TACTICAL NEW ORDER
MANAGED CYBER PROTECTION

HUMAN VALIDATION

MACHINES FIND NOISE. OPERATORS FIND TARGETS.

CYBER SECURITY THAT STOPS HACKERS

TACTICAL

WWW.NEWORDERGROUP.NET

ISO/IEC 27001 & ISO9001

// 01 // EXTERNAL CTEM & ASM

THE CRUX — HUMAN VALIDATION

Continuous external reconnaissance, fused with a tactical human validation layer, delivered as a managed cyber operation. Every exposure our autonomous discovery surfaces is triaged, verified, and weaponised into a remediation decision by a NEWORDER operator before it ever reaches your team.

> // TACTICAL DOCTRINE
>
> **WE DO NOT WATCH. WE HUNT. EVERY DOMAIN ON YOUR PERIMETER IS TERRAIN. EVERY FORGOTTEN SUBDOMAIN IS A FLANKING ROUTE. EVERY LEAKED CREDENTIAL IS AN INSERTION POINT. WE GET THERE FIRST.**

ADVERSARY-SIDE
EXTERNAL, UNAUTHENTICATED, CONNECTORLESS BY DESIGN

24 / 7
CONTINUOUS RECONNAISSANCE AND OPERATOR REVIEW

100+ GROUPS
RANSOMWARE CREWS TRACKED BY NAME ON THE DARK WEB

// FIVE QUESTIONS NO ALGORITHM CAN CLOSE

Our tactical analysts do not simply review alerts. They operate the intelligence. Every exposure surfaced by the autonomous discovery layer moves through a deliberate tactical review before it ever touches your team.

01
IS THIS REAL?

False positives are eliminated before they reach you. If we cannot independently confirm the exposure, it does not advance.

02
IS THIS YOURS?

Legal-grade attribution. We verify asset ownership with evidence you can defend to an insurer, an auditor, or a board.

03
IS THIS EXPLOITABLE?

Validated against known adversary behaviour, exploit probability, and ransomware group targeting — not vanity severity.

04
IS THIS PART OF A CHAIN?

We correlate isolated findings into complete attack paths. One exposure is a finding. Five in sequence is a breach timeline.

05
WHAT DO WE DO ABOUT IT?

A prioritised remediation mandate, not a homework assignment. Validated, ranked, actionable — ready for your team to execute.

AUTOMATION PRODUCES A LIST. NEWORDER PRODUCES A DECISION.

You are not buying software. You are buying a tactical cyber team operating a purpose-built intelligence platform on your behalf, twenty-four hours a day, against an adversary who never sleeps.

// 02 // EXTERNAL CTEM & ASM

EXTERNAL ATTACK SURFACE MANAGEMENT

THE TERRAIN. THE ASSETS. THE EXPOSURES.

External ASM is the tactical discipline of continuously discovering, inventorying, and assessing every asset, identity, and exposure your organisation presents to the open internet. Not what you think you own — what the adversary can actually see, touch, and use as an insertion point.

Our capability operates as a forward-deployed reconnaissance element outside your organisational perimeter. Purely external, unauthenticated discovery across your complete digital footprint, using only a domain name. No agents. No API keys. No internal credentials. No connectors into your production estate.

// SIX DISCOVERY VECTORS

DOMAIN & SUBDOMAIN INFRASTRUCTURE

Every registered asset, every DNS configuration, every dangling record, every forgotten perimeter.

SANCTIONED & UNSANCTIONED CLOUD

AWS, Azure, GCP assets, open buckets, shadow SaaS, orphaned resources across the decentralised edge.

EXPOSED CREDENTIALS & SECRETS

Leaked API keys, RSA private keys, hardcoded database credentials, tokens in public code repositories.

TECHNOLOGY STACK FINGERPRINT

Nearly 4,000 public-facing technologies detected — CDNs, WAFs, CRMs, DevOps — checked against vulnerable versions.

DARK WEB & UNDERGROUND PRESENCE

Compromised credentials, 100+ tracked ransomware groups, underground forum chatter targeting your brand.

BRAND, SENTIMENT & NARRATIVE RISK

Executive impersonation, domain squatting, public filings, and negative news that trigger hacktivist interest.

// BREAKING THE CONNECTOR TRAP

Traditional tools force your team into a labyrinth of API keys, agents, and permissions that leaves you blind to shadow IT and orphaned assets — the hidden majority of your attack surface. NEWORDER refuses that model. We operate from the outside in, exactly as an adversary does, and we see exactly what an adversary sees.

// TACTICAL RATING OUTPUT — A TO F, EVIDENTIARY, LEGAL-GRADE

Web Application Hijack · Subdomain Takeover · Cyber Risk Exposure · BEC & Phishing · Data Leak · Supply Chain & Third-Party · Non-Human Identity · Breach & Ransomware · Brand Damage · ESG Exposure.

// 03 // EXTERNAL CTEM & ASM

TACTICAL RECONNAISSANCE MODULES

TEN INVESTIGATION DISCIPLINES — ONE ADVERSARY-EYE VIEW

Our autonomous discovery layer is a coordinated suite of ten tactical reconnaissance disciplines, each purpose-built to find a specific class of exposure that adversaries routinely weaponise. Operators orchestrate, fuse, and validate.

// THE TEN MODULES

10 / 10 MODULES LIVE

M/01

DOMAIN INTELLIGENCE

Full DNS landscape. Dangling records, subdomain takeovers, Web3 squatting, HSTS / CSP / SPF / DMARC weaknesses.

M/02

SENSITIVE CODE EXPOSURE

Tactical sweeps of public code. Leaked API keys, RSA keys, hardcoded credentials, database strings, proprietary logic.

M/03

CLOUD & SAAS EXPOSURE

Unmasks Machine Ghosts and misconfigured buckets. AWS, Azure, GCP — sanctioned, unsanctioned, and orphaned.

M/04

ONLINE SHARING EXPOSURE

Continuous watch on document-sharing and paste sites. Closes the Certainty Intelligence gap beyond internal DLP.

M/05

SENTIMENT & FINANCIALS

SEC filings, 8-K incidents, lawsuits, ESG violations — indicators that predict hacktivist and adversary targeting spikes.

M/06

ARCHIVED WEB PAGES

Historic snapshots reveal credentials, endpoints, and abandoned infrastructure that never appear in current crawls.

M/07

DARK WEB PRESENCE

Illicit forums and marketplaces. 100+ ransomware groups tracked by name. Disrupts narratives before encryption begins.

M/08

TECHNOLOGY STACK

Live inventory of frameworks, servers, third-party scripts. Ground truth for CVE targeting across your portfolio.

M/09

SEARCH ENGINE EXPLOITATION

Operator-driven advanced querying. Surfaces indexed sensitive directories and configuration files internal tools miss.

M/10

SOCIAL MEDIA

Conversational attack surface. Executive impersonations, LinkedIn persona cloning, social engineering preparation.

THE RECONNAISSANCE DOES NOT OPERATE ITSELF.

The modules are the weapons. Our operators are the service. Raw intelligence is fused, verified, and weaponised into decision-ready output before it ever reaches your team.

// 04 // EXTERNAL CTEM & ASM

THE CTEM MISSION CYCLE

CTEM IS NOT A TOOL. IT IS A TACTICAL MISSION CYCLE.

Continuous Threat Exposure Management is a cyclical, continuous programme that manages your security posture by identifying, prioritising, and mitigating real-world threats across your external attack surface. Most organisations cannot run CTEM at the required tempo internally. This is where NEWORDER inserts.

// THE FIVE PHASES

01	**SCOPING** DEFINE THE THEATRE	Agree the full digital footprint with executive stakeholders — subsidiaries, acquisitions, cloud tenants, third parties. This becomes the operating theatre for the mission cycle.
02	**DISCOVERY** MAP THE TERRAIN	Purely external, unauthenticated reconnaissance across the scoped theatre. Operators monitor collection in real time and expand scope as newly attributed assets appear.
03	**PRIORITISATION** RANK THE TARGETS	Automation ends, Human Validation begins. Analysts fuse discovery with KEV data, exploit probability, ransomware targeting, and your business context to rank real breach likelihood.
04	**VALIDATION** CONFIRM THE KILL CHAIN	Every prioritised exposure is validated by a human. Ownership, exploitability, and attack path confirmed. Attack Choke Points are identified and marked for decisive action.
05	**MOBILISATION** ISSUE THE MANDATE	A prioritised, actionable remediation mandate with legal-grade attribution, framework mapping (PCI, HIPAA, GDPR, POPIA, NIST, ISO 27001, SOC 2) and MITRE ATT&CK correlation.

// WORKED EXAMPLE · THE LEAKED CREDENTIAL CHAIN

ONE CHAIN. BROKEN AT THE CHOKE POINT.

Sensitive Code Exposure surfaces an AWS Access Key and database credential in a public GitHub repo. Dark Web Presence flags a linked email in a recent dump. Domain Intelligence notes a weak DMARC policy on the same domain. Automation would produce three separate findings. Our operators correlate them into a single validated attack chain and the client receives one mandate: rotate credentials, harden DMARC, monitor the dump for reuse.

// 05 // EXTERNAL CTEM & ASM

WE SHARPEN YOUR STACK

INTEGRATION WITH CLIENT SECURITY OPERATIONS

Our service is an outside-in intelligence and operations layer. It does not replace your SIEM, EDR, vulnerability management, or SOC. It feeds them with validated, prioritised, tactically relevant intelligence that makes every internal tool more effective.

// FOUR INTEGRATION POINTS

// NEWORDER + SIEM

PRIOR KNOWLEDGE OF THE ADVERSARY TOOLKIT

Validated compromised credentials are sent to your SIEM as watch lists. The SIEM alerts the moment those specific usernames attempt authentication, catching the initial breach attempt at the exact second it happens.

// NEWORDER + VPM

SPEND FINITE REMEDIATION CAPACITY WELL

Risk-based prioritisation fuses KEV feeds, exploit probability, and active ransomware targeting. Your VPM tool focuses on the two or three CVEs most likely to cause a real breach — not thousands of tickets.

// NEWORDER + GRC

AUDIT TRAIL BUILT INTO THE FINDING

Every validated finding is mapped to PCI DSS, HIPAA, GDPR, POPIA, NIST CSF, ISO 27001, and SOC 2. GRC receives evidence packages already formatted for audit, regulators, and insurers.

// NEWORDER + BOARD

GOVERN CYBER — DON'T JUST REPORT ON IT

Technical exposure translated into business-centric metrics and MITRE ATT&CK mapping. Your CISO walks into the boardroom with defensible, empirical evidence in language the board can defend.

// 06 // THE NEWORDER DIFFERENTIATORS

WHY IT EXISTS · WHY IT WORKS · WHY WE WIN

FIVE DIFFERENTIATORS

ADVERSARY PATH ENGINEERING	We do not list vulnerabilities. We reconstruct the exact sequence an adversary would use to breach you, and we break the chain at the choke point.
HUMAN VALIDATION AT SCALE	Trained analysts validate every exposure before it reaches you. No false positives, no wasted remediation cycles, no alert fatigue — only decision-ready intelligence.
OUTCOME OVER OUTPUT	We measure ourselves on exposures closed and attack chains broken, not findings surfaced. If the work does not change your risk posture, it does not count.
SPEED TO INSIGHT	Continuous reconnaissance, operators acting in operational time, not quarterly review time. The tempo of defence must match the tempo of attack.
INTEGRATED LEADERSHIP & EXECUTION	We engage the CISO, GRC, board, and external counsel directly — translating tactical output into strategic decisions. Same team, same tempo, top to bottom.

DISCOVER

CONNECTORLESS EXTERNAL RECON FROM A SINGLE DOMAIN SEED. ZERO AGENTS. ZERO BLIND SPOTS.

VALIDATE

HUMAN OPERATORS TRIAGE EVERY FINDING. REAL, YOURS, EXPLOITABLE, CHAINED, ACTIONABLE.

MOBILISE

PRIORITISED REMEDIATION MANDATES WITH LEGAL-GRADE ATTRIBUTION, NOT BACKLOGS OF ALERTS.

// 07 // EXTERNAL CTEM & ASM

FREQUENTLY ASKED QUESTIONS

OPERATIONAL Q&A

// EIGHT QUESTIONS

Q / WHAT IS HUMAN VALIDATION, AND WHY DOES IT MATTER?

A trained analyst personally reviews, confirms, and contextualises every exposure our autonomous discovery layer surfaces before delivery. Automation cannot distinguish real exploit from benign artefact, attribute with legal confidence, or reconstruct multi-step chains.

Q / HOW IS THIS DIFFERENT FROM BUYING AN EASM PLATFORM?

A platform is software. We sell the operation of a platform by a tactical team, validated by analysts, delivered as a managed service. You are left with validated intelligence and executed outcomes, not licence cost.

Q / HOW DO YOU DISCOVER ASSETS WITHOUT AGENTS OR CREDENTIALS?

Iterative, recursive attribute discovery from a single domain seed. Each query feeds the next, producing a self-expanding loop that uncovers shadow IT and orphaned assets from an adversary-centric perspective.

Q / HOW DOES THIS REDUCE SOC BURNOUT AND ALERT FATIGUE?

By refusing to send unvalidated findings. Every alert has been confirmed, prioritised, and correlated by a human operator. Your SOC does not receive more work — it receives higher-quality work.

Q / WHY BETTER THAN LEGACY SECURITY RATING AGENCIES?

Legacy agencies issue delayed, opaque scores from black-box algorithms on stale data. NEWORDER delivers continuous, transparent, objective ratings backed by legal-grade attribution you can defend.

Q / DOES THIS REPLACE TRADITIONAL THREAT INTELLIGENCE FEEDS?

Yes — with better signal. Generic feeds deliver global macro data with no bearing on you. We deliver personalised tactical intelligence fused with your verified external assets.

Q / HOW DIFFICULT IS THE SERVICE TO DEPLOY?

Near zero. We require only a domain name to begin. No internal agents, API connectors, credentials, or change management. Validated findings begin reaching your team inside the first operational cycle.

Q / WHAT MAKES THIS TACTICAL RATHER THAN THEORETICAL?

We operate adversary-side. Every output is actioned by a human, not a dashboard. We measure on exposures closed and attack chains broken — operational outcomes, not reports.

WANT TO SEE YOUR BUSINESS THE WAY ATTACKERS DO?

Contact us for a no-obligation discussion. We require only a domain name to begin. Validated findings reach your team inside the first operational cycle.

ENGAGE →

WEB NEWORDERGROUP.NET · EMAIL INFO@NEWORDERGROUP.NET