Intelligence to Arrests: The Business Case for Public-Benefit Cyber Defense

Deconstructing INTERPOL's Operation Ramz and the hidden infrastructure powering global cybercrime disruption.

Operation Ramz: A First-of-its-Kind Disruption in MENA

Between October 2025 and February 28, 2026, INTERPOL coordinated an unprecedented takedown of phishing, malware, and large-scale cyber scam infrastructure across 13 countries in the Middle East and North Africa.

Takeaway: Coordinated intelligence sharing moved beyond "awareness" into concrete, physical disruption of criminal syndicates.

201 Arrests	**3,867** Victims Identified
53 Servers Seized	**8,000+** Pieces of Intelligence Disseminated

Regional Execution, Localized Impact

case file

Target: Jordan

Action: Raided a fraudulent trading platform; rescued 15 human trafficking victims forced into financial fraud; arrested 2 key orchestrators.

case file

Target: Algeria

Action: Dismantled a regional Phishing-as-a-Service (PhaaS) platform; seized the central server; took 1 primary administrator into custody.

case file

Target: Morocco

Action: Seized hardware containing compromised banking databases and custom phishing software; initiated judicial proceedings against 3 suspects.

case file

Targets: Qatar & Oman

Action: Identified and secured compromised edge nodes (CPE) acting as proxies; disabled vulnerable residential storage servers before exploitation.

The Unseen Intelligence Partner

> “During **Operation Ramz**, INTERPOL worked **closely with its partners, Group-IB, Kaspersky,** the Shadowserver Foundation, Team Cymru and TrendAI to illegal cyber activities and identify malicious servers.”
>
> — INTERPOL Official Release, May 18, 2026

Behind the synchronized physical raids sits a highly restricted Traffic Light Protocol (TLP:RED) data-sharing framework. **Shadowserver** Shadowserver provided the actionable threat telemetry that allowed law enforcement to map the infrastructure without tipping off the syndicates.	Behind the synchronized physical raids sits a highly restricted Traffic Light Protocol (TLP:RED) data-sharing framework. **Shadowserver** Shadowserver provided the actionable threat telemetry that allowed law enforcement to map the infrastructure without tipping off the syndicates.

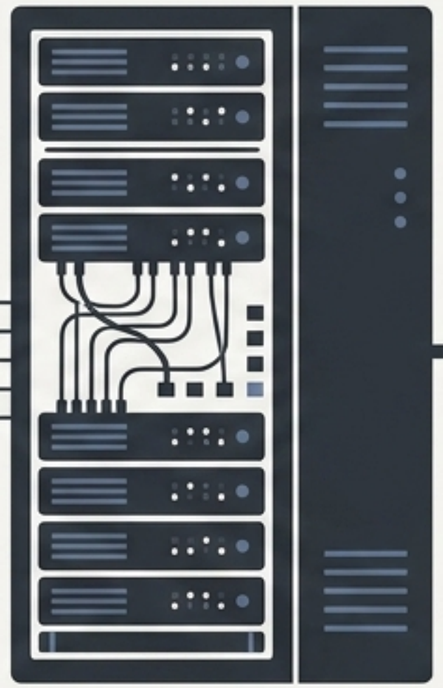
The Global Collection Engine

IPv4 Scanning: 3.7 Billion addresses scanned 148 times daily.

IPv6 Scanning: 1.07 Billion addresses scanned 77 times daily.

Sinkholing: 4 Million+ infected IP addresses redirected daily across 400 malware families.

Malware Processing: 1.115 Million unique malware samples ingested and sandboxed daily.



The Core: A data-center footprint of over 1,300 servers and endpoints distributed across more than 80 countries.

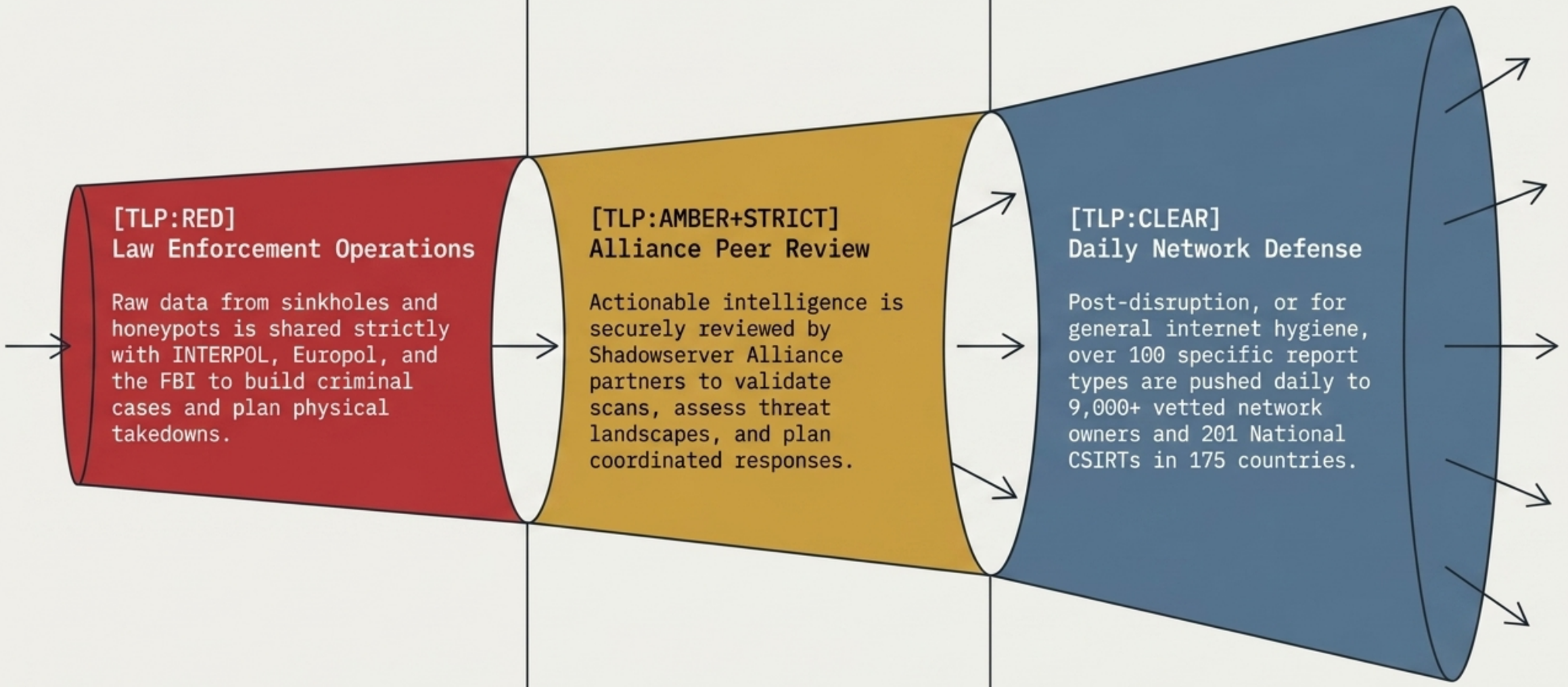
Outputs: Daily delivery of over 100 distinct report types.

The Trust Model: Why Law Enforcement Relies on Non-Profits

Dimension	Commercial Threat Intel	Shadowserver (Public Benefit)
Primary Motive	Licensing Revenue / Product Sales	Public Benefit / Open Internet Security
Data Access	Paywalled / Client-restricted	Free to vetted network owners and 201 National CSIRTs
Law Enforcement Role	Marketing-driven event participation	Decades of quiet, TLP:RED sustained case support
Data Utilization	Monetized indicators	Never sells victim data; dedicated to remediation

Conclusion: Shadowserver acts as a trusted, neutral intermediary. Sensitive information moves quickly and accurately to those who can act, without the friction of commercial licensing.

The Intelligence Pipeline: From Sinkhole to Dashboard



Two Decades of Unbroken Disruption

2004

Founded as a volunteer watchdog group.

2016-2019

Operation Avalanche: Seized 2.4 million domains; intercepted 2.5M Andromeda botnet connections daily.

August 2023

Qakbot: Processed seized databases containing over 700,000 discrete infections across 230 countries.

May 2024

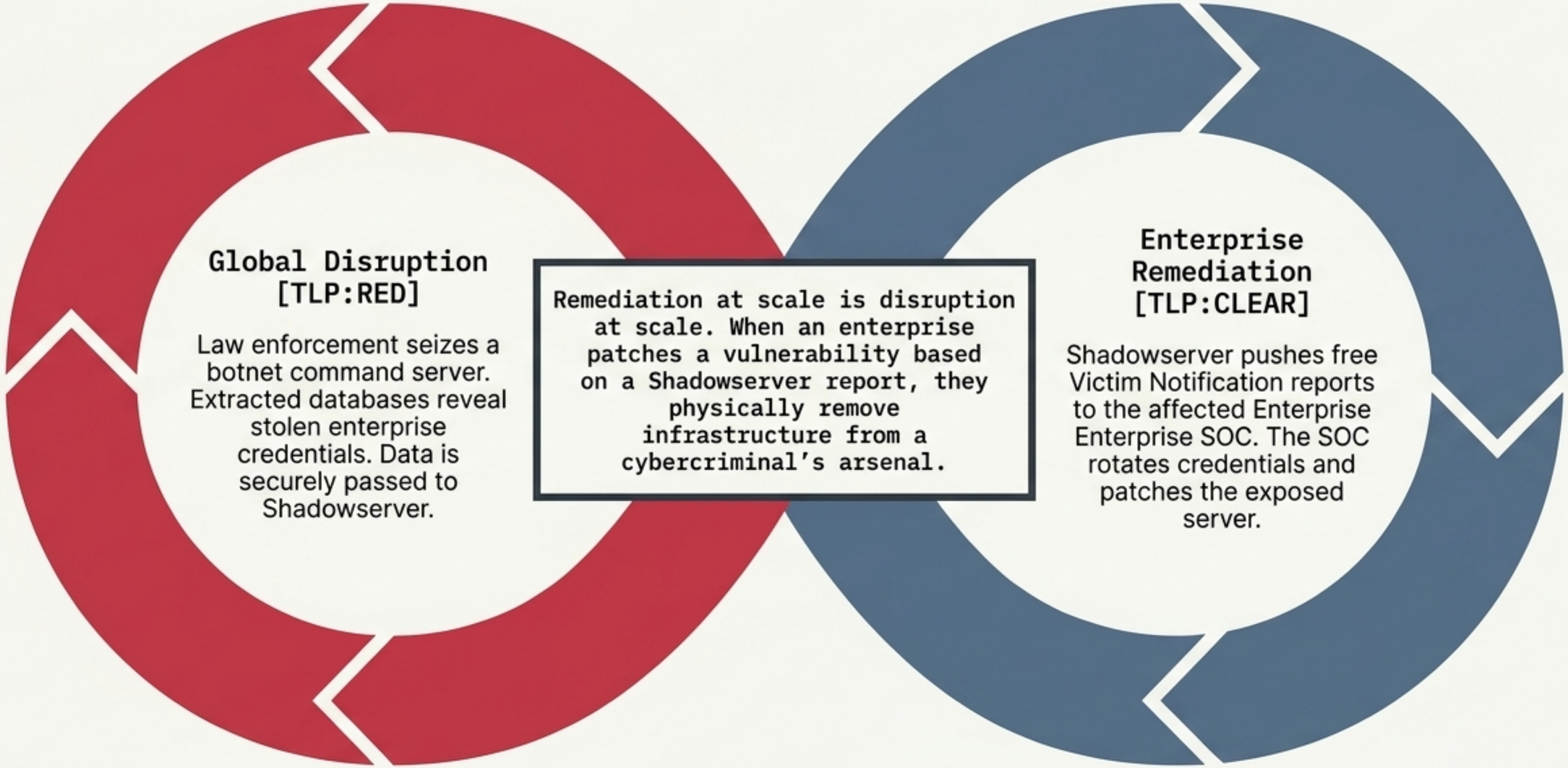
Operation Endgame: Disrupted IcedID, SystemBC, Pikabot, Smokeloader, and Bumblebee, pushing data to over 10,000 network owners.

2026

Operation Ramz: The first large-scale MENA takedown.

Shadowserver is the operational connective tissue in the technical subgroup of essentially every major international cybercrime disruption of the modern era.

The Symbiosis of Cyber Defense



Turning “Outside-In” Telemetry Into SOC Action

Threat Vector to Remediation

Feed	Threat	Action
Open SNMP Report	Amplification DDoS via OIDs	Deploy iACLs at network edge to restrict access.
Malware URL Report	C2 callbacks / Log4j payloads	Update web gateways to block outbound connections.
Compromised Website Report	Persistent webshells on FortiWeb/Ivanti	Isolate host, preserve logs, force password resets.
Special Outbreak Reports	Rhadamanthys Infostealer databases	Activate emergency IR, audit Active Directory, global credential rotation.

Takeaway: This is exactly what threat actors see when scanning your external attack surface.

The Upstream Advantage: Operation Endgame (Season 3)

The Event: On November 13, 2025, the Rhadamanthys infostealer was taken down.

The Raw Data Scale

86,214,924
information stealing events recorded.

525,303
unique IP addresses across 226 countries.

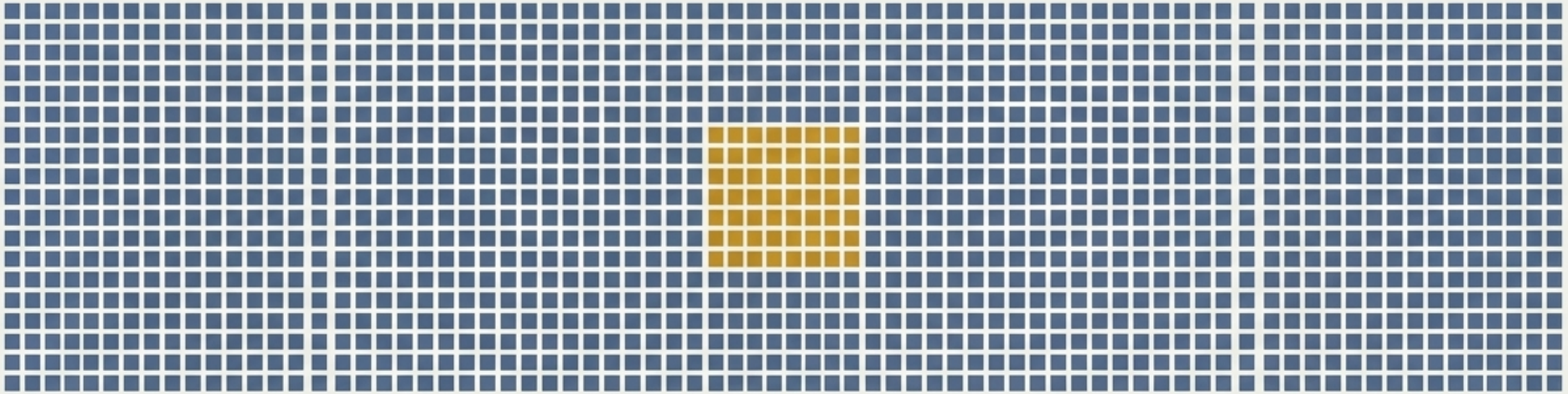
The Defensive Advantage

Shadowserver processed the seized law enforcement databases and delivered targeted Special Reports to defenders.

Because stolen credentials operate on a

“timer” before password resets occur, subscribers received precise, device-level data (URLs, stolen credentials) allowing them to isolate hosts before secondary ransomware attacks could be launched.

The Free-Rider Crisis in Global Cyber Defense



Fewer than 1% of the 9,000+ organizations and 201 National CSIRTs that rely on Shadowserver data financially contribute to its operation.

The internet’s immune system is being sustained by a fraction of its beneficiaries. Most organizations spend heavily on internal, inward-facing tools, but budget zero dollars for the public-benefit infrastructure that actively disrupts the adversaries targeting them.

The Economics of Internet-Scale Defense

The Burn Rate

$400,000 / month

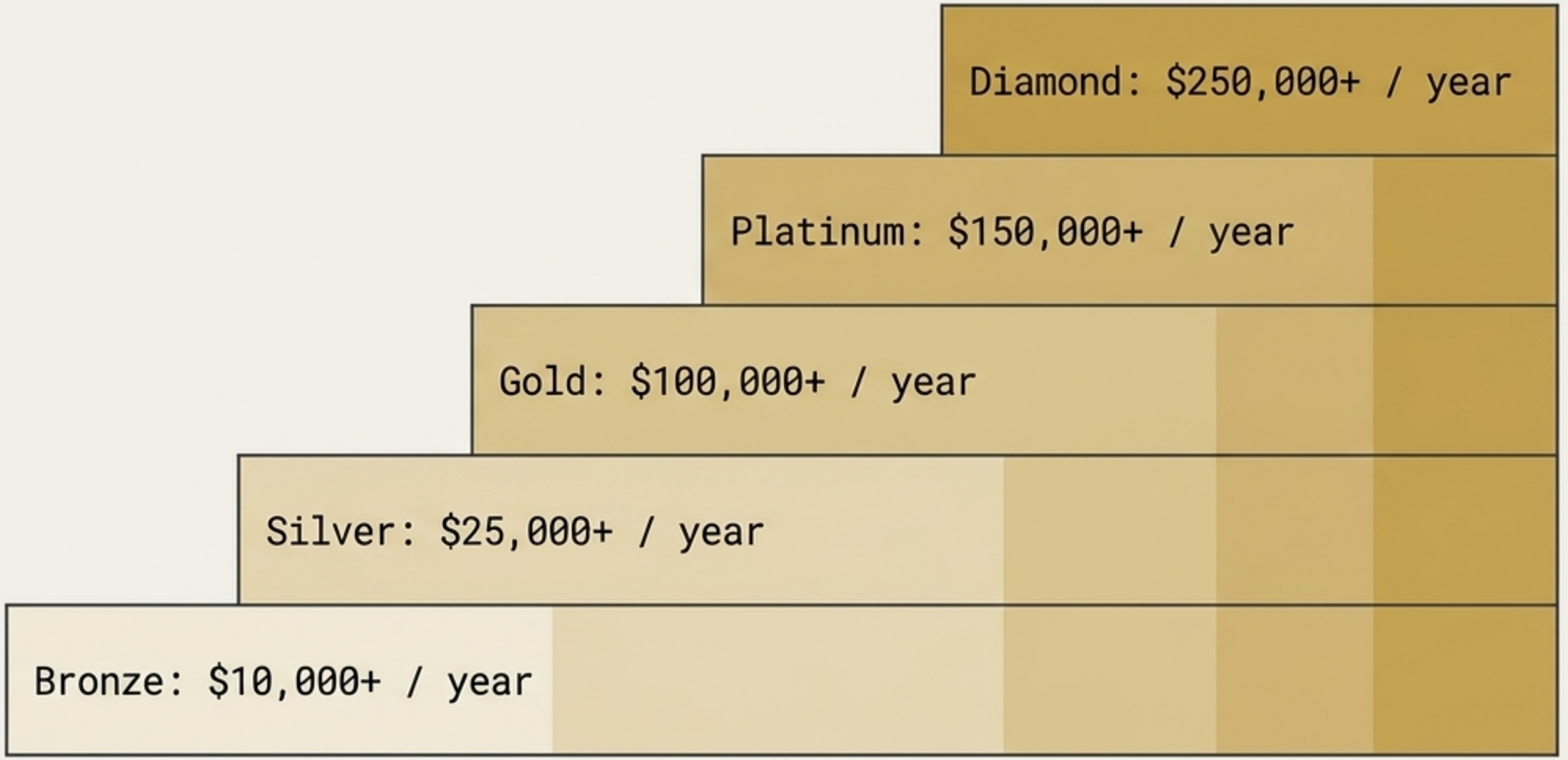
This covers the data center footprint housing over 1,300 servers and endpoints, massive bandwidth requirements, and expert engineering talent.

The 2020 Near-Miss	For 15 years, Shadowserver was heavily bankrolled by a single corporate sponsor (Cisco). In 2020, that funding was suddenly withdrawn, bringing the internet's premier early warning system within weeks of going permanently dark.

The Lesson: Neutral, public-benefit infrastructure cannot survive on ad-hoc charity or single-vendor reliance. It requires a distributed, strategic funding model.

The Shadowserver Alliance: A Framework for Strategic Reinvestment

Launched in October 2022, the Alliance provides a resilient, multi-stakeholder funding model that preserves foundation neutrality.



Current Public Partners:

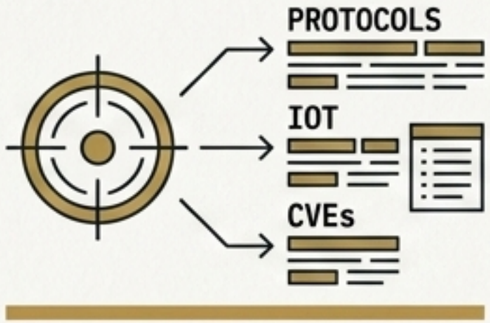
Mastercard, Akamai, Team Cymru, watchTowr, Red Hat, National CSIRTs.

Note: Prominent tech giants are noticeably absent. There is room at the table.

ROI: What Alliance Funding Physically Buys

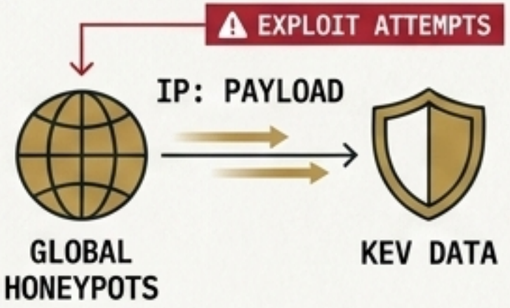
Sponsor-Driven Prioritization

Help determine global scanning and sinkholing targets. Direct the engine toward the protocols, IoT profiles, or CVEs most relevant to your industry.



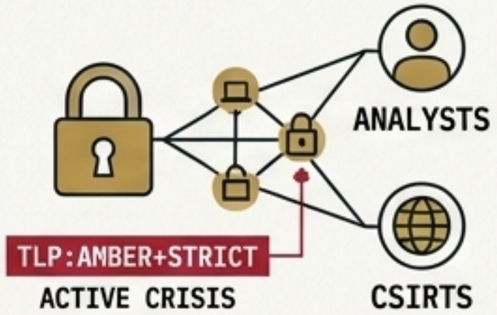
Upstream Threat Telemetry

Gain direct access to global honeypot and Known Exploited Vulnerabilities (KEV) data, tracking exploit attempts at the IP and payload level before they hit public registries.



Secure Crisis Channels

Access to monitored **TLP:AMBER+STRICT** workspaces to share intelligence directly with analysts and national CSIRTs during active global crises.



Strategic Governance

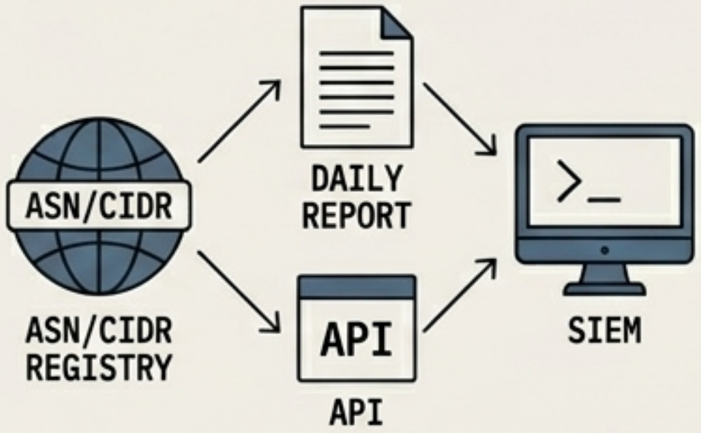
Diamond tier sponsors gain Class C corporate seats on the Governance Board of Trustees, actively steering the foundation's global missions.

The C-Suite Mandate: From Passive Benefit to Active Defense

Step 1: This Week (Operational)

Action: Register your ASN/CIDR ranges for free daily reports and plug the REST API into your SIEM.

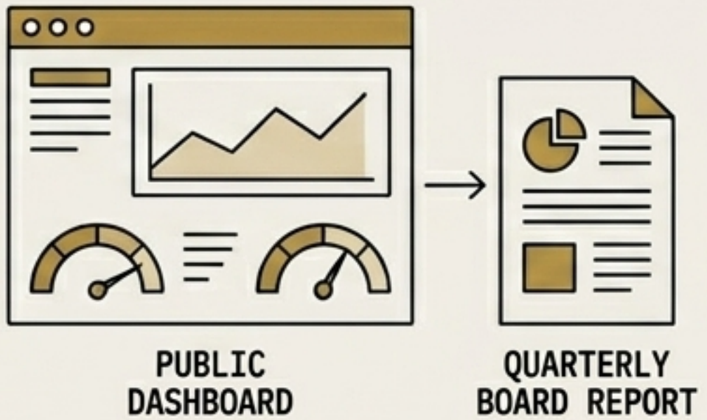
Benchmark: Remediate Shadowserver-flagged exposures within the same SLA as Tier-1 internal alerts.



Step 2: This Quarter (Governance)

Action: Wire the Shadowserver public Dashboard into your quarterly Board reporting pack.

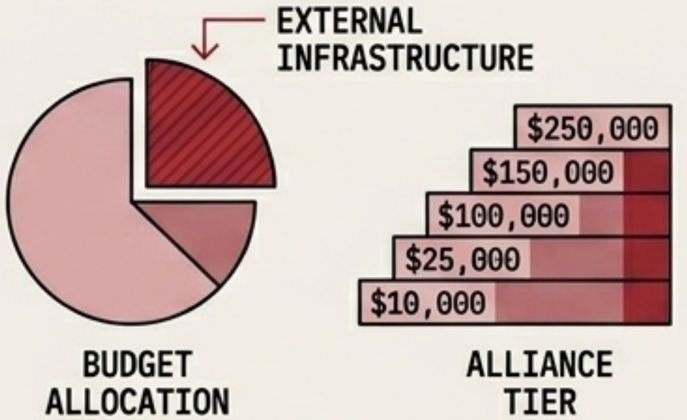
Benchmark: Achieve zero net-new high-severity exposures across two consecutive quarters.



Step 3: This Budget Cycle (Strategic)

Action: Fund the public-benefit infrastructure. Join the Shadowserver Alliance at the appropriate tier.

Benchmark: Redirect a fraction of inward-facing security spend toward the external infrastructure that physically dismantles threat actors.



The Cost of Inaction

“Cybercrime is a borderless, multi-billion-dollar enterprise. We cannot defend against it solely by building taller walls around individual networks. Operation Ramz proves that actionable intelligence, combined with trusted public-private partnerships, results in actual arrests and dismantled infrastructure.”

The organizations most concerned about cybercrime must fund the non-profit engine that actually disrupts it.

Call to Action: Visit shadowserver.org/partner/ to invest in action.