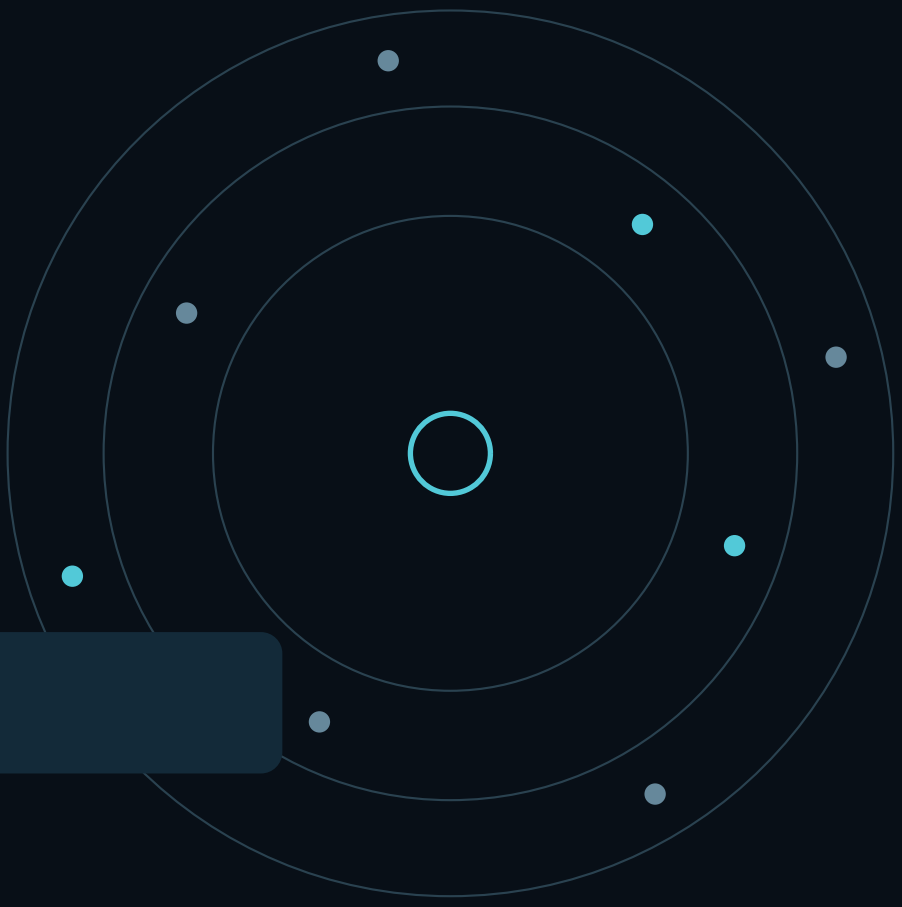
11 / WOLF ENGINE COLLECTION

WOLF CYBERSECURITY

Eight security layers. One connected command environment. Specialist cyber defense, intelligent monitoring and authorized protection for the systems businesses depend on.



EIGHT LAYERS. ONE SECURITY CONTEXT.

Wolf OS + Think Unlimited Cybersecurity

01 / THE CYBER ECOSYSTEM

Protection is a business system.

Wolf Cybersecurity combines technical expertise, connected telemetry and owner-controlled response in a single security operating model.

THE BUSINESS & ITS DIGITAL ESTATE

Websites / APIs / Clouds / Accounts / Windows / Customer Data

WOLF OS / CYBER COMMAND

Live security posture, suspicious traffic, attack events, threat evidence, authorized changes, Windows device checks and executive visibility.

AI & MONITORING

Security automation and evidence analysis

EXPERT CYBERSECURITY

Testing, hardening, response and assurance

The platform organizes security evidence and permissioned actions. Specialist services are delivered under an agreed client scope, with technical validation and human oversight.

02 / EIGHT CYBERSECURITY LAYERS

Observe. Filter. Defend. Discover.

The first four layers establish attack-surface visibility and help distinguish significant digital exposure from background noise.

01

SURFACE MONITORING

Monitor public pages, visible endpoints, certificates, headers, availability and exposed digital assets.

02

BOT & NOISE FILTERING

Distinguish suspicious automation and unwanted traffic patterns from meaningful business activity.

03

GUARD WORKERS

Use automated checks and scheduled workers to watch selected websites, routes and service health.

04

VULNERABILITY AWARENESS

Identify and prioritize weak configurations, risky exposure and findings requiring authorized validation.

These layers are presented as coordinated defensive functions. A detected signal is not automatically a confirmed breach or exploited vulnerability.

03 / EIGHT CYBERSECURITY LAYERS

Control. Investigate. Watch. Explain.

The second four layers connect identity, security evidence, automated vigilance and decisions that business leadership can act on.

05

ACCESS & ACCOUNT HYGIENE

Review staff roles, sensitive accounts, permissions and opportunities to reduce unnecessary exposure.

06

EVENT & LOG INTELLIGENCE

Interpret observed traffic, defenses, incidents and operational records with traceable context.

07

24-HOUR WATCH LOGIC

Run recurring automated observation and alerts for important security and availability signals.

08

EXECUTIVE SECURITY REPORTS

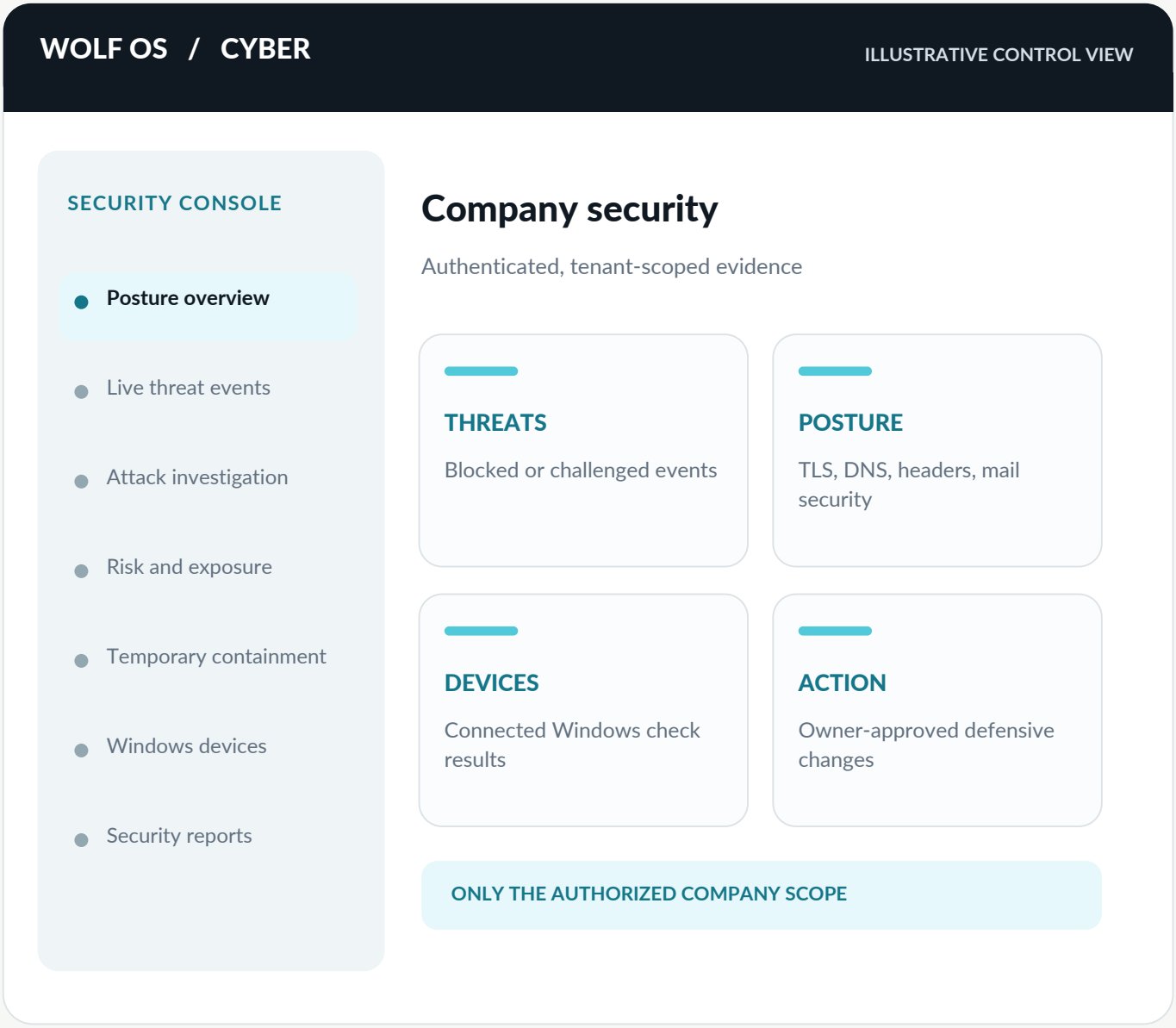
Translate technical findings into prioritized risks, decisions, responsibilities and remediation steps.

Continuous automated checks are distinct from a human-staffed 24/7 response service. The response arrangement depends on the contracted engagement.

04 / WOLF OS CYBER COMMAND

A security cockpit for the company.

Authenticated business workspaces expose their own connected cyber records, incident evidence and protection status.



CONCEPTUAL WORKSPACE / NOT A PRODUCTION SCREENSHOT

The interface groups verified OS Cyber modules. Individual panels and controls depend on entitlement, role, connected domain and available telemetry.

05 / WOLF OS SECURITY CAPABILITIES

A complete security command layer.

Inside the business operating system, security information becomes a practical workspace for observation, investigation, and protected actions.

01

COMPANY ACCESS

A company-scoped security workspace with entitlement checks, mapped domains and protected session roles.

02

SECURITY TELEMETRY

Protected-domain traffic metrics, challenged and blocked events, observed defensive activity and incident history.

03

ATTACK INVESTIGATION

Security incident views with rule context, time, network signals, masked identifiers and evidence-linked explanations.

04

LIVE POSTURE REVIEW

Checks for TLS, HTTPS, DNSSEC, HSTS, CSP, browser security and domain or email configuration.

05

OWNER CONTROLLED FIXES

Selected safety settings may be changed only under authorized access and a reversible, logged workflow.

06

TEMPORARY CONTAINMENT

Scoped, time-limited network blocking with inspection, expiry handling and an explicit reversal path.

07

WINDOWS DEVICE EVIDENCE

Authorized Windows security-state checks and a consolidated result inside the proper company workspace.

08

CONTROLLED EXERCISES

Owner-restricted security exercises with tracked state and rollback, separate from ordinary customer traffic.

Each action remains bound to the authorized client, connected protection source, access role and available evidence. A feature visible in the OS is not universal access to every client account.

06 / CONNECTED CYBER OPERATIONS

From evidence to action in one place.

Wolf OS brings security work closer to business owners while Think Unlimited provides the specialist validation and response behind complex threats.

THE OWNER / COMMAND VIEW

"What is attacking our websites, which assets are exposed, and what can my team safely do today?"

01	**IDENTITY**	Select the authorized company, protected domains and connected security services.
02	**OBSERVATION**	Review live traffic-defense evidence, health checks and Windows protection reports.
03	**ANALYSIS**	Inspect suspicious paths, matched defense rules, identity risks and hardening findings.
04	**DECISION**	Translate technical evidence into a prioritized business risk and a named corrective action.
05	**PROTECTION**	Use owner-permitted security controls, time-bound containment or expert-led remediation.
06	**PROOF**	Recheck the affected service, log actions, retain restore options and brief the owner.

CONNECTED OPERATING MODEL / ILLUSTRATIVE REQUEST, PERMISSIONED ACTIONS

07 / THREAT & ATTACK INTELLIGENCE

From network noise to readable evidence.

Wolf Cyber connects defense events with an investigation room so a company can understand what its protective controls observed.

01

LIVE THREAT STREAM

Review observed blocked, challenged or closed connections for an authorized company.

02

ATTACK-BASED CLASSIFICATION

Interpret rule and request-path evidence to label suspected techniques when justified.

03

TRAFFIC CONTEXT

Summarize protection sources, network origins, targets, event timing and defensive actions.

04

DEFENSIVE MAP

Visualize supported geographic or network evidence without manufacturing attack locations.

05

EVIDENCE LINKS

Keep event identifiers and relevant rule information for investigation and troubleshooting.

06

LEADERSHIP SIGNAL

Explain what was seen, which controls acted and what requires a further review.

An observed blocked request is evidence of a defensive action, not proof that an attacker compromised the business. Attack labels require matching rule or path evidence.

08 / CLOUD, EDGE & EMAIL SECURITY

Harden the paths businesses expose.

Network-edge configuration, transport security, application headers and domain trust can be assessed and improved under authorization.

01

WEB APPLICATION FIREWALL

Review managed security rules, custom controls, rate limiting and challenged traffic.

02

ENCRYPTION & TLS

Evaluate HTTPS enforcement, TLS configuration, origin encryption and certificate posture.

03

DNS & DOMAIN TRUST

Assess DNSSEC, domain records, dangerous exposure and domain-related protections.

04

CONTENT & BROWSER SECURITY

Check HSTS, CSP, framing restrictions, mixed-content protections and security headers.

05

EMAIL AUTHENTICATION

Examine SPF, DKIM and DMARC alignment, reporting and staged enforcement.

06

REVERSIBLE HARDENING

Apply only the authorized safe settings, retain change evidence and verify the live result.

Some hardening actions can break a website or mail flow if applied blindly. Wolf Cyber requires the correct owner authority, evidence and safe rollback.

09 / WINDOWS ENDPOINT VISIBILITY

Bring the device into the security picture.

Wolf OS supports an authorized Windows device security check using protection components already available on the computer.

WINDOWS DEVICE CHECK

A company-authorized device runs the check and submits a concise security-state report to its own Wolf OS workspace using a short-lived enrollment code.

01 **PROTECTION STATUS**

Microsoft Defender status, available antivirus information and observed threat detections.

02 **QUICK SCAN**

On supported devices, request a Defender quick scan and report the recorded status.

03 **FIREWALL & OS**

Firewall profile state, Windows version and recent update information.

04 **SECURITY CONFIGURATION**

User Account Control and disk-encryption state where access permits.

05 **PRIVACY & REPORTING**

A device-state summary rather than reading personal documents, browser history or passwords.

DEVICE CHECKS USE THE HOST OPERATING SYSTEM; THEY ARE NOT A REPLACEMENT AV ENGINE.

10 / SPECIALIST SECURITY TESTING

Test real attack paths - with permission.

Think Unlimited delivers structured security assessments and technical validation for business-critical applications and infrastructure.

01

WEB & APPLICATION SECURITY

Review authentication, sessions, forms, uploads, workflows and abuse of application logic.

02

API PENETRATION TESTING

Test scoped API authentication, authorization, data handling and business logic.

03

NETWORK & INFRASTRUCTURE

Assess exposed services, certificate issues, configurations and segmentation where in scope.

04

CLOUD & SAAS EXPOSURE

Review cloud configuration, publicly accessible data, identity boundaries and risky integrations.

05

RED TEAM VALIDATION

Explore realistic multi-step attack scenarios and control effectiveness under written rules of engagement.

06

REMEDIATION RETEST

Document repeatable evidence, prioritize fixes and independently verify the corrected behavior.

Security tests are restricted to the customer-authorized scope. Intrusive tests, traffic disruption, credential attacks and exploitation are never presumed authorized.

11 / CONTINUOUS SECURITY OPERATIONS

Stay aware between security reviews.

Scheduled watchers, monitoring workers, operational records and alerts help teams identify problems that cannot wait for the next audit.

01

WEBSITE & SERVICE HEALTH

Observe important host and route availability, external access, response failures and changes in service state.

02

PROTECTION-EVENT MONITORING

Collect and summarize supported threat and firewall activity for protected company domains.

03

SECURITY POSTURE CHANGES

Watch security configuration evidence for deviations and emerging weaknesses.

04

ESCALATION & PRIORITIZATION

Convert evidence into actionable alerts and route exceptions to the responsible owner or operator.

05

REVIEW & TREND CONTEXT

Retain activity records, summarize incidents and distinguish recurring patterns from one-off noise.

06

MANAGED DELIVERY

Combine automated visibility with contracted specialist reviews, incident triage and agreed response arrangements.

Monitoring operates on configured, authorized services. A human-response SLA or staffed 24-hour operations desk is specified separately in the customer service agreement.

12 / INCIDENT RESPONSE & CONTAINMENT

A response that is clear - and reversible.

Wolf Cyber pairs evidence-led response actions with explicit approval, expiry rules and a record of what changed.

01 DETECT	A protected site or monitoring source records an actionable abnormal event or security gap.
02 VALIDATE	Confirm the affected client, domain, evidence source and potential business impact.
03 AUTHORIZE	The company owner or permitted operator approves any protective change that modifies live traffic.
04 CONTAIN	Where supported, apply a scoped network block or safe hardening control with an undo path.
05 LIFT OR RESTORE	Time-limited rules expire; approved manual reversals and recovery procedures remain available.
06 REVIEW	Confirm the actual effect, preserve evidence and communicate the findings to leadership.

Temporary network containment and automated cleanup are actual OS capabilities for connected zones. They require role and scope checks; not every incident is suitable for automatic blocking.

13 / GOVERNANCE, PRIVACY & RECOVERY

Security extends beyond the firewall.

Secure operations depend on people, permissions, customer data, change control, resilience and verifiable evidence.

01

IDENTITY & ACCESS

Account and role review, least privilege, administrative boundaries and verification of permitted actions.

02

TENANT DATA SEPARATION

Keep each company's threat evidence, connected domains, tokens and operational records separated.

03

APPLICATION GOVERNANCE

Secure release checks, approval records, configuration review and change accountability.

04

DATA & CUSTOMER TRUST

Review sensitive records, secure storage, handling practices and exposed customer workflows.

05

RESILIENCE & RECOVERY

Assess backup readiness, restore pathways, monitoring and operational continuity plans.

06

REGULATORY READINESS

Conduct scoped gap assessment and technical discovery for relevant requirements, including PCI DSS when applicable.

A security assessment or PCI DSS scoping engagement is not itself an audit certification or guarantee of compliance. Evidence, scope and independent assessment determine any formal outcome.

14 / COMPLETE CYBERSECURITY PRACTICE

From assessment to defense.

A broad professional service catalog connects technical testing, operational hardening and business-oriented risk management.

01

CYBER RISK ASSESSMENT

Business-critical asset and exposure review.

02

VULNERABILITY ASSESSMENT

Prioritized technical findings and validation.

03

PENETRATION TESTING

Authorized application and infrastructure testing.

04

RED TEAM EXERCISES

Realistic attack-path and control validation.

05

WEB & API SECURITY

Login, authorization and business-logic testing.

06

CLOUD & SAAS SECURITY

Configuration, identity and integration reviews.

07

ENDPOINT & WINDOWS

Device posture, malware defenses and OS hygiene.

08

NETWORK & EDGE DEFENSE

WAF, bot, TLS, DNS and service protection.

09

DETECTION & MONITORING

Security-event review and threat awareness.

10

INCIDENT RESPONSE

Evidence triage, scoped containment and recovery.

11

COMPLIANCE READINESS

Framework gap review and control evidence.

12

SECURITY ADVISORY

Executive reporting, remediation plans and retesting.

Every engagement has an approved scope, protected systems, named responsibilities, delivery method and evidence standard. Product automation complements expert delivery.

15 / BUSINESS PROTECTION JOURNEY

One request. A coordinated defense.

An illustrative owner journey joins a website security review, staff account hygiene and Windows device checks.

BUSINESS OWNER / COMMAND BRIEF

“Review my websites and staff devices, show me suspicious attacks, explain the most serious weaknesses and prepare safe fixes for approval.”

01	COLLECT	Map the authenticated business domains, available security telemetry and connected device checks.
02	ASSESS	Review attack events, TLS and DNS settings, security headers, access concerns and endpoint status.
03	VALIDATE	Separate observed events from confirmed weaknesses; schedule expert testing where needed.
04	RECOMMEND	Rank verified issues by severity and operational impact, with proposed actions and rollback.
05	ACT & REPORT	Perform owner-approved safe changes, retest, and deliver a clear evidence-based security summary.

ILLUSTRATIVE OWNER JOURNEY / EXECUTION DEPENDS ON THE AUTHORIZED CONNECTORS.

16 / UNIFIED WOLF ENGINE ARCHITECTURE

Security belongs in every engine.

The security practice connects to Wolf OS and the adjacent intelligence, governance and operational systems.

WOLF CYBERSECURITY

Security monitoring, authorized testing, incident evidence, protective controls, endpoints and executive risk reporting.

01	WOLF OS	Company-scoped security panels, roles, posture checks, device reports and approved changes.
02	WOLF MANAGEMENT	Conversational owner access to connected business evidence and prepared security actions.
03	WOLF SHADOW	Pre-release verification, audit records and controlled change governance.
04	WOLF SIGNAL	Trusted event pipelines and measurement integrity for connected websites.
05	WOLF COMMANDER	Orchestration of permitted checks, tasks, reporting and verification routines.

CONNECTIONS USE AUTHORIZED COMPANY DATA, ENTITLEMENTS AND APPROVED WORKFLOWS.

17 / PRODUCT & SERVICE PROFILE

Security, delivered with accountability.

Wolf Cybersecurity unites the eight-layer monitoring model, a connected OS security workspace and a comprehensive specialist practice.

EIGHT-LAYER MODEL	Surface, bots, guard workers, vulnerability, access, events, watch logic and executive reporting.
WOLF OS CYBER	Threat monitoring, defensive events, attack room, posture and controlled containment.
WINDOWS SECURITY	Consent-based device check, native protection status, quick scan and OS configuration.
SPECIALIST TESTING	Authorized web, API, infrastructure, cloud, red team and remediation assessments.
DEFENSIVE DELIVERY	Hardening, monitoring, incident triage, reversible changes and follow-up verification.
GOVERNANCE	Company identity, evidence, access control, reporting and recovery planning.
CLIENT ACCESS	Features depend on service scope, subscribed entitlements, connected domains and owner permissions.

THE THINK UNLIMITED STANDARD

Authorized scope. Security evidence. Clear action. Verified outcomes. Expert-led services and AI-assisted protection are combined without promising invulnerability, unsupported automation or automatic compliance certification.