— REAL VISIBILITY. RAPID RESPONSE.

Block before they knock.

The QMasters IOC service is a daily-curated IP blacklist — 150,000–200,000 verified malicious addresses tied to active scanners, C2 infrastructure, phishing hosts, and hacking campaigns. Cross-referenced across 20+ direct feeds, pushed inline to FortiGate, Palo Alto, and Check Point every three hours. No appliance. No ingestion script. No analyst time.

200K peak
VERIFIED MALICIOUS IPS

3 hours
REFRESH CADENCE

20+
DIRECT FEEDS

0 touch
MANUAL SYNC

Daily IP blacklist

LIVE · SYNC

INDICATOR	VECTOR	SEVERITY
185.243.115.84	Scanner	WARNING
45.142.213.10	C2 infrastructure	CRITICAL
91.218.50.122	Phishing host	CRITICAL
162.247.74.27	Hacking campaign	CRITICAL

— WHAT YOU GET

- **Inline IP blocking.** Hourly sync into FortiGate, Palo Alto, Check Point.
- **20+ direct feeds.** Cross-referenced before any IP commits to the list.
- **Attack-attributed.** Every IP linked to an active scan, campaign, or C2.
- **Validated and scored.** Enriched and deduplicated to keep false positives down.
- **SIEM-ready format.** Standardized output your playbooks consume on day one.

01 · INTELLIGENCE

Daily IP updates.

Verified malicious IPs on a tight cadence. Cross-checked against 20+ direct feeds before they hit your stack.

02 · ENFORCEMENT

Seamless firewall sync.

Inline blocking on FortiGate, Palo Alto, and Check Point. Real-time mitigation, zero manual ingestion.

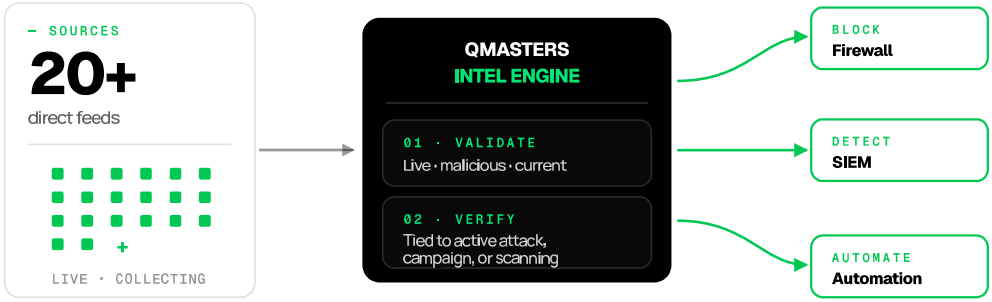
03 · RESPONSE

Playbook automation.

Standardized alerts feed your SIEM and SOAR. Faster triage. Less keyboard. Cleaner audit trail.

— HOW IT WORKS

From feed to firewall. In three steps.



SOURCES · 20+ DIRECT FEEDS ENGINE · VALIDATE / VERIFY OUTPUTS · BLOCK / DETECT / AUTOMATE

— REVIEWS ARE IN

Measured outcomes. From the field.

Government agency PUBLIC SECTOR

−30%

INBOUND MALICIOUS TRAFFIC

“ We run the IOC blacklist inline to block access in real time. Bad traffic dropped by about 30%, firewall performance is up, and we're in control. More visibility. Less noise. Safer overall.

— NETWORK OPERATIONS · GOV. AGENCY

Hightech · fintech app FIN. SERVICES

Earlier.

RECON BLOCKED BEFORE EXPLOIT WINDOWS

“ AI changed the vulnerability game. We use IOC blocking to buy time — scanning and early reconnaissance get cut at the firewall. Results land live in our firewall and SIEM. Time we didn't have before.

— APP SECURITY · FINTECH

No new appliance. Just sync.

Inline IP enforcement on the firewalls you already run. Standardized output your SIEM, SOAR, and TIP already speak.

Fortinet | Palo Alto | Check Point

SUPPORTED WAF SOLUTIONS

STIX / TAXII | CSV | JSON / REST

Get the feed running in under 24 hours.

Onboarding covers firewall integration, validation against your existing ruleset, and a tuning pass with our SOC. Ask us about a trial.

CONTACT SALES → | QMASTERS.CO

SALES
sales@qmasters.co

WEB
qmasters.co

OFFICE
Derech Begin 46, 4th floor
Tel Aviv, Israel