

— PREMIUM MANAGED CTI • OPTION 04

See what attackers see.

Premium Managed CTI turns external signals into confirmed, fixed risk. Continuous clear- and dark-web monitoring, ~18-source IOC enrichment and analyst-reviewed relevance — then validation of what's actually exploitable, operated by the QMasters CTI team as an extension of your security function.

2INTELLIGENCE ENGINES
REACTIVE + PROACTIVE**~18**IOC ENRICHMENT
SOURCES**200K+**VALIDATED IOC
BLOCKLIST
20+ FEEDS • 3-HOURLY**6-STEP**VULNERABILITY-CTI
LIFECYCLE

WHAT PREMIUM ADDS • OVER OPTION 03

• Premium CTI vendors, operated for you

Cyberint, Kaspersky and more — run by our CTI team, not handed to you as another login.

• Validated exposure

We confirm findings with evidence, not just flag them.

• Vulnerability assessment

In-scope weaknesses assessed and prioritized by real impact.

• Selected penetration testing

Deeper testing where warranted — under written rules of engagement.

— WHAT YOU GET

- ✓ Clear + dark-web monitoring — code, paste, Telegram, Tor forums, ransomware feeds
- ✓ On-demand IOC enrichment — any indicator, ~18 sources, verdict in seconds
- ✓ Leaked-credential & identity exposure, tied to your org
- ✓ External attack-surface mapping — domains, hosts, services
- ✓ Analyst-reviewed relevance — AI classifies, humans confirm
- ✓ Validated exposure & selected testing on authorized scope

01 • INTELLIGENCE

See it first

Continuous clear- and dark-web coverage, enriched and analyst-reviewed for relevance to you.

02 • VALIDATION

Confirm what's real

Match vulnerabilities to your exposure and prove exploitability under rules of engagement.

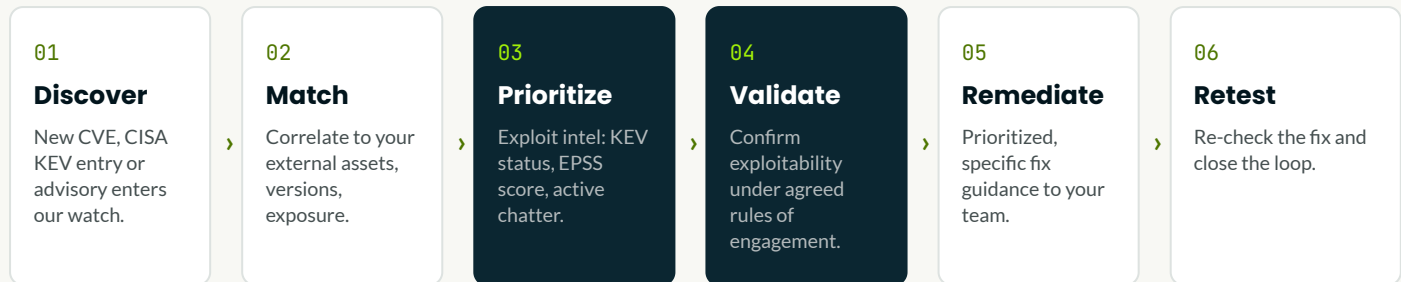
03 • ACTION

Fix what matters

Validated indicators to your SIEM and firewalls; prioritized remediation your team can run.

— HOW IT WORKS · VULNERABILITY CTI

From a new CVE to a **fixed, retested risk**.



STEPS 04-06 RUN ONLY ON AUTHORIZED TARGETS, WITHIN AGREED WINDOWS AND RULES OF ENGAGEMENT.

— PROOF · FROM RECENT ENGAGEMENTS

What this surfaces in the real world.

FINANCIAL CLEARING HOUSE · SIEM DISCOVERY, 3-DAY WINDOW

77.6%

of firewall-deny traffic was tied to known-bad IPs (8,365 of 10,776) — noise turned into prioritized action.

- Leaked credentials recovered on the deep web; 87 accounts enumerable
- Delivered: a 200K+ malicious-IP blocklist, synced to firewalls every 3 hours

TOP-TIER LAW FIRM · EXTERNAL ASSESSMENT

7,988 / 18,701

firewall-denied IPs scanned carried >50% malicious confidence — many already on public blocklists.

- External recon escalated to administrator access on the service desk
- MiCollab path-traversal CVE-2024-41713 (CVSS 9.1, on CISA KEV)

ANONYMIZED · AUTHORIZED EXTERNAL ASSESSMENTS · CVEs ARE PUBLIC REFERENCES.

TWO ENGINES

Reactive + proactive

An analyst looks up any indicator on demand (IP · domain · URL · hash) while the platform continuously watches your exposure across code, paste, dark web and Telegram.

DELIVERS INTO YOUR STACK

No new appliance

Validated intelligence feeds the tools you already run.

Fortinet

Palo Alto

Check Point

QRadar

CrowdStrike NG-SIEM

STIX/TAXII

CSV

JSON/REST

Engagement & trust — a named CTI analyst, agreed reporting cadence, and written rules of engagement for any testing. Premium works mostly from the outside in, so onboarding is light and sensitive data stays with you — aligned to **INCD** guidance, **Bank of Israel Directive 361** (where applicable) and **Privacy Protection Law Amendment 13**.

Start with an **Exposure & Vulnerability Snapshot**
— a scoped 2–3 week engagement on your own environment.

sales@qmasters.co
qmasters.co
Tel Aviv, Israel