60080...
Event Id	event_id	50092
Host Ip	host_ip	10.24.0.52
Hostip	hostip	10.24.0.52
Hostip Geo City	hostip_geo_city	Paris
Hostip Geo CountryCode	hostip_geo_countryCode	FR
Hostip Geo CountryName	hostip_geo_countryName	France
Hostip Geo Latitude	hostip_geo_latitude	48.8323
Hostip Geo Longitude	hostip_geo_longitude	2.4075

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 traffic

Attack session

L init: proxychains-ng 4.16\n[proxychains] DLL init: proxychains-ng 4.16\n[proxychains] Strict chain ... 172.17.0.1:9050 ... 192.168.10.2:22 ... OK\nWarning: Permanently added '192.168.10.2' (ED25519) to the list of known hosts.\n[*] Payload uploaded to target!\n[*] Setting executable permissions...\n[*] Command executed successfully on attempt 1\n[*] Permissions set!\n[*] Executing the payload...\n[*] SSH command execution failed\n[*] SSH connection lost. Reconnecting... (Attempt 1)\n[*] SSH reconnection succeed in 1 attempts\n[*] Command executed successfully on attempt 1\n[*]

File View Server Document Settings Help

Project Data Access View

Address Space

No Highlight

Server

Auditing

Dictionaries

EstimatedReturnTime

GetMonitoredItems

LocalTime

NamespaceArray

Namespaces

PublishSubscribe

CurrentTime: 2025-04-22 07:28:50.487899

Attributes

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

References

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 07:25:49.038	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.

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 traffic

Attack session

The screenshot shows the Kraken interface for the 'Fin11 OT' scenario. At the top, there's a navigation bar with tabs for Scenario, VNC, Network topology, Chat, and Cases (0). The main area displays scenario details: Name (Fin11 OT), Network topology (Kill2OT), Furtivity and Sophistication level (2), Number of machine (21), and Number of user (1). Below this is a 'Description' section with a detailed paragraph about the Fin11 group. Under 'Users', there's a table with one entry: Name (admin), E-mail (admin@neverhack.com), and Username (admin). On the right, a large list of 'Suspected techniques' is shown, each with a count of 0. The techniques include collection, command-and-control, credential-access, defense-evasion, discovery, execution, exfiltration, impact, initial-access, lateral-movement, persistence, privilege-escalation, reconnaissance, resource-development, collection, command-and-control, credential-access, and defense-evasion.

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 traffic

Attack session

End session

The screenshot shows a web browser window titled "KRAKEN | Neverhack" with the URL "https://10.24.0.188:8081/sessions". The page has a dark theme and displays a table of sessions. The columns are: Id, Date, Author, Scenario, Difficulty level, Users, and Action. There is one row visible with the following data:

Id	Date	Author	Scenario	Difficulty level	Users	Action
1	10/24/2024, 2:35:56 PM	admin	FINTI Attack	Medium	admin antoine	Play Stop

At the bottom right of the interface, there is a small footer with the text "Copyright © 2024 - neverhack.com | Legal notice".

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 traffic

Attack session

End session

The screenshot displays the KRAKEN interface with the following sections:

- Attack timeline:** A detailed log of 15 attacks on machine 192.168.10.5, categorized by T1018, T1595, T1592, T1003, and T1021. Each entry includes a timestamp and detection status.
- Detected attacks:** Summary: 12/29
- Time spent:** 00:14:10
- Cases created:** 5
- Mean Time to Detect:** 7m
- Trophy:** None
- MITRE ATT&CK:** Categorizes attacks into Credential access, Discovery, Lateral movement, and Reconnaissance.
- Network topology:** Shows the network structure.
- Cases:** Shows the status of 5 cases.

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 traffic

Attack session

End session

Fin11 OT

Attack timeline

- User detection time: 10m
4/25/2025, 3:26:33 PM
- T1592 attack on machine 192.168.10.5
No detection
4/25/2025, 3:26:41 PM
- T1003 attack on machine 192.168.10.5
No detection
4/25/2025, 3:26:42 PM
- T1595 attack on machine 192.168.10.3
No detection
4/25/2025, 3:26:46 PM
- T1021 attack on machine 192.168.10.3
No detection
4/25/2025, 3:29:53 PM
- T1592 attack on machine 192.168.10.3
No detection
4/25/2025, 3:29:55 PM
- T1003 attack on machine 192.168.10.3
No detection
4/25/2025, 3:29:55 PM
- T1595 attack on machine 192.168.10.2
User detection time: 7m
4/25/2025, 3:29:58 PM
- T1021 attack on machine 192.168.10.2
No detection
4/25/2025, 3:30:56 PM
- T1018 attack on machine 192.168.20.1
No detection
4/25/2025, 3:51:56 PM
- T1018 attack on machine 192.168.20.1
No detection

Detected attacks: 12 / 29 | Time spent: 00:14:10 | Cases created: 5 | Mean Time to Detect: 7m | Trophy: None

MITRE ATT&CK | Network topology | Cases

gw, routerUser, winmanager, wincommercial, winskretaire, linuxdev, routerProd, serverweb, serverdevops, clientOPCUA, winadminprod, serverExchange, serveurOffice, serverDns, routerIT, routerAd, serverAD, winsadminAD, serveradminAD

VPN

Copyright © 2024 - neverhack.com | Legal notice

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



Meet KRAKEN

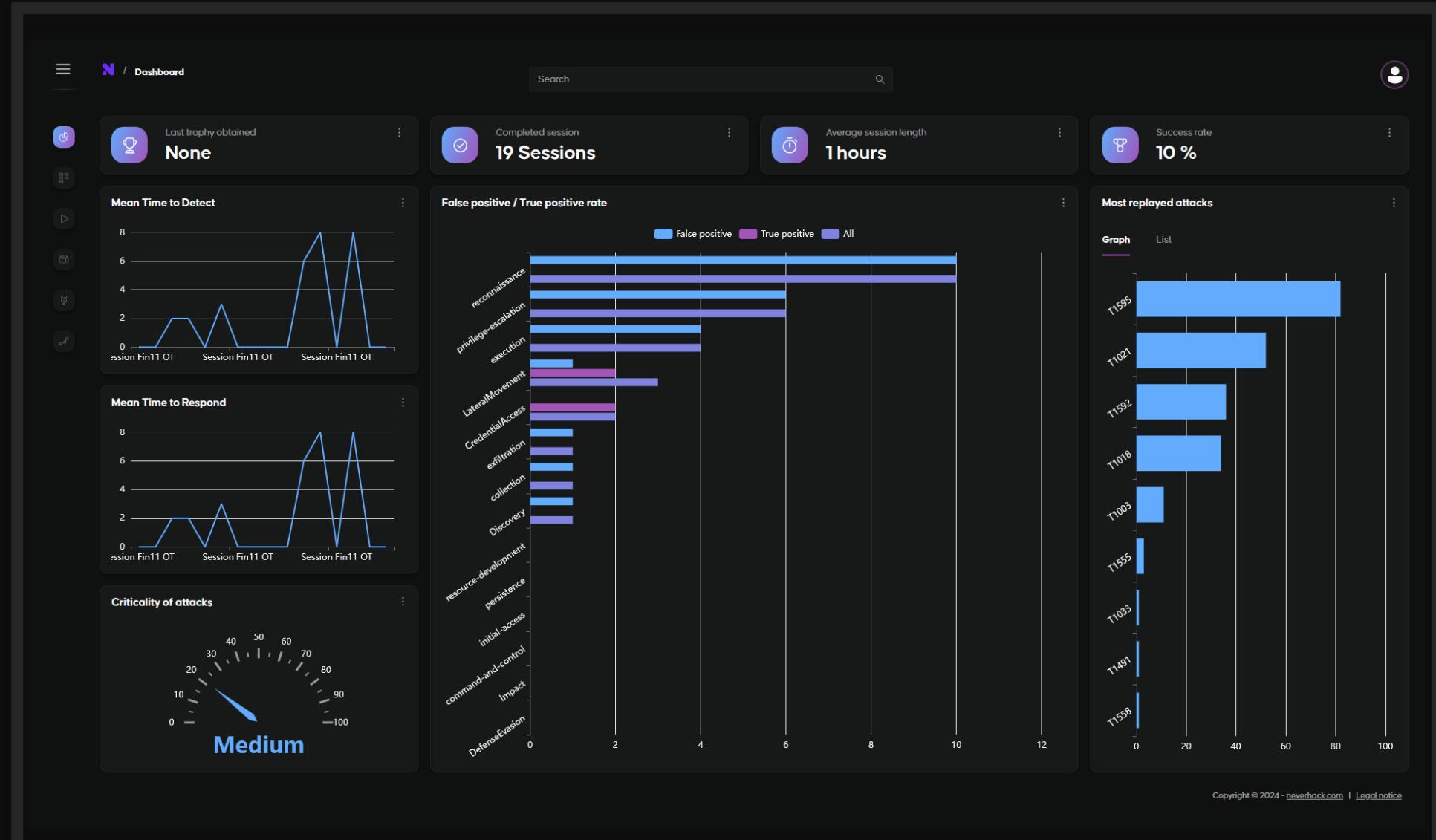
The interface

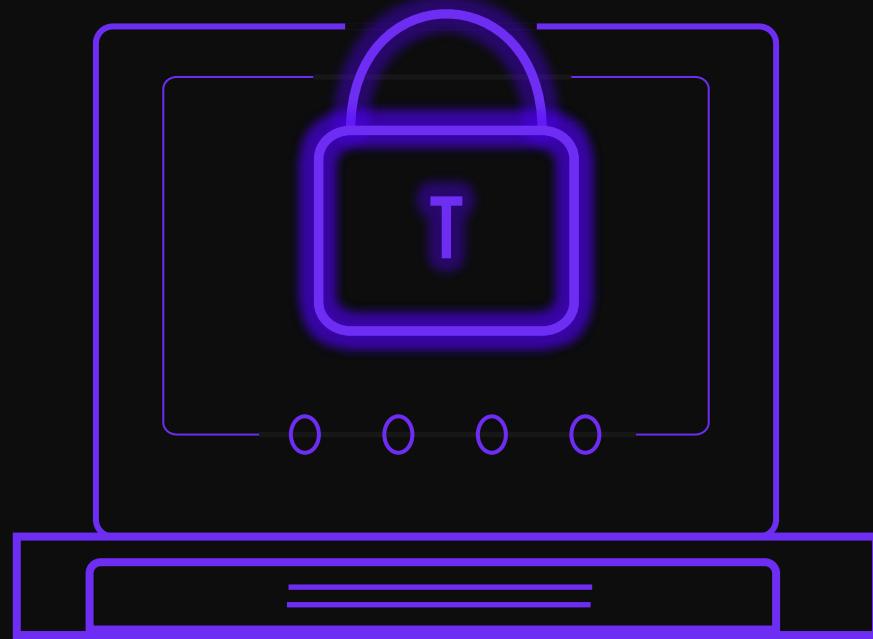
The killchain

Life traffic

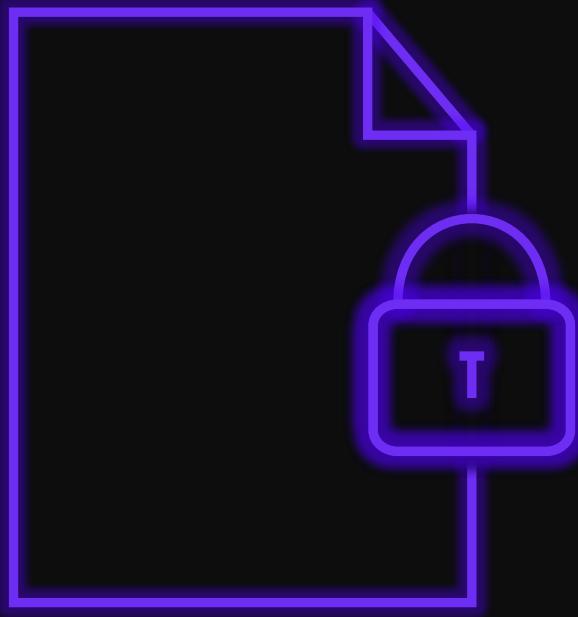
Attack session

End session





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.



The logo features the word "NEVERHACK" in a bold, white, sans-serif font. The letter "N" is unique, composed of two overlapping purple rectangles: a larger one at the top and a smaller one at the bottom, creating a layered effect.

NEVERHACK