

CYBERTOTAL GLOBAL THREAT INTELLIGENCE PLATFORM

Reduce Costs & Speed Up SecOps with Automated Threat Intelligence Investigations and Seamless Collaboration

WHAT IS CYBERTOTAL?

CyberTotal is a global cyber threat intelligence platform that collects, integrates, and manages intelligence gathered from global feeds as well as CyCraft MDR intelligence, global intel initiatives, your intel, and manages intrusion sets for collaboration across SecOps and Threat Intelligence Teams with one-click investigations and graph investigations across all global threat intel, including API access for easy integration into your SecOps and threat intel practices.

CYBER DEFENSE MATRIX

	Identify	Protect	Detect	Respond	Recover
Devices					
Applications					
Networks					
Data					
Users					

CRITICAL DELIVERABLES

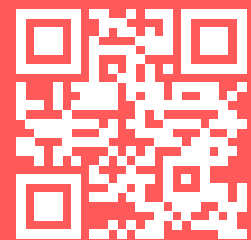
- > **A SaaS web interface and a set of APIs** (including STIX) that can be used to analyze CyberTotal's threat intel for triage, validation, and investigation as well as creating and maintaining intrusion sets to follow and disseminate pertinent threat intel org-wide.
- > **The threat intel you need for actionable investigations:** threat data type, severity score, confidence score, related intel, recent activity, as well as searchable analyses by industry, APT, threat type, and country
- > **A daily-vetted block list** that can be used to block and hunt across your network and endpoints.
- > **Graph investigations** to reveal hidden connections in the threat intel landscape for attribution, severity analysis, and more
- > **Intrusion sets** for your collected pertinent threat data and a proprietary Precog feature that monitors changes in the threat landscape so you can track threats and actors and know what they do before it affects your org

“ We literally have the full support from the CyCraft team. They solve issues promptly. Sometimes, we’ve even asked for assistance to solve other vendors’ issues, and they’ve always been positive and helpful.

Associate Executive VP,
Security and Risk Management
Banking, 30B+

READY FOR A
DEMO?

Visit [CyCraft.com](https://www.cycraft.com)



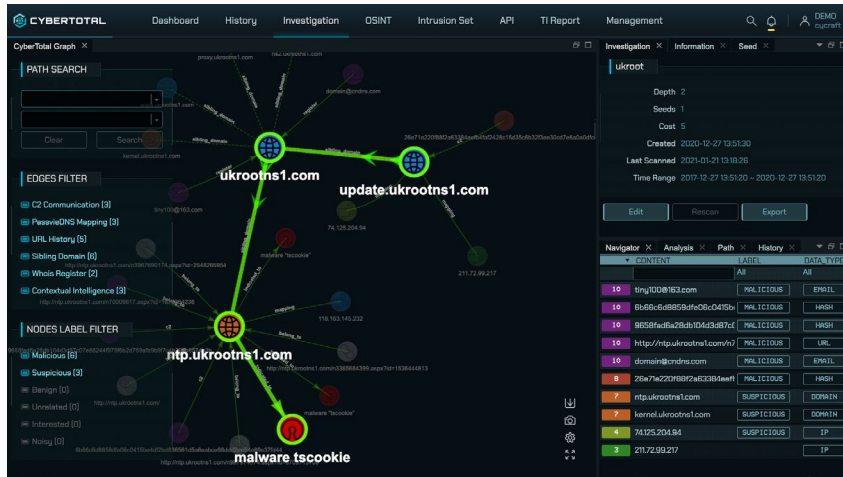
About CyCraft

CyCraft provides organizations worldwide with the innovative AI-driven technology necessary to stop cyber threats in the 2020s. CyCraft technology is uniquely designed to detect the latest trends in malicious behavior, automate investigations, and auto-triage alerts, allowing CyCraft customers to detect, track, contain, and eradicate threats in near real-time.

engage@cycraft.com

HOW DOES IT WORK?

CyberTotal ingests, vets, and normalizes threat intelligence data from global sources, CyCraft MDR, and intelligence sharing initiatives into one cohesive data set that is updated daily for querying and graph-based investigation. CyberTotal provides automated, proprietary backend analyses of all threat intel to generate confidence and severity scores for each indicator and to maintain the cleanliness and accuracy of the dataset, which is accessible by API as well.



EASE OF USE

- > **Available as SaaS** with an API for integration via JSON or STIX/TAXII
- > **One-click searches** across domain, IP, URL, file hash or name, CVE with JSON data export of STIX data
- > **Hands-free:** Auto monitoring of intrusion sets for changes in the threat landscape that can affect your org

WHAT SETS CYCRAFT APART?

- > CyCraft's experience in Taiwan and Japan provides valuable intelligence and insight on threats targeting the region, their attack behavior, and their past and potential targets.
- > CyberTotal's API allows fast, flexible deployment as well as ease of integration into your stack.
- > Talk to a person and get immediate answers. CyCraft Support has built a reputation for their fast response times to immediately relieve any friction in your investigation process.

CYCRAFT MEETS GDPR & JAPAN PRIVACY LAWS

- > We collect far less data than Windows
- > We don't collect payment data, presentation files, messaging/email contents, or anything that would violate GDPR/Privacy laws
- > In fact, we aid in GDPR/Privacy law compliance:
 - > We stop attackers from stealing your data
 - > We enable quicker reporting to meet compliance

WHY IT MATTERS

URGENT PAIN RESOLVED

- > Collate and normalize all threat intelligence from multiple sources into a single base for collaboration across SecOps and threat intelligence teams
- > See beyond the standard feeds by understanding associations and changes in the threat intelligence space, and monitor changes in threat intel that could affect your org
- > Leverage CyberTotal's API to automate SecOps workflow including validation, triage, investigation, and enrichment—complete with clear and accurate scores of severity and confidence for each indicator

BENEFITS TO CUSTOMERS + PARTNERS

- > Single source of truth for threat intelligence across your organization complete with full text and indicator search.
- > Create, maintain, disseminate, monitor, and integrate intrusion sets for threats across geographically dispersed orgs.
- > **Block the Past**
Detect and block inbound and outbound known threats (up to 80% of the attacks orgs face today), which not only saves orgs from these attacks but also reduces bandwidth usage and the follow-on investigative workflow that those attacks bring.
- > **Hunt the Present**
Proactively hunt down known and highly suspicious threats by hunting on each endpoint. Stop threats before they become tickets in the SOC, reduce workload, and remove known and highly suspicious artifacts before they do damage.
- > **Know the Future**
CyberTotal's Precog automatically monitors threat groups and other sets of indicators for new connections in the threat landscape. Proactively identify and block threats before they are registered on competitors' radars, keeping you more secure than other products.