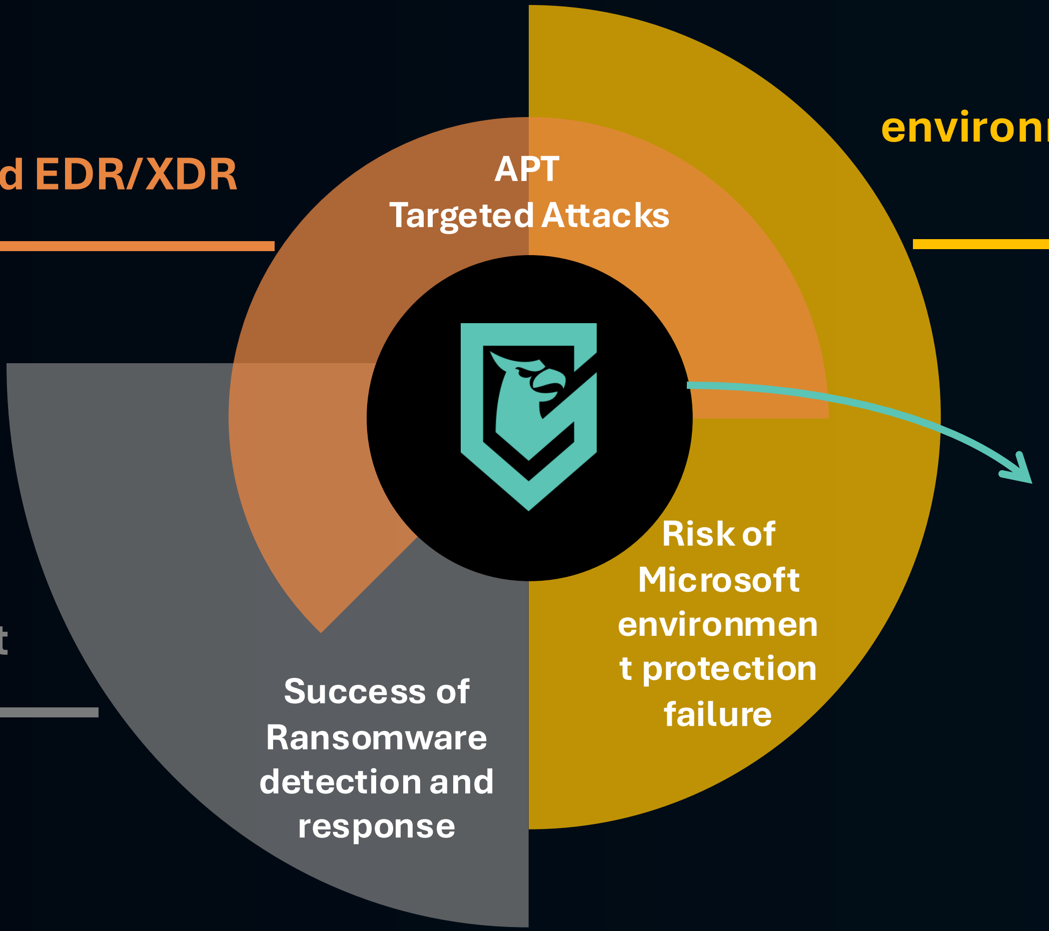
IstroSec

TRUE PASSION
REAL CYBERSECURITY

APTs using targeted TTPs to avoid EDR/XDR technologies

Targeted attacks on Microsoft environments often lead to EDR/EPP/XDR protection malfunctioning


APT
Targeted Attacks
Risk of Microsoft environment protection failure
Success of Ransomware detection and response

Drops from 22% to 13% in recent years

Extension to EDR/EPP/XDR as a next layer of Ransomware and Targeted Attacks protection

By Incident Responders for Incident Responders

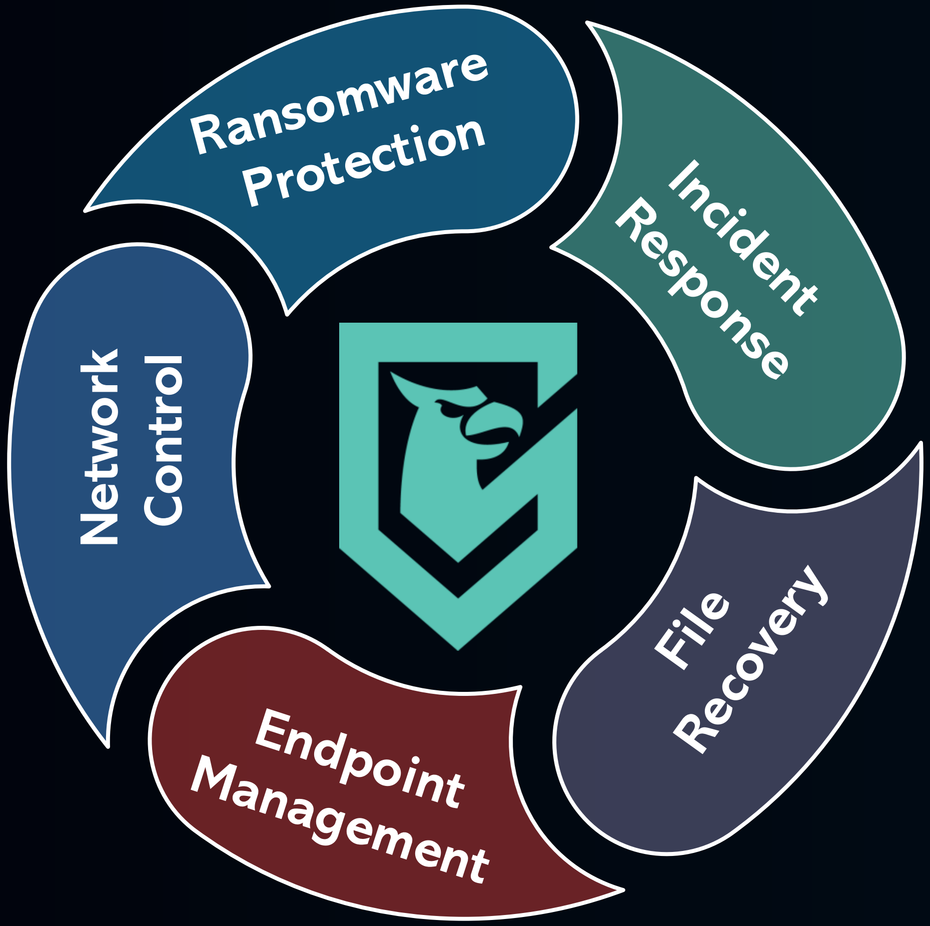
IstroSec

ISTROSEC GRYPHON

The ultimate ransomware protection toolkit

IstroSec Gryphon

Ransomware Protection Toolkit



Built-in Intelligence

- AI-behavioral based detection in real-time
- Complete device protection
- Block malicious code injection within processes

User Experience

- Driver integrated directly into the operating system
- Automatic blocking of ransomware on system level
- Central management console to respond threats from anywhere

Online and Offline Protection

- Designed to offer protection even in offline mode
- An agent-based extension to EDR/XDR/EPP tools for multi-layered security
- Integration with Windows standard protection systems

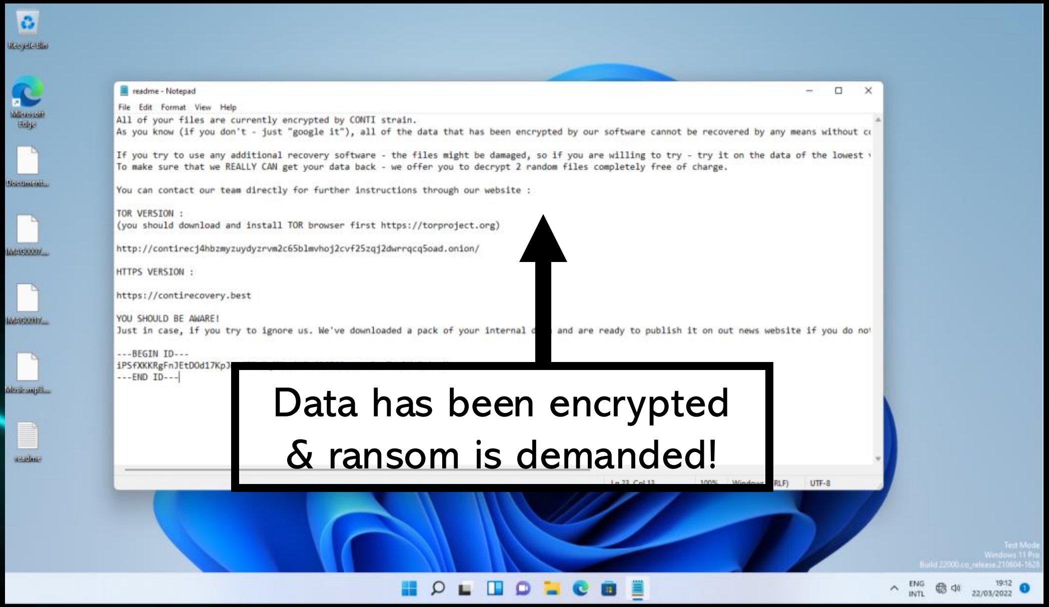
GRYPHON MDR platform – ransomware protection

The key focus is on behavioral analysis of standard system and application behavior to detect ransomware and immediately block it. Currently the behavior is measured by 13 different behavior markers to identify ransomware behavior on the system. This version has a 99% success rate…!

Current functionality:

- Behavioral detection of ransomware and protection against ransomware (24/7 tested against current ransomware strains)
- Own driver for detection and response capabilities
- Automatic blocking of ransomware on system level
- Detection and blocking of malicious usage of LOLBINS in the system
- Realtime behavioral rules

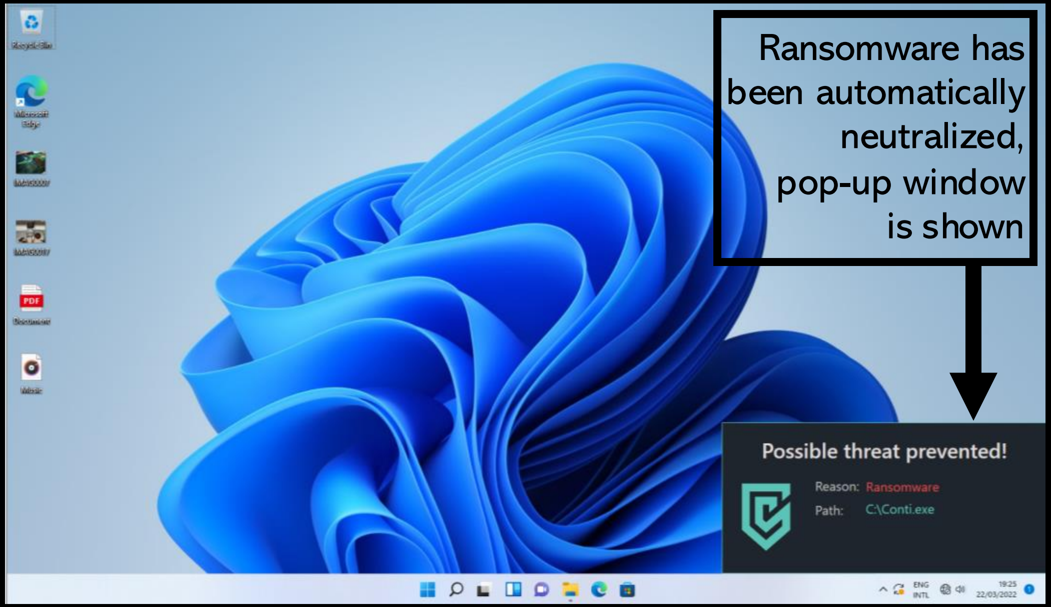
↓ CONTI Ransomware on Win 11 with basic protection (standard NGAV/EDR) ↓



```
All of your files are currently encrypted by CONTI strain.
As you know (if you don't - just "google it"), all of the data that has been encrypted by our software cannot be recovered by any means without cc

If you try to use any additional recovery software - the files might be damaged, so if you are willing to try - try it on the data of the lowest v
To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files completely free of charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://contirecj4hbzmyzuydyzrvm2c65blmvhoj2cvf25zqj2dwrrqcq5oad.onion/

HTTPS VERSION :

https://contirecovery.best

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded a pack of your internal d   and are ready to publish it on out news website if you do not

---BEGIN ID---
iPSfXKKRgFnJEtDOd17KpJ
---END ID---
```

Data has been encrypted & ransom is demanded!

↓ CONTI Ransomware on Win 11 with GRYPHON ↓


Ransomware has been automatically neutralized, pop-up window is shown

Possible threat prevented!

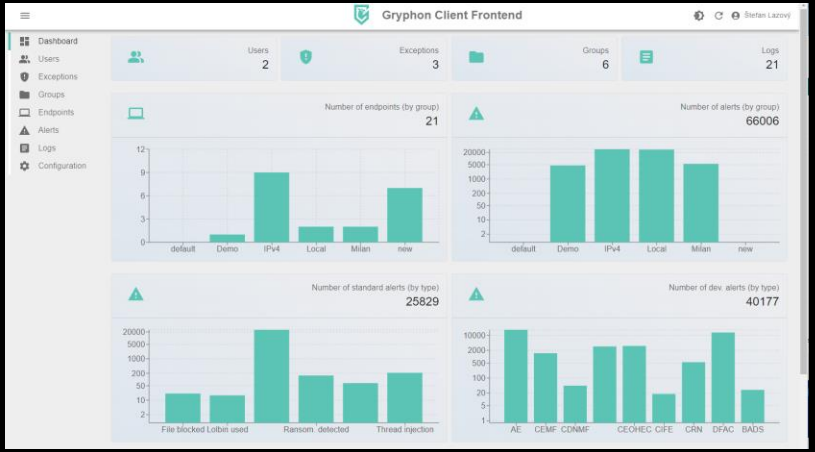
Reason: Ransomware

Path: C:\Conti.exe

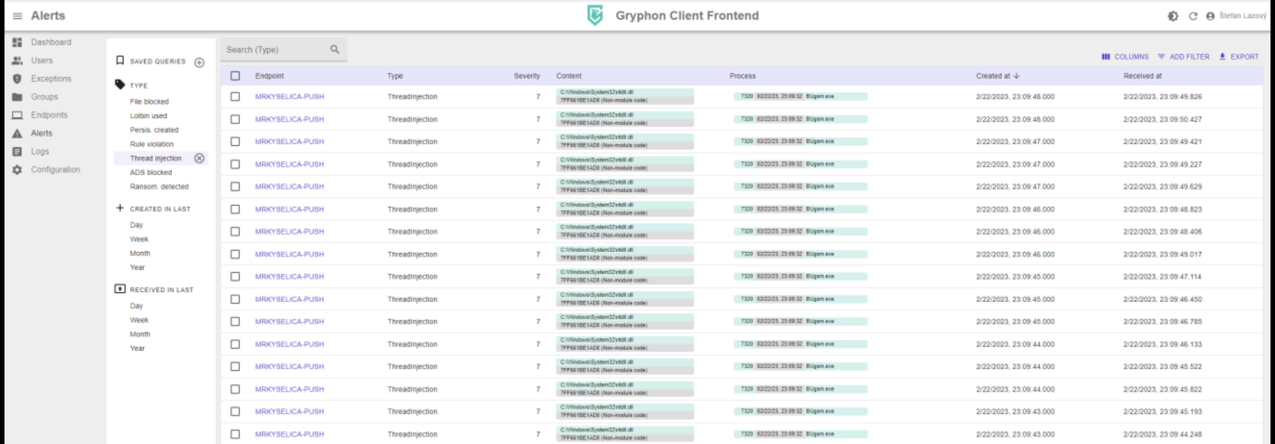
GRYPHON Admin UI

IstroSec

Admin view (Dashboard) ↓

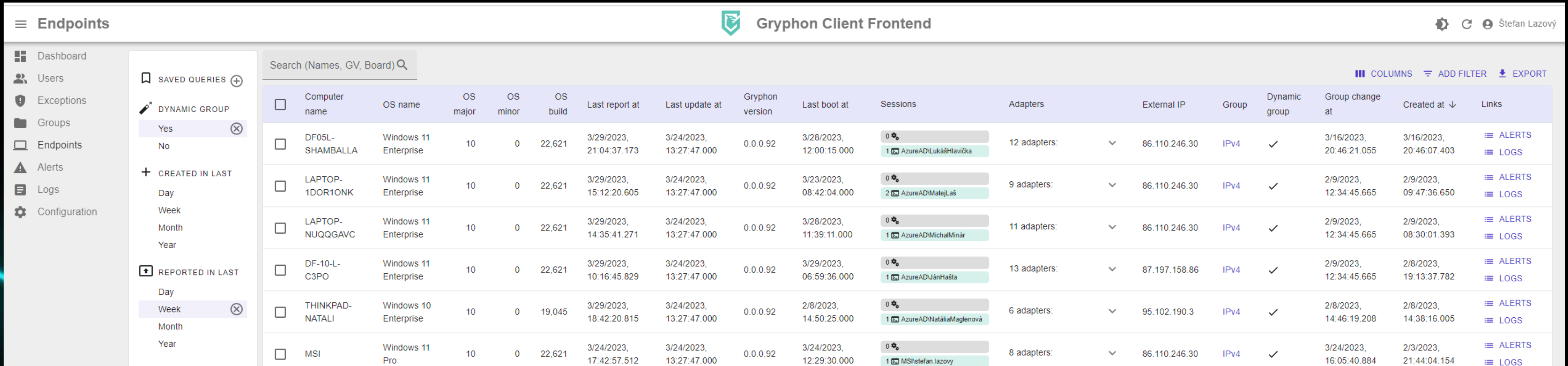


Admin view (Console / Alerts view) ↓



☐	Endpoint	Type	Severity	Content	Process	Created at ↓	Received at
☐	MRKYSELICA-PUSH	ThreadInjection	7	C:\Windows\System32\ntdll.dll 7FF661BE1AD0 (Non-module code)	7320 02/22/23, 23:09:32 BUgsm.exe	2/22/2023, 23:09:48.000	2/22/2023, 23:09:49.826
☐	MRKYSELICA-PUSH	ThreadInjection	7	C:\Windows\System32\ntdll.dll 7FF661BE1AD0 (Non-module code)	7320 02/22/23, 23:09:32 BUgsm.exe	2/22/2023, 23:09:48.000	2/22/2023, 23:09:50.427
☐	MRKYSELICA-PUSH	ThreadInjection	7	C:\Windows\System32\ntdll.dll 7FF661BE1AD0 (Non-module code)	7320 02/22/23, 23:09:32 BUgsm.exe	2/22/2023, 23:09:47.000	2/22/2023, 23:09:49.421
☐	MRKYSELICA-PUSH	ThreadInjection	7	C:\Windows\System32\ntdll.dll 7FF661BE1AD0 (Non-module code)	7320 02/22/23, 23:09:32 BUgsm.exe	2/22/2023, 23:09:47.000	2/22/2023, 23:09:49.227
☐	MRKYSELICA-PUSH	ThreadInjection	7	C:\Windows\System32\ntdll.dll 7FF661BE1AD0 (Non-module code)	7320 02/22/23, 23:09:32 BUgsm.exe	2/22/2023, 23:09:47.000	2/22/2023, 23:09:49.629
☐	MRKYSELICA-PUSH	ThreadInjection	7	C:\Windows\System32\ntdll.dll 7FF661BE1AD0 (Non-module code)	7320 02/22/23, 23:09:32 BUgsm.exe	2/22/2023, 23:09:46.000	2/22/2023, 23:09:48.823
☐	MRKYSELICA-PUSH	ThreadInjection	7	C:\Windows\System32\ntdll.dll 7FF661BE1AD0 (Non-module code)	7320 02/22/23, 23:09:32 BUgsm.exe	2/22/2023, 23:09:46.000	2/22/2023, 23:09:48.406
☐	MRKYSELICA-PUSH	ThreadInjection	7	C:\Windows\System32\ntdll.dll 7FF661BE1AD0 (Non-module code)	7320 02/22/23, 23:09:32 BUgsm.exe	2/22/2023, 23:09:46.000	2/22/2023, 23:09:49.017
☐	MRKYSELICA-PUSH	ThreadInjection	7	C:\Windows\System32\ntdll.dll 7FF661BE1AD0 (Non-module code)	7320 02/22/23, 23:09:32 BUgsm.exe	2/22/2023, 23:09:45.000	2/22/2023, 23:09:47.114
☐	MRKYSELICA-PUSH	ThreadInjection	7	C:\Windows\System32\ntdll.dll 7FF661BE1AD0 (Non-module code)	7320 02/22/23, 23:09:32 BUgsm.exe	2/22/2023, 23:09:45.000	2/22/2023, 23:09:46.450
☐	MRKYSELICA-PUSH	ThreadInjection	7	C:\Windows\System32\ntdll.dll 7FF661BE1AD0 (Non-module code)	7320 02/22/23, 23:09:32 BUgsm.exe	2/22/2023, 23:09:45.000	2/22/2023, 23:09:46.785
☐	MRKYSELICA-PUSH	ThreadInjection	7	C:\Windows\System32\ntdll.dll 7FF661BE1AD0 (Non-module code)	7320 02/22/23, 23:09:32 BUgsm.exe	2/22/2023, 23:09:44.000	2/22/2023, 23:09:46.133
☐	MRKYSELICA-PUSH	ThreadInjection	7	C:\Windows\System32\ntdll.dll 7FF661BE1AD0 (Non-module code)	7320 02/22/23, 23:09:32 BUgsm.exe	2/22/2023, 23:09:44.000	2/22/2023, 23:09:45.522
☐	MRKYSELICA-PUSH	ThreadInjection	7	C:\Windows\System32\ntdll.dll 7FF661BE1AD0 (Non-module code)	7320 02/22/23, 23:09:32 BUgsm.exe	2/22/2023, 23:09:44.000	2/22/2023, 23:09:45.822
☐	MRKYSELICA-PUSH	ThreadInjection	7	C:\Windows\System32\ntdll.dll 7FF661BE1AD0 (Non-module code)	7320 02/22/23, 23:09:32 BUgsm.exe	2/22/2023, 23:09:43.000	2/22/2023, 23:09:45.193
☐	MRKYSELICA-PUSH	ThreadInjection	7	C:\Windows\System32\ntdll.dll 7FF661BE1AD0 (Non-module code)	7320 02/22/23, 23:09:32 BUgsm.exe	2/22/2023, 23:09:43.000	2/22/2023, 23:09:44.248

Admin view (Console / Endpoints view) ↓



☐	Computer name	OS name	OS major	OS minor	OS build	Last report at	Last update at	Gryphon version	Last boot at	Sessions	Adapters	External IP	Group	Dynamic group	Group change at	Created at ↓	Links
☐	DF05L-SHAMBALLA	Windows 11 Enterprise	10	0	22,621	3/29/2023, 21:04:37.173	3/24/2023, 13:27:47.000	0.0.0.92	3/28/2023, 12:00:15.000	0 1 AzureAD\LukášHlavička	12 adapters:	86.110.246.30	IPv4	✓	3/16/2023, 20:46:21.055	3/16/2023, 20:46:07.403	ALERTS LOGS
☐	LAPTOP-1DOR1ONK	Windows 11 Enterprise	10	0	22,621	3/29/2023, 15:12:20.605	3/24/2023, 13:27:47.000	0.0.0.92	3/23/2023, 08:42:04.000	0 2 AzureAD\MatejLaš	9 adapters:	86.110.246.30	IPv4	✓	2/9/2023, 12:34:45.665	2/9/2023, 09:47:36.650	ALERTS LOGS
☐	LAPTOP-NUQQGAVC	Windows 11 Enterprise	10	0	22,621	3/29/2023, 14:35:41.271	3/24/2023, 13:27:47.000	0.0.0.92	3/28/2023, 11:39:11.000	0 1 AzureAD\MichalMinár	11 adapters:	86.110.246.30	IPv4	✓	2/9/2023, 12:34:45.665	2/9/2023, 08:30:01.393	ALERTS LOGS
☐	DF-10-L-C3PO	Windows 11 Enterprise	10	0	22,621	3/29/2023, 10:16:45.829	3/24/2023, 13:27:47.000	0.0.0.92	3/29/2023, 06:59:36.000	0 1 AzureAD\JánHašta	13 adapters:	87.197.158.86	IPv4	✓	2/9/2023, 12:34:45.665	2/8/2023, 19:13:37.782	ALERTS LOGS
☐	THINKPAD-NATALI	Windows 10 Enterprise	10	0	19,045	3/29/2023, 18:42:20.815	3/24/2023, 13:27:47.000	0.0.0.92	2/8/2023, 14:50:25.000	0 1 AzureAD\NatáliaMaglenová	6 adapters:	95.102.190.3	IPv4	✓	2/8/2023, 14:46:19.208	2/8/2023, 14:38:16.005	ALERTS LOGS
☐	MSI	Windows 11 Pro	10	0	22,621	3/24/2023, 17:42:57.512	3/24/2023, 13:27:47.000	0.0.0.92	3/24/2023, 12:29:30.000	0 1 MSI\stefan.lazovy	8 adapters:	86.110.246.30	IPv4	✓	3/24/2023, 16:05:40.884	2/3/2023, 21:44:04.154	ALERTS LOGS

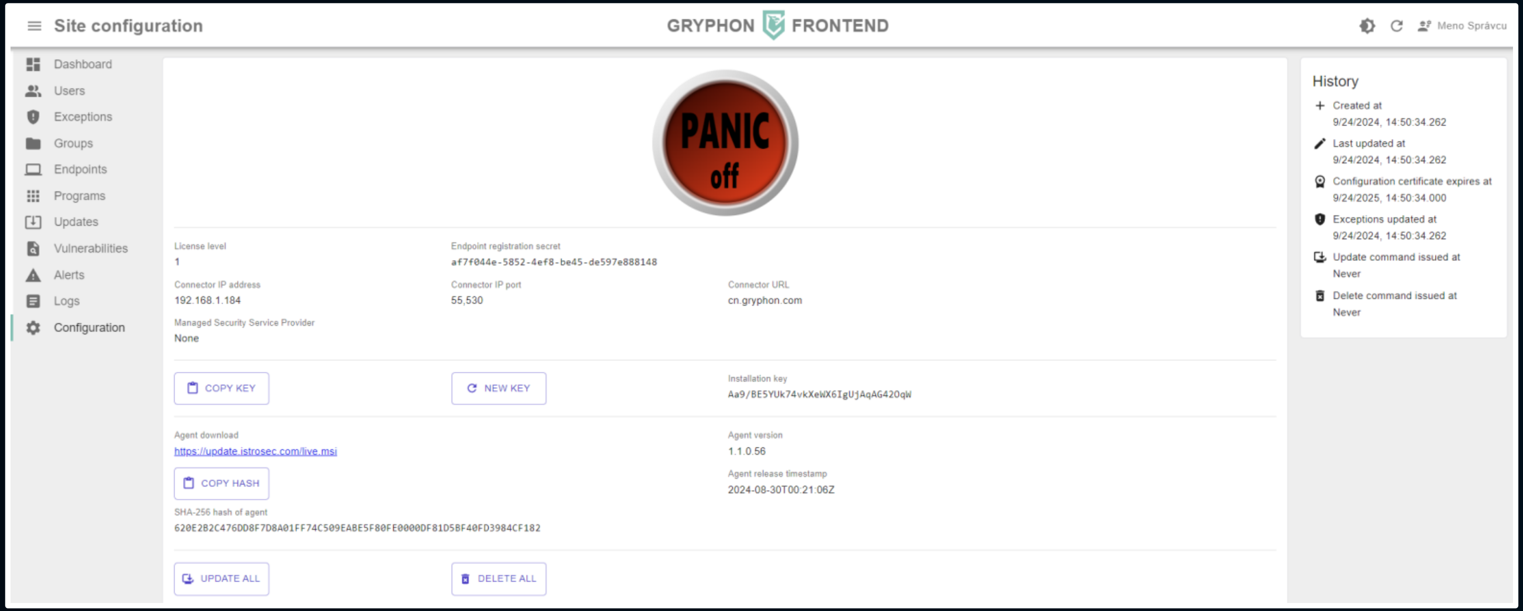
1) Behavioral model of ransomware detection at the endpoint level.

2) Remote execution of commands and actions on selected endpoints

3) Automatic recovery of encrypted / compromised files

4) Visual secure console, secure remote access and forensic file management

5) Central network communication control



License level
1

Endpoint registration secret
af7f044e-5852-4ef8-be45-de597e888148

Connector IP address
192.168.1.184

Connector IP port
55,530

Connector URL
cn.gryphon.com

Managed Security Service Provider
None

Installation key
Aa9/BE5YUk74vkXeWX6IgUjAqAG420qW

Agent download
https://update.istrosec.com/live.msi

Agent version
1.1.0.56

Agent release timestamp
2024-08-30T00:21:06Z

SHA-256 hash of agent
620E2B2C476DD8F7D8A01FF74C509EABE5F80FE0000DF81D5BF40FD3984CF182

History

Created at
9/24/2024, 14:50:34.262

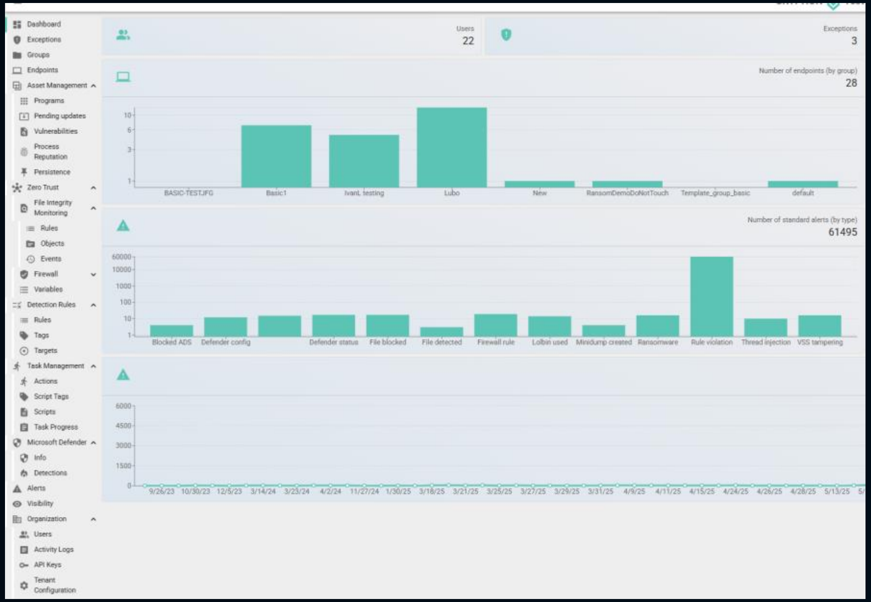
Last updated at
9/24/2024, 14:50:34.262

Configuration certificate expires at
9/24/2025, 14:50:34.000

Exceptions updated at
9/24/2024, 14:50:34.262

Update command issued at
Never

Delete command issued at
Never



Users
22

Exceptions
3

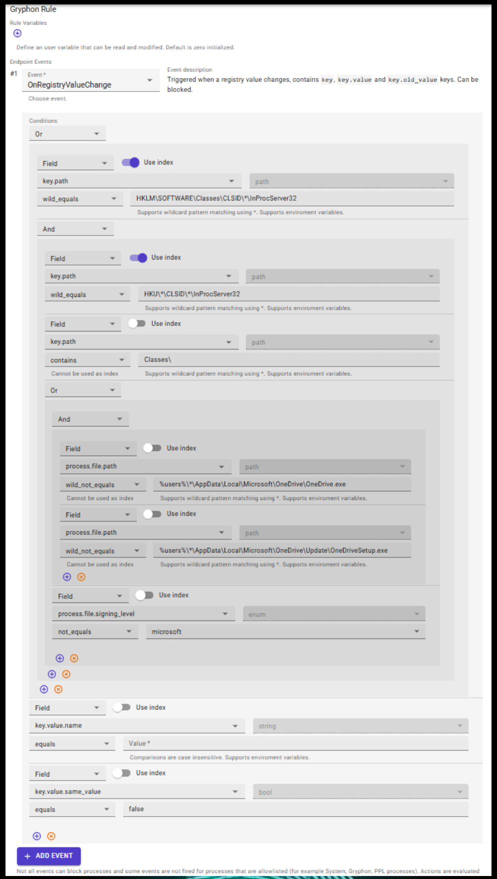
Number of endpoints (by group)
28

Number of standard alerts (by type)
61495

GRYPHON Realtime kernel rules

IstroSec

Gui rule ↓



Gryphon Rule

Rule Variables

⊕

Define an user variable that can be read and modified. Default is zero initialized.

Endpoint Events

#1 Event * OnRegistryValueChange

Choose event.

Event description

Triggered when a registry value changes, contains `key`, `key.value` and `key.old_value` keys. Can be blocked.

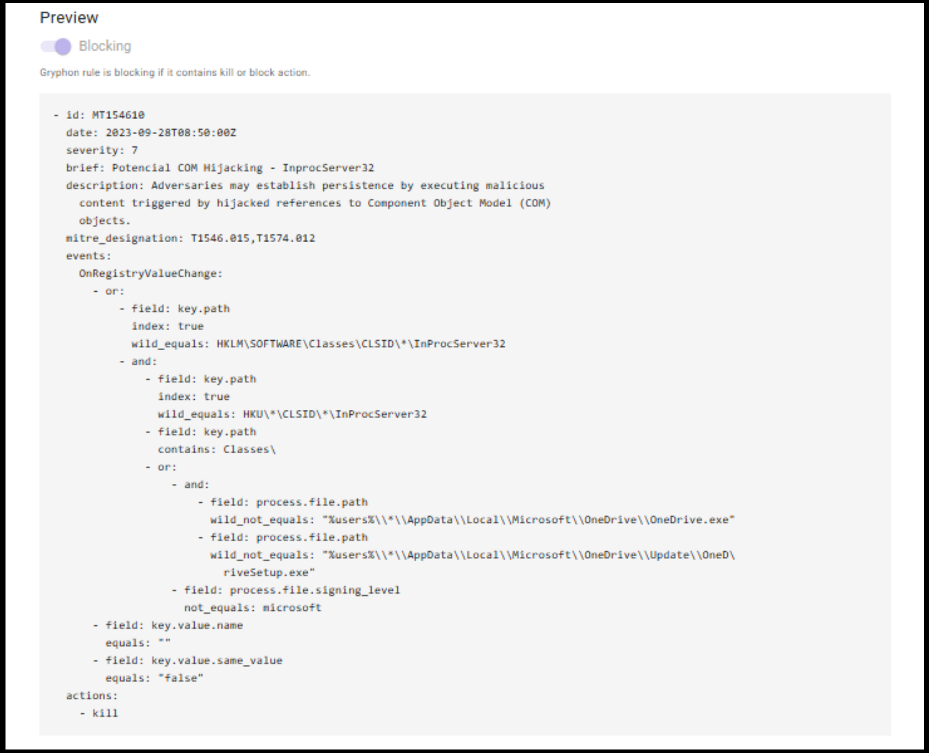
Conditions

Or

- Field — Use index (on)
  - key.path — path
  - wild_equals — HKLM\SOFTWARE\Classes\CLSID\*\InProcServer32
  - Supports wildcard pattern matching using *. Supports enviroment variables.
- And
  - Field — Use index (on)
    - key.path — path
    - wild_equals — HKU*\CLSID*\InProcServer32
    - Supports wildcard pattern matching using *. Supports enviroment variables.
  - Field — Use index (off)
    - key.path — path
    - contains — Classes\
    - Cannot be used as index — Supports wildcard pattern matching using *. Supports enviroment variables.
  - Or
    - And
      - Field — Use index (off)
        - process.file.path — path
        - wild_not_equals — %users%*\AppData\Local\Microsoft\OneDrive\OneDrive.exe
        - Cannot be used as index — Supports wildcard pattern matching using *. Supports enviroment variables.
      - Field — Use index (off)
        - process.file.path — path
        - wild_not_equals — %users%*\AppData\Local\Microsoft\OneDrive\Update\OneDriveSetup.exe
        - Cannot be used as index — Supports wildcard pattern matching using *. Supports enviroment variables.
    - Field — Use index (off)
      - process.file.signing_level — enum
      - not_equals — microsoft
- Field — Use index (off)
  - key.value.name — string
  - equals — Value *
  - Comparisons are case insensitive. Supports enviroment variables.
- Field — Use index (off)
  - key.value.same_value — bool
  - equals — false

Not all events can block processes and some events are not fired for processes that are allowlisted (for example System, Gryphon, PPL processes). Actions are evaluated

Text rule↓

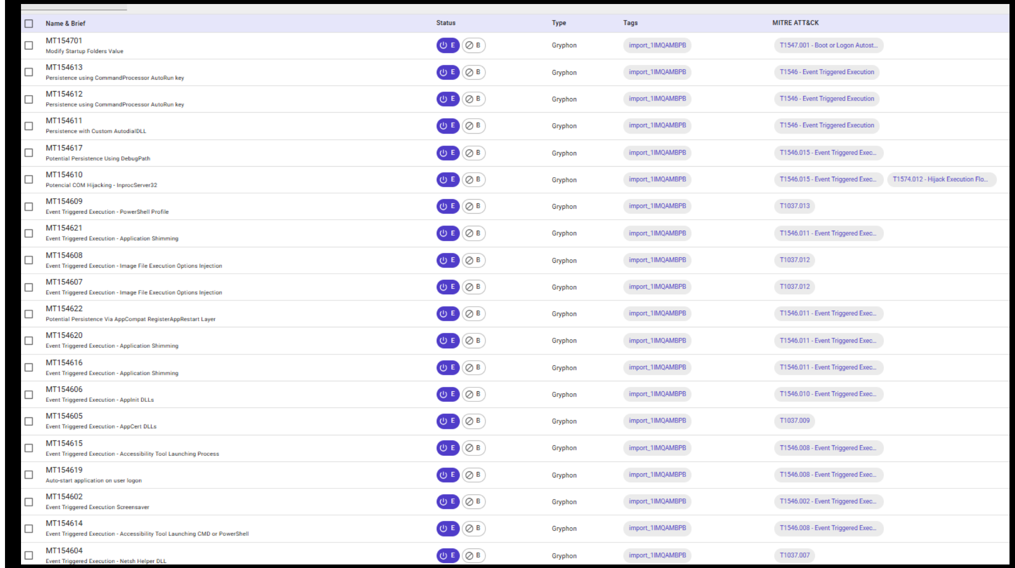


Preview

Blocking

Gryphon rule is blocking if it contains kill or block action.

```yaml
- id: MT154610
  date: 2023-09-28T08:50:00Z
  severity: 7
  brief: Potencial COM Hijacking - InprocServer32
  description: Adversaries may establish persistence by executing malicious
    content triggered by hijacked references to Component Object Model (COM)
    objects.
  mitre_designation: T1546.015,T1574.012
  events:
    OnRegistryValueChange:
      - or:
          - field: key.path
            index: true
            wild_equals: HKLM\SOFTWARE\Classes\CLSID\*\InProcServer32
          - and:
              - field: key.path
                index: true
                wild_equals: HKU\*\CLSID\*\InProcServer32
              - field: key.path
                contains: Classes\
              - or:
                  - and:
                      - field: process.file.path
                        wild_not_equals: "%users%\\*\\AppData\\Local\\Microsoft\\OneDrive\\OneDrive.exe"
                      - field: process.file.path
                        wild_not_equals: "%users%\\*\\AppData\\Local\\Microsoft\\OneDrive\\Update\\OneD\
                          riveSetup.exe"
                  - field: process.file.signing_level
                    not_equals: microsoft
      - field: key.value.name
        equals: ""
      - field: key.value.same_value
        equals: "false"
  actions:
    - kill
```



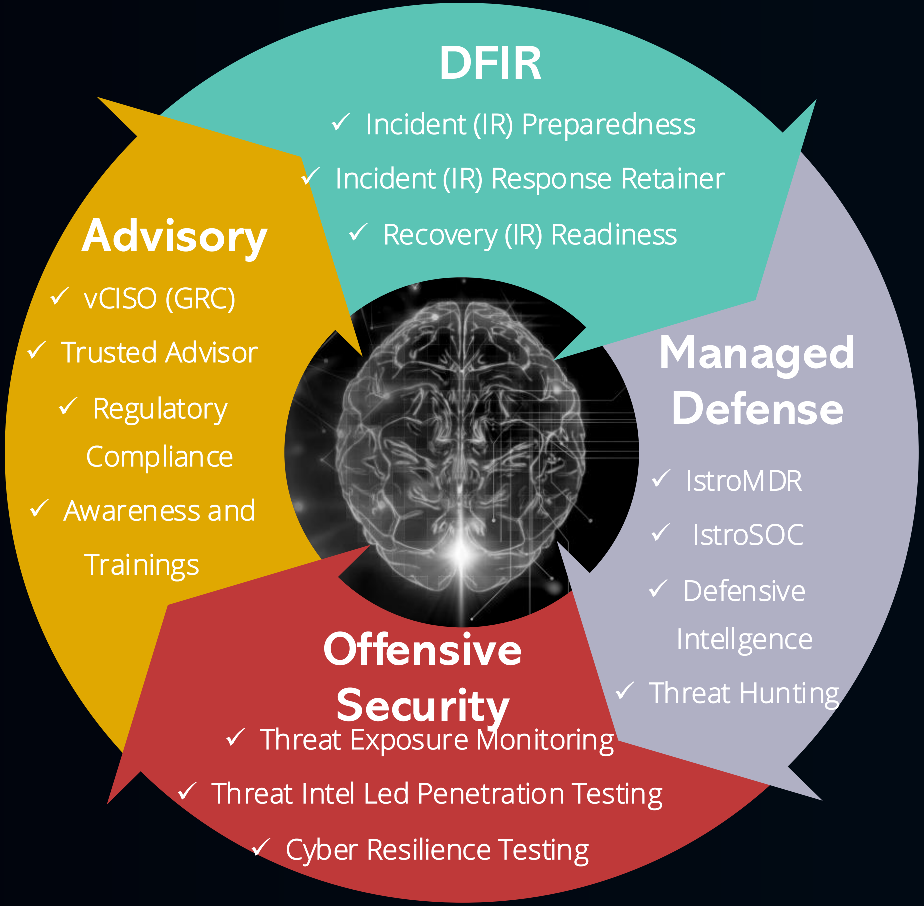
□	Name & Brief	Status	Type	Tags	MITRE ATT&CK
□	MT154701 Modify Startup Folders Value	E ⊘ B	Gryphon	import_1IMQAMBPB	T1547.001 - Boot or Logon Autost...
□	MT154613 Persistence using CommandProcessor AutoRun key	E ⊘ B	Gryphon	import_1IMQAMBPB	T1546 - Event Triggered Execution
□	MT154612 Persistence using CommandProcessor AutoRun key	E ⊘ B	Gryphon	import_1IMQAMBPB	T1546 - Event Triggered Execution
□	MT154611 Persistence with Custom AutodialDLL	E ⊘ B	Gryphon	import_1IMQAMBPB	T1546 - Event Triggered Execution
□	MT154617 Potential Persistence Using DebugPath	E ⊘ B	Gryphon	import_1IMQAMBPB	T1546.015 - Event Triggered Exec...
□	MT154610 Potencial COM Hijacking - InprocServer32	E ⊘ B	Gryphon	import_1IMQAMBPB	T1546.015 - Event Triggered Exec... T1574.012 - Hijack Execution Flo...
□	MT154609 Event Triggered Execution - PowerShell Profile	E ⊘ B	Gryphon	import_1IMQAMBPB	T1037.013
□	MT154621 Event Triggered Execution - Application Shimming	E ⊘ B	Gryphon	import_1IMQAMBPB	T1546.011 - Event Triggered Exec...
□	MT154608 Event Triggered Execution - Image File Execution Options Injection	E ⊘ B	Gryphon	import_1IMQAMBPB	T1037.012
□	MT154607 Event Triggered Execution - Image File Execution Options Injection	E ⊘ B	Gryphon	import_1IMQAMBPB	T1037.012
□	MT154622 Potential Persistence Via AppCompat RegisterAppRestart Layer	E ⊘ B	Gryphon	import_1IMQAMBPB	T1546.011 - Event Triggered Exec...
□	MT154620 Event Triggered Execution - Application Shimming	E ⊘ B	Gryphon	import_1IMQAMBPB	T1546.011 - Event Triggered Exec...
□	MT154616 Event Triggered Execution - Application Shimming	E ⊘ B	Gryphon	import_1IMQAMBPB	T1546.011 - Event Triggered Exec...
□	MT154606 Event Triggered Execution - AppInit DLLs	E ⊘ B	Gryphon	import_1IMQAMBPB	T1546.010 - Event Triggered Exec...
□	MT154605 Event Triggered Execution - AppCert DLLs	E ⊘ B	Gryphon	import_1IMQAMBPB	T1037.009
□	MT154615 Event Triggered Execution - Accessibility Tool Launching Process	E ⊘ B	Gryphon	import_1IMQAMBPB	T1546.008 - Event Triggered Exec...
□	MT154619 Auto-start application on user logon	E ⊘ B	Gryphon	import_1IMQAMBPB	T1546.008 - Event Triggered Exec...
□	MT154602 Event Triggered Execution Screensaver	E ⊘ B	Gryphon	import_1IMQAMBPB	T1546.002 - Event Triggered Exec...
□	MT154614 Event Triggered Execution - Accessibility Tool Launching CMD or PowerShell	E ⊘ B	Gryphon	import_1IMQAMBPB	T1546.008 - Event Triggered Exec...
□	MT154604 Event Triggered Execution - Netsh Helper DLL	E ⊘ B	Gryphon	import_1IMQAMBPB	T1037.007

Out of the BOX more than 800 detection rules known attacks

Out of the box more than 200 RMM detection rules

OUR MISSION

IstroSec



DFIR

- ✓ Incident (IR) Preparedness
- ✓ Incident (IR) Response Retainer
- ✓ Recovery (IR) Readiness

Managed Defense

- ✓ IstroMDR
- ✓ IstroSOC
- ✓ Defensive Intellgence
- ✓ Threat Hunting

Offensive Security

- ✓ Threat Exposure Monitoring
- ✓ Threat Intel Led Penetration Testing
- ✓ Cyber Resilience Testing

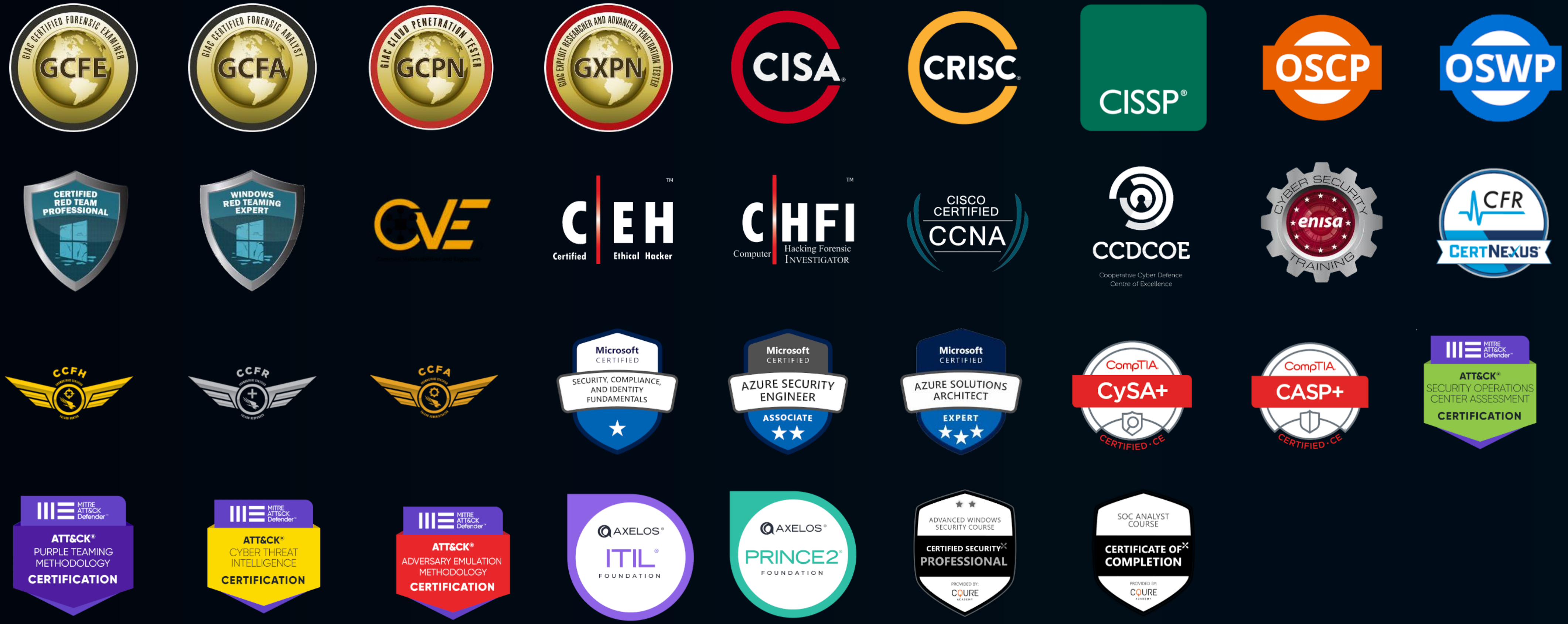
Advisory

- ✓ vCISO (GRC)
- ✓ Trusted Advisor
- ✓ Regulatory Compliance
- ✓ Awareness and Trainings

To be a trusted tactical cyber security intelligence vendor delivering first class advanced services and top-notch toolkits to ensure overall complex cyber resilience.

OUR EXPERIENCES

IstroSec


GIAC CERTIFIED FORENSIC EXAMINER GCFE
GIAC CERTIFIED FORENSIC ANALYST GCFA
GIAC CLOUD PENETRATION TESTER GCPN
GIAC EXPLOIT RESEARCHER AND ADVANCED PENETRATION TESTER GXPN
CISA
CRISC
CISSP
OSCP
OSWP
CERTIFIED RED TEAM PROFESSIONAL
WINDOWS RED TEAMING EXPERT
CVE
C|EH Certified Ethical Hacker
C|HFI Computer Hacking Forensic Investigator
CISCO CERTIFIED CCNA
CCDCOE Cooperative Cyber Defence Centre of Excellence
CYBER SECURITY TRAINING enisa
CFR CERTNEXUS
CCFH
CCFR
CCFA
Microsoft CERTIFIED SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS
Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE
Microsoft CERTIFIED AZURE SOLUTIONS ARCHITECT EXPERT
CompTIA CySA+ CERTIFIED · CE
CompTIA CASP+ CERTIFIED · CE
MITRE ATT&CK Defender ATT&CK® SECURITY OPERATIONS CENTER ASSESSMENT CERTIFICATION
MITRE ATT&CK Defender ATT&CK® PURPLE TEAMING METHODOLOGY CERTIFICATION
MITRE ATT&CK Defender ATT&CK® CYBER THREAT INTELLIGENCE CERTIFICATION
MITRE ATT&CK Defender ATT&CK® ADVERSARY EMULATION METHODOLOGY CERTIFICATION
AXELOS ITIL FOUNDATION
AXELOS PRINCE2 FOUNDATION
ADVANCED WINDOWS SECURITY COURSE CERTIFIED SECURITY PROFESSIONAL PROVIDED BY: CQURE
SOC ANALYST COURSE CERTIFICATE OF COMPLETION PROVIDED BY: CQURE

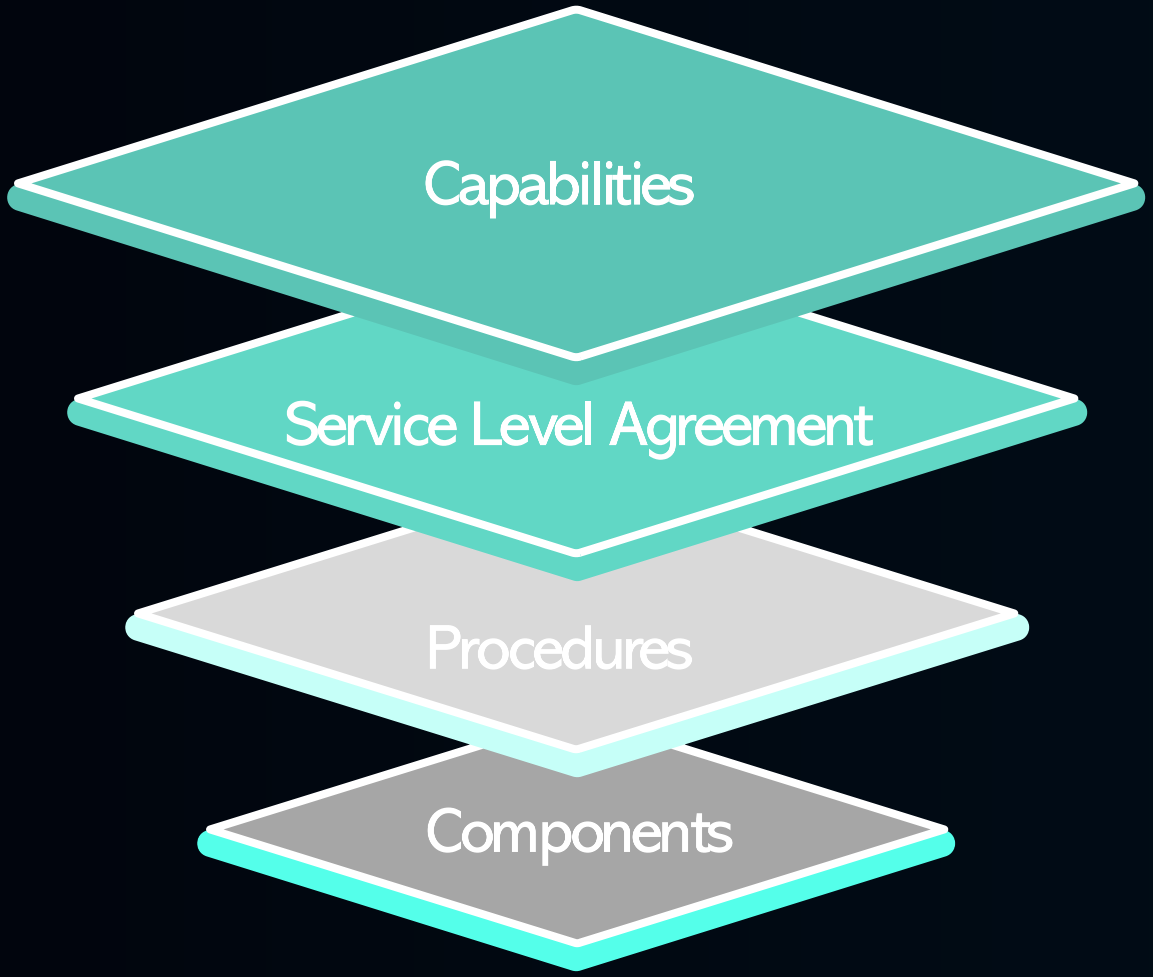
IstroSec

THANK YOU

FOR YOUR ATTENTION

IstroSec

INCIDENT RESPONSE (IR) RETAINER



Capabilities

Service Level Agreement

Procedures

Components

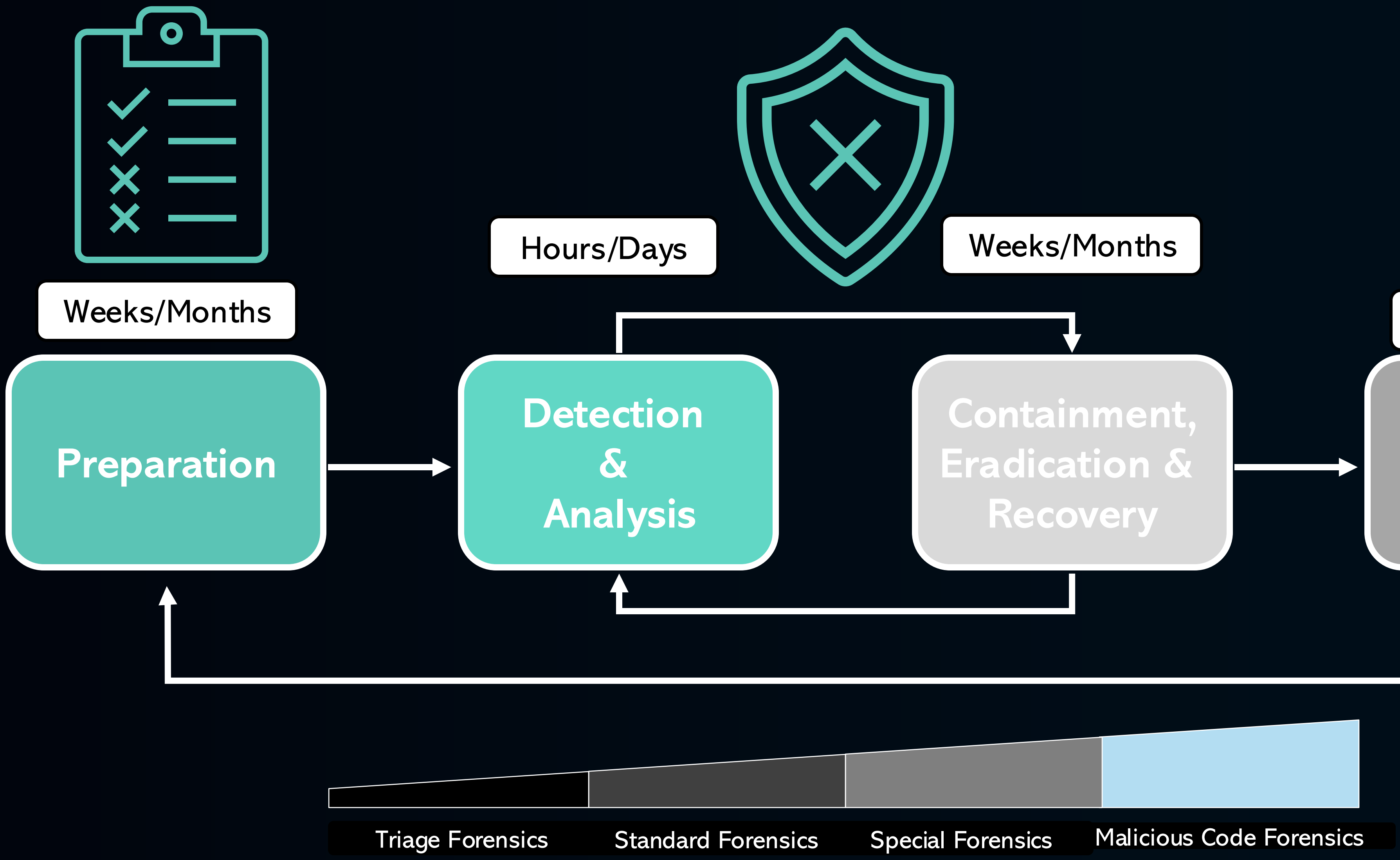
Expertise, Toolkits, Experiences and Methodologies

Special Tiering for 24/7 L4 DFIR services

Expert capacity reservation and 24/7 L4 DFIR services

Methodology based IR service and optional components

IstroSec



Weeks/Months

Preparation

Hours/Days

Detection & Analysis

Weeks/Months

Containment, Eradication & Recovery

Months/Years

Post-Incident Activity

Triage Forensics

Standard Forensics

Special Forensics

Malicious Code Forensics