

CyCraft

 CYCRAFT



Who We Are

- Established in 2017
 - HQ: Taipei, Taiwan (100+ Employees)
 - Market Position: AI-Driven Threat Exposure Management Services encompassing Identity, EDR, EASM, MDR, CA, CTI and IR.
 - Office: Taiwan, Japan, Singapore.
 - Customer Base: Over 300, including Government, Financial, High Tech, Telecom, Education, etc.
-



Award & Recognition



**MITRE ATT&CK APT29 Rated
Highest in Threat Detection &
Lowest in Telemetry.**



**Awarded Interop 2020 Best of
Show Grand Prize in Security
Category.**



**Awarded Cybersecurity
Excellence Awards from 2020
to 2022.**



**Momentum CyberScape
Inclusion: EDR and Security
Analytics.**



**Awarded Taiwan's leading
startup brand NEXT BIG in
2023.**



**The only Taiwanese
cybersecurity company
awarded in 2023.**

CyCraft is the only Cybersecurity Corporation Selected by Gartner and IDS in Taiwan



Frost & Sullivan (2019)

《Reducing Digital Forensic Investigation Time with CyCraft's CyCarrier AIR Platform》

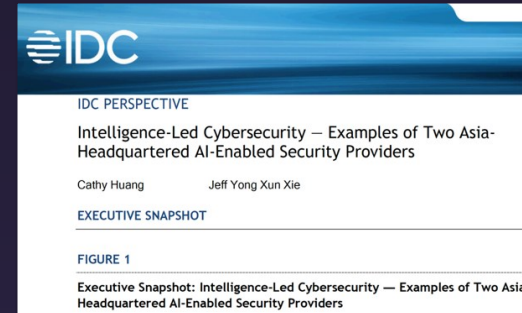
The Investigation shows CyCraft AI Technology can reduce 99% of forensic time and 95% of labor cost



Gartner (2021, 2022)

《Market Guide for AI Startups, Greater China》

Selected as the sole representative enterprise case study by the cybersecurity company.



IDC Perspective (2021)

《Intelligence-Led Cybersecurity — Examples of Two Asia-Headquartered AI-Enabled Security Providers》

Authoritative institutions Analyze CyCraft technical advantage and market validation



Gartner (2022, 2023)

《Emerging Tech: Adoption Growth Insights for Managed Detection and Response》

Top Research Institution recognize CyCraft as a representative of MDR service provider

CyCraft AI + Cyber Received Recognition at the Prestigious International Conference

The screenshot shows the Black Hat USA 2023 website. At the top, the Black Hat logo is on the left, and a 'REGISTER NOW' button is on the right. Below the logo, the text 'black hat USA 2023' is displayed. To the right of the logo, the dates 'AUGUST 5-10, 2023' and the location 'MANDALAY BAY / LAS VEGAS + VIRTUAL' are shown. A navigation bar contains links: ATTEND, TRAININGS, BRIEFINGS, ARSENAL, FEATURES, SCHEDULE, BUSINESS HALL, SPONSORS, and PROPOSALS. Below the navigation bar, a sidebar on the left has buttons for 'ALL SESSIONS' and 'SPEAKERS'. The main content area displays the session 'IRonMAN: InterpRetable Incident Inspector Based ON Large-Scale Language Model and Association miNing'. The session is presented by Sian-Yao Huang (Data Scientist, CyCraft Technology), Cheng-Lin Yang (Senior Data Science Architect, CyCraft Technology), and Chung-Kuan Chen (Security Research Director, CyCraft Technology). The date is Thursday, August 10, 10:20am-11:00am (Jasmine AE, Level 3). The format is 40-Minute Briefings, and the track is AI, ML, & Data Science. The session description discusses contextual incident investigation and the use of LLMs for security incidents. The conclusion states that the method merges traditional incident response strategies with advanced data science techniques.

black hat
USA 2023

REGISTER NOW

AUGUST 5-10, 2023
MANDALAY BAY / LAS VEGAS
+ VIRTUAL

ATTEND TRAININGS BRIEFINGS ARSENAL FEATURES SCHEDULE BUSINESS HALL SPONSORS PROPOSALS

All times are Pacific Time (GMT/UTC -7h)

ALL SESSIONS
SPEAKERS

IRonMAN: InterpRetable Incident Inspector Based ON Large-Scale Language Model and Association miNing

Sian-Yao Huang | Data Scientist, CyCraft Technology
Cheng-Lin Yang | Senior Data Science Architect, CyCraft Technology
Chung-Kuan Chen | Security Research Director, CyCraft Technology
Date: Thursday, August 10 | 10:20am-11:00am (Jasmine AE, Level 3)
Format: 40-Minute Briefings
Track: AI, ML, & Data Science

Contextual incident investigation and incident similarity assessment are crucial components of modern IR and proactive threat hunting strategies. However, current automated systems often rely on pattern- and heuristic-based approaches due to their reliability and competitive performance. These approaches lack the ability to correlate events with contextual information and are susceptible to evasion through slight variations, resulting in false alerts. Recent advances in large-scale language models (LLMs) have shown promising results in language representation. By adopting LLM embedding strategies for security incidents, contextual relationships and similarities of events can be modeled, leading to a reduced false alert rate. However, LLM-based approaches often lack interpretability, which is essential for security analysts.

In this work, we propose the first explainable LLM-based incident inspector. We combine a large-scale language embedding model with a frequent association algorithm to extract significant tokens, providing strong interpretability for incident similarity in feature space representation. Moreover, the contextual comprehension capabilities of the LLM ensure robustness against input variations. We demonstrate the practicality of our method in real-world incidents by applying it to our global visibility platform (200M+ events per day). The significant tokens generated by our model clearly identify the reasons why incidents are believed to stem from the same APT groups. Additionally, compare the results generated by our method to feedback from security analysts and thus provide different analytical perspectives for incident analysis.

In conclusion, our method seamlessly merges traditional incident response strategies with advanced data science techniques, enriching the information available to security analysts. Moreover, our method can be applied to incident similarity, attribution and archiving. Our work, along with the comparative analysis, serves as a catalyst for the development of even more robust and interpretable methods for incident analysis.

Black hat 2023

《 IRonMAN: InterpRetable incident Inspector Based ON Large-Scale Language Model and Association miNing 》

The only Taiwanese team to present in 2023 received recognition for leveraging LLMs for cybersecurity incident investigation and correlation analysis.

Joining International Organizations - Committed to Establishing Standards and Sharing Intelligence



FIRST (Forum of Incident Response and Security Teams)



日本シーサート協議会
(Nippon CSIRT Association, NCA)



NO MORE RANSOM

No More Ransom Org.



SEMI TAIWAN



Taiwan National Defense Industry Development Association

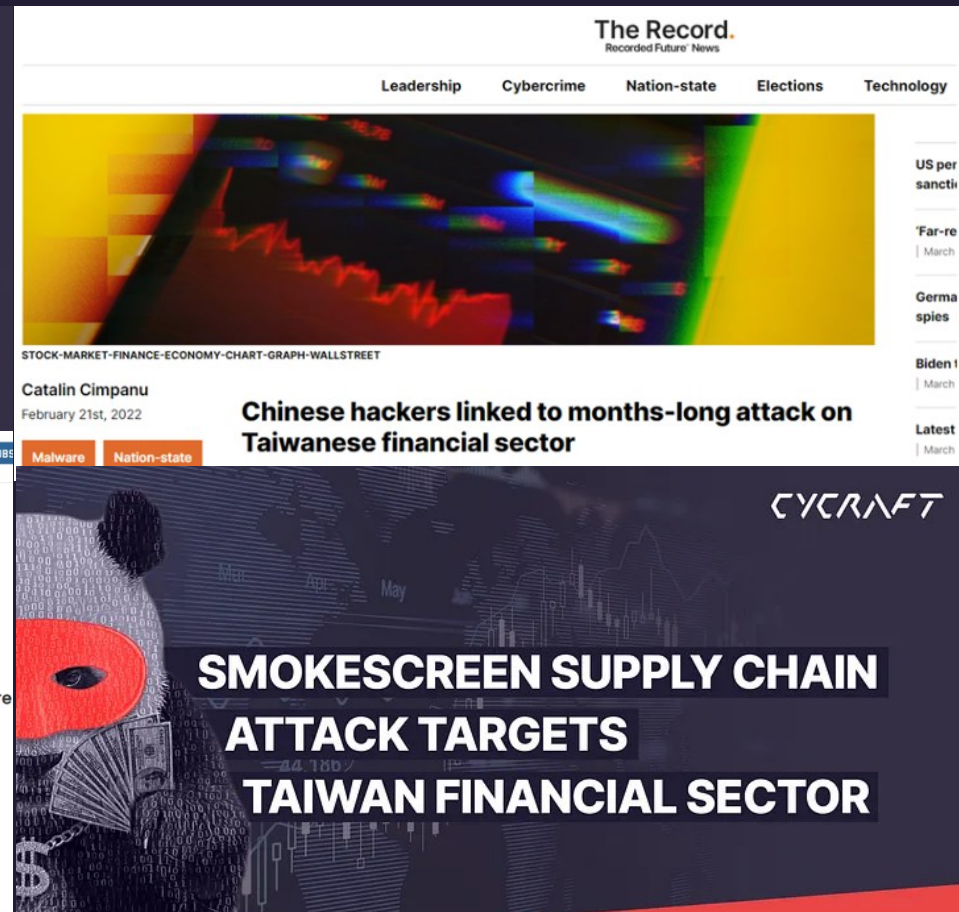
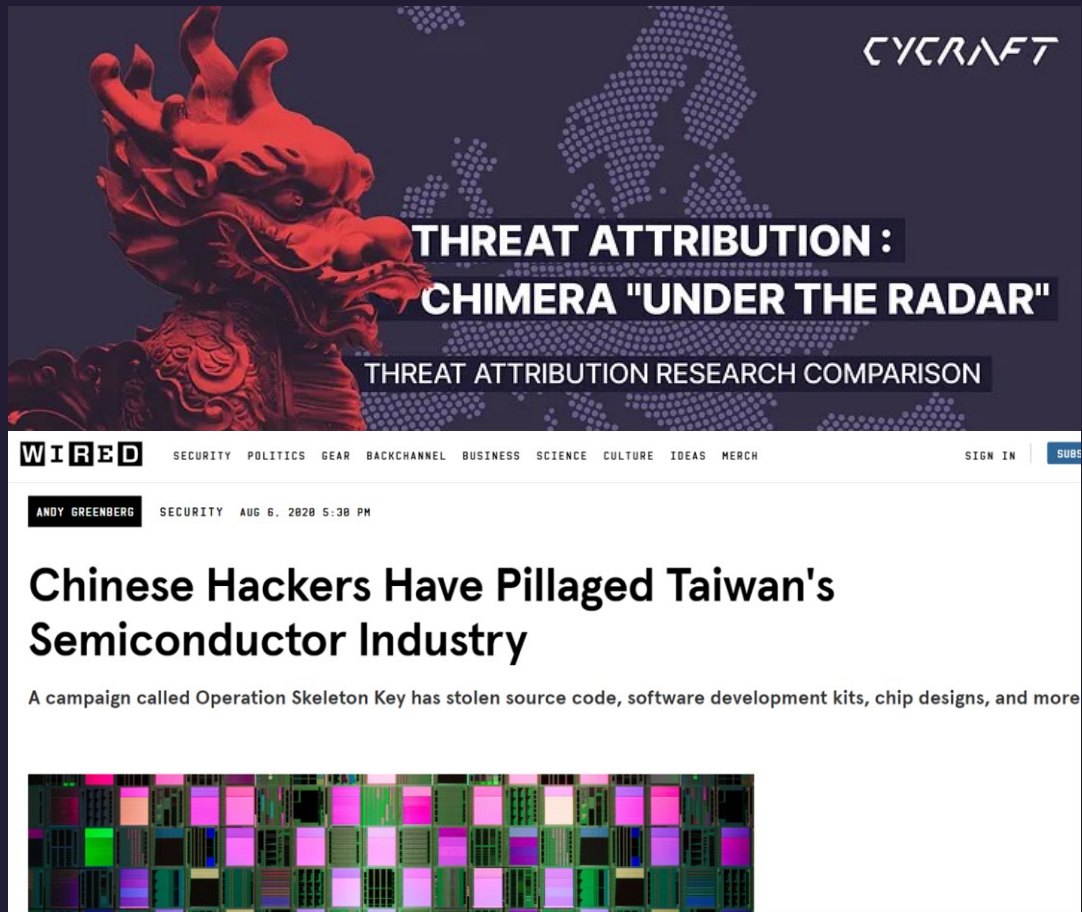


National Center for Cyber Security Technology



MIH Consortium

Unveiling Nation-State Attacks: Tactics Targeting Semiconductor and Financial Industries



Testimonial Customers Recognizes us as a 5-Star Performer on G2

"CyCraft's services provide customers with uninterrupted and continuous monitoring of serious network threats. Automated attack behavior investigation and root cause analysis have greatly improved their high-quality service. They present fewer false positives than other cybersecurity solutions. CyCraft can verify the accuracy of the warning messages of other network security products."

Deputy Head of Information Security | Bank SinoPac
Taiwan

★★★★★ May 18, 2022

"Our CyCraft Fantastic Experience"

What do you like best?

1. We—as a bank—put a great emphasis on day-to-day business operations. As a result, slowing down the computers will be a fatal flaw for us when we select a cybersecurity product. And that's why we choose CyCraft. CyCraft doesn't greatly affect the performance of computers.

2. The most impressive feature is FAST. An incident once occurred, and it took about half a day for CyCraft to inspect 4,000+ endpoints.

3. CyCraft alerts accurately, so sometimes we will ask CyCraft to assist in investigating, checking if there is a false positive from other cybersecurity suppliers.

<https://cycraft.com/customers/>

<https://www.g2.com/products/cycraft-mdr/reviews/cycraft-mdr-review-6631803>

Customers Recognizes us as a 5-Star Performer on Gartner Peer Insights

5.0 ★★★★★ May 18, 2022

No Alert Fatigue, Well Done!

Reviewer Function: IT Security and Risk Management

Company Size: 30B + USD

Industry: Banking Industry

Thanks to CyCraft, we finally get rid of alert fatigue. As the Finance sector is very easy to become hackers' top target, we adopted ...

5.0 ★★★★★ Apr 13, 2022

Outstanding MDR solution saves us a ton of time!

Reviewer Function: Other

Company Size: 50M - 250M USD

Industry: Transportation Industry

The experience with CyCraft has been fantastic. When we conduct a red team/blue team assessment, CyCraft always reports ...

5.0 ★★★★★ Feb 6, 2022

CyCraft caught everything the top-tier red team threw at it

Reviewer Function: Other

Company Size: Gov't/PS/ED 5,000 - 50,000

Employees

Industry: Government Industry

By AI-driven forensic investigation and 24*7 detection & response, CyCraft AIR helps us save a ton of time on endpoint ...

5.0 ★★★★★ Apr 15, 2021

10/10 would recommend for EDR meets automated MDR!

Reviewer Function: IT Security and Risk Management

Company Size: 3B - 10B USD

Industry: Finance (non-banking) Industry

10/10! From deployment to operations this had been the EDR solution that we truly needed--It can be on prem as well as in ...



300+

Trusted by over 300 customers spanning private global enterprises and public sectors.



> 96%

Five-year consecutive outstanding Renewal Rate.



500,000+

Real-time monitoring of endpoints.



Gartner Peer
Insights



Customers rate the MDR solution with a 5-star rating



 **XCOCKPIT**

Autonomous Threat Exposure Management Platform

Risk Identification And Team Performance Metrics

Overall risk Assessment and cybersecurity service team performance metrics (MTTI/MTTD)

AI-powered Virtual Analyst

Integrate AI automated analysis, incident explanation, Decrease the cost of labor force, increase the efficiency



Comprehensive Threat Monitoring

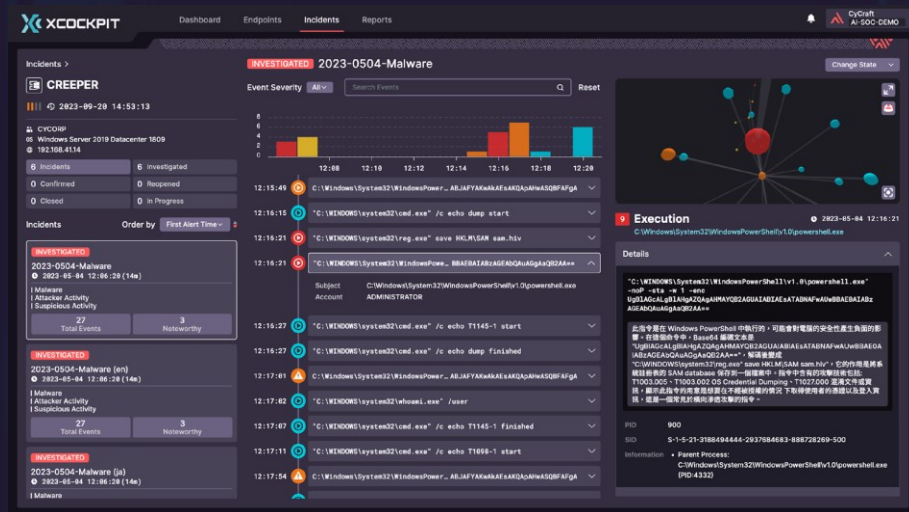
EDR endpoint threat monitor + AD account monitor + EASM exposure monitor

Visualized Cybersecurity Dashboard

Fast and Simple interface, various operational report , incident real-time analysis and correlation analysis report

XCockpit Endpoint

Security Posture Management



Threat Monitor

Real-time



**Incident Detection
(MTTD)**

3 mins



**Incident Investigation
(MTTI)**

15 mins

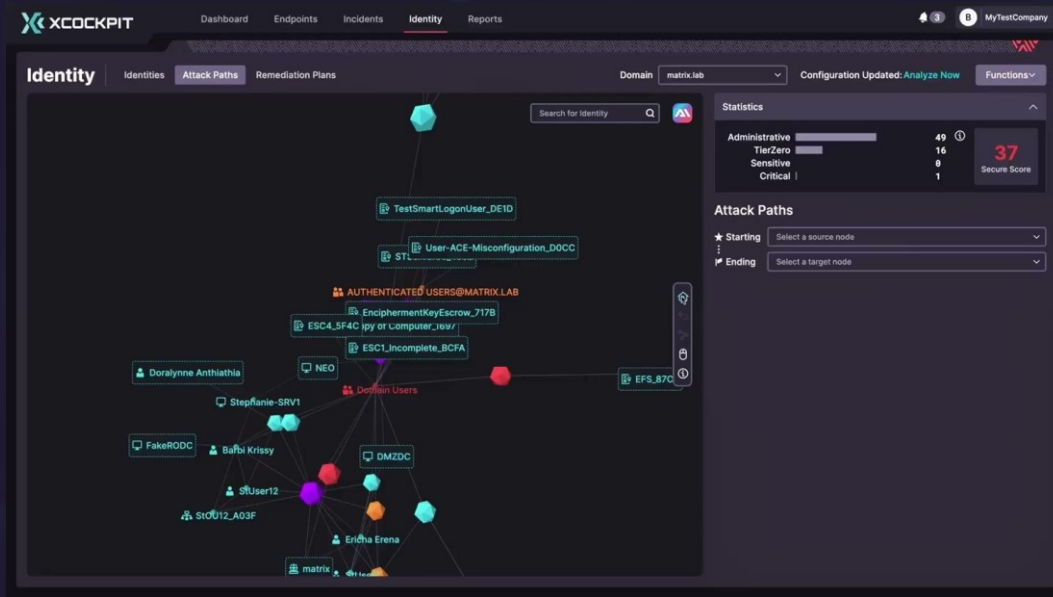
- **Enhance Analyst Productivity**
Pioneer AI security assistant, provide automatic incident analysis and explanations, to swiftly organize cybersecurity incidents

- **Expand Team Capability**
From automated alerts and correlation analysis to automatic filing and ticket creation, enhance overall team efficiency and productivity

- **Streamline Workflow Processes**
Offer API-driven integration with SOC/SIEM ticket system, streamline the process and enhance overall team efficiency

XCockpit Identity

Identity Security Posture Management



- **Account Impact Analysis**

Employ AI-driven simulations to analyze the impact of account breaches, foreseeing hackers' attack paths and uncovering enterprise privilege perimeter.

- **Threat Detection and Early Warning**

Monitor anomalous activities of privileged accounts, swiftly identifying various AD account attack techniques and detecting pre-attack indicators.

- **Quantified Identity Management**

Evaluate the exposure of identity attack surfaces and quantify enterprise Identity Security Indicators, offering a comprehensive overview of security posture.

XCockpit EASM

External Attack Surface Management

The screenshot displays the XCockpit EASM interface. The top navigation bar includes 'Dashboard', 'Endpoints', 'Incidents', 'Identity', 'EASM', and 'Reports'. The 'EASM' section is active, showing a list of assets for the domain 'apple-tech.com'. The assets table has columns for Risk, Asset, Type, Information, Last Seen, Status, and Tags. Below the assets table, there is a section for 'elearning.apple-tech.com - Events' with columns for Severity, Event Time, Identity, Edge Type, and Category.

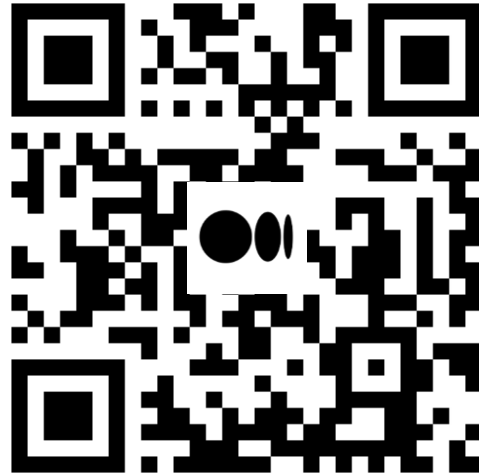
Risk	Asset	Type	Information	Last Seen	Status	Tags
100	2017survey.apple-tech.com	FQDN	https://2017survey.apple-tech.com/survey...	2023-08-30 02:14	Unreachable	LEAKED INTRANET
100	elearning.apple-tech.com	FQDN	https://elearning.apple-tech.com/clicms/unl...	2023-08-30 02:14	Unreachable	LEAKED INTRANET
100	epmd.apple-tech.com	FQDN	https://epmd.apple-tech.com/	2023-08-30 02:14	Unreachable	LEAKED INTRANET
100	eportal.apple-tech.com	FQDN	https://eportal.apple-tech.com/irj/portal	2023-08-30 02:14	Unreachable	LEAKED INTRANET
100	128.233.68.195	IP	hostname: NA, windows 10 Enterprise x64	2023-08-30 02:14	Unreachable	COMPROMISED
100	fex.apple-tech.com	FQDN	https://fex.apple-tech.com/LoginWebUser.a...	2023-08-30 02:14	Unreachable	LEAKED INTRANET
100	healthy.apple-tech.com	FQDN	https://healthy.apple-tech.com/nws	2023-08-30 02:14	Unreachable	LEAKED INTRANET
100	sso3.apple-tech.com	FQDN	https://sso3.apple-tech.com/	2023-08-30 02:14	Unreachable	LEAKED INTRANET

Severity	Event Time	Identity	Edge Type	Category
10	2023-08-30 2:14	Surface	Compromised Endpoint	Device
10	2023-08-30 2:14	apple-tech02797	Compromised Credentials	User

- **Automatically discover exploitable assets to accelerate mean time to resolution**
Identify all assets, devices, services, credentials, and resources exposed to external threats on a daily basis. Expand the coverage of scanning and monitoring to detect potential entry points that hackers might leverage proactively.
- **Start from a small breach to meaningful insights**
Ensure real-time access to the most current vulnerability data and exploitation methods. Triage and prioritize external risks into five main domains: user, endpoint, network, data, and applications. Enable risk visibility and control through robust process management.
- **Continuously manage cyber threat exposure to benchmark the security investment**
Scan and inventory external vulnerabilities in just 30 minutes, enabling the cybersecurity team to promptly verify the enterprise's security posture.



CyCraft | Website



CyCraft | Medium



CyCraft | Facebook

An abstract graphic on the left side of the slide. It consists of several overlapping geometric shapes: a large dark blue triangle pointing right, a smaller orange triangle pointing left, and a white outline of a right-pointing chevron. The background of the entire slide is a solid coral color.

Thank You