Building cyber resilience into SEMI supply chains

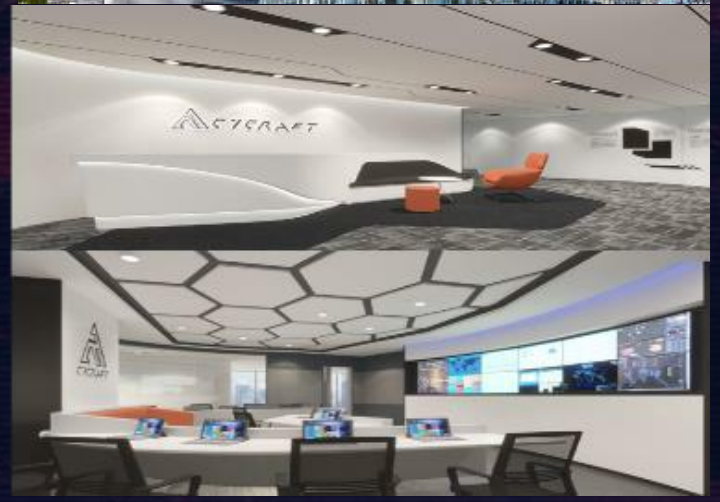
Peikan Tsung

CyCraft Technology Corporation, Co-Founder

Hacks in Taiwan Committee

SEMI Taiwan Cybersecurity Committee

CyCraft develops world's first AI autonomous platform for endpoint and identity security



- Established : July, 2017
- Headquarter : Taipei, Taiwan (100 Employees)
- Product : World's 1st Generative AI SOC Automation platform
- Office: Taiwan and Japan
- Customers : Over 200, including Government, Financial, High Tech
- Leadership : Founded by 3-peat serial entrepreneurs Pioneered discovery of China APTs *Chimera & Cache Panda* https://attack.mitre.org/groups/G0114/

天下雜誌 訂閱天下

天下晨間新聞 ‣ 那斯達克跌光今年漲幅，就因鮑威爾沒給承諾？

Chimera APT Group Targeting SEMI and Airline Sector

中國駭客「凱美拉行動」：台7家半導體公司受害 ，連設計圖都被看光光

一個客戶的意外發現，讓資安公司奧義智慧查出：至少有7家台灣半導體相關公司被中國駭客攻擊，部份案例潛伏時間甚至超過1年，連晶片設計圖、技術藍圖等文件都淪陷。難怪台積告訴供應商，資安過不了評鑑，就不能供貨。

今周刊 輸入關鍵字... 搜尋

熱門：COVID-19 台股 ETF 存股 蕭金河

從竹科七家半導體廠遭駭　到七家金融業者遭攻擊！中國駭客全新手法　為何一般資安軟體難抓出？

CyCraft is covered by top media Nikkei in Japan and is selected by Japan gov to protect SMEs

CyCraft uses AI cybersecurity to empower TSMC's cyber resilience

日本経済新聞

台湾サイクラフト、AIでサイバー対策　顧客にTSMCなど

アジア企業プロファイル

アジアBiz　＋フォローする

2023年4月17日 21:20 [有料会員限定]

保存

サイバー対策支援の台湾スタートアップである奥義智慧科技（サイクラフト）が、日本など海外への進出を積極化している。独自の人工知能（AI）を駆使し、ウイルスなど脅威の発見から対処方法の提案までを自動化するのが強みだ。中国からの攻撃が集中する台湾で技術を鍛え、世界の顧客を支える。

呉明蔚・共同創業者兼最高経営責任者（CEO）は20年の業界経験を持つ「ホワイトハッカー（正義のハッカー）」として世界的に有...

AI駆使しサイバー対策

奥義智慧科技(サイクラフト)（台湾）

アジア企業プロファイル

≪会社概要≫	
▼設立	2017年
▼本社	台湾北部・新北市
▼代表	呉明蔚・共同創業者兼CEO
▼事業	サイバーセキュリティー
▼業績	非公表

日本や米国に相次ぎ進出

サイバー対策支援の台湾スタートアップである奥義智慧科技（サイクラフト）が、日本など海外への進出を積極化している。独自の人工知能（AI）を駆使し、ウイルスなど脅威の発見から対処方法の提案までを自動化するのが強みだ。中国からの攻撃が集中する台湾で技術を鍛え、世界の顧客を支える。

呉明蔚・共同創業者兼最高経営責任者（CEO）は20年の業界経験を持つ「ホワイトハッカー（正義のハッカー）」として世界的に有名だ。2017年創業のスタートアップながら、顧客の顔ぶれは台湾積体電路製造（TSMC）など有力企業や、台湾の当局機関が名を連ねる。

台湾は中国からのサイバー攻撃に日々さらされ、世界のサプライチェーン（供給網）を支える企業を狙う攻撃も増えている。社員らの端末1台にでも穴があれば、被害は大きくなりかねない。

サイクラフトは端末上の脅威の検知から、検知した脅威の分析、対処方法の提案に至る重要工程それぞれにAIを導入し、顧客対応が早いのが売りだ。通常は数週間かかるとされる一連の作業を、1日以内に短縮できるという。

呉氏は最近のサイバー攻撃事情について、「中国は台湾を一種の『練習台』にし、日本などへの攻撃能力を高めている」と警鐘を鳴らす。

創業時から世界展開を意識し、19年にシンガポール政府系のベンチャーキャピタル（VC）から65万ドル（約7000万円）を調達。21年までに日本やシンガポール、米国に相次ぎ進出した。日本では東京都内の中小100社のサイバー対策を支援している。今後も積極的な世界展開を進める構えだ。（台北＝龍元秀明）

ラ・マレーシアを通じマレ

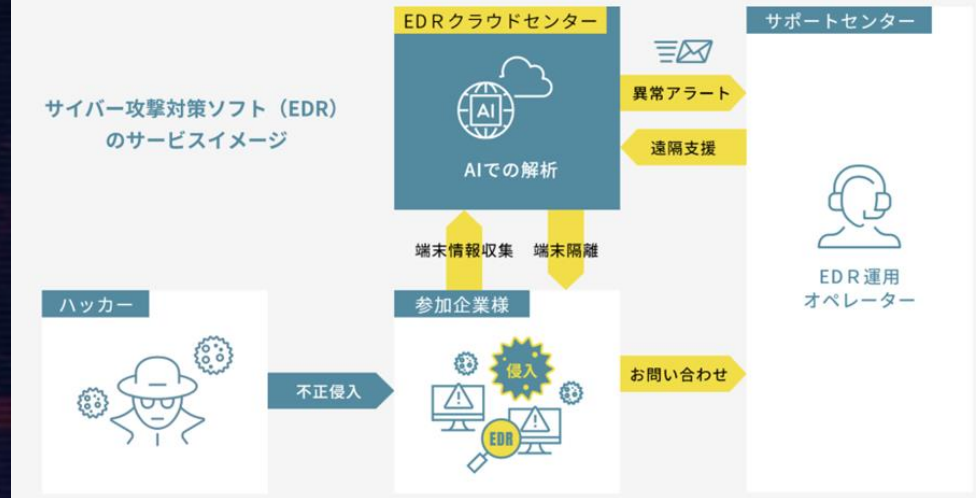
Recognized in Tokyo Interop as the Best of Show

東京都産業労働局

中小企業サイバーセキュリティ対策強化緊急サポート事業

EDRの導入とサイバー攻撃状況の把握・分析

社内の端末に不正侵入検知ソフト(EDR)をインストールし、不正アクセスを検知します。EDRソフトがサイバー攻撃を検知した場合は、セキュリティ監視センターからリモートで隔離対応を行い、被害の拡大を防ぎます。また、定期的なレポートを発行します。このレポートにより自社のサイバー攻撃状況を把握することも可能です。



不正侵入検知ソフト(EDR)のインストールに関して

- 本事業に基づき、受託事業者が提供する「CyCraft AIR」（EDR）サービスの体験機会（3か月間・無償）を提供いたします。

Source: https://security-kyoka.metro.tokyo.lg.jp/

Joint defense with global security communities

FIRST (Forum of Incident Response and Security Teams)

tsmc ASE

Sponsor by CyCraft

CSIRT 日本シーサート協議会

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

NO MORE RANSOM

NO MORE RANSOM

semi **Semi**
國際半導體產業協會

NCCST **N-ISAC**
國家資安資訊分享與分析中心

TW-DIDA **TW-DIDA**
台灣國防產業發展協會

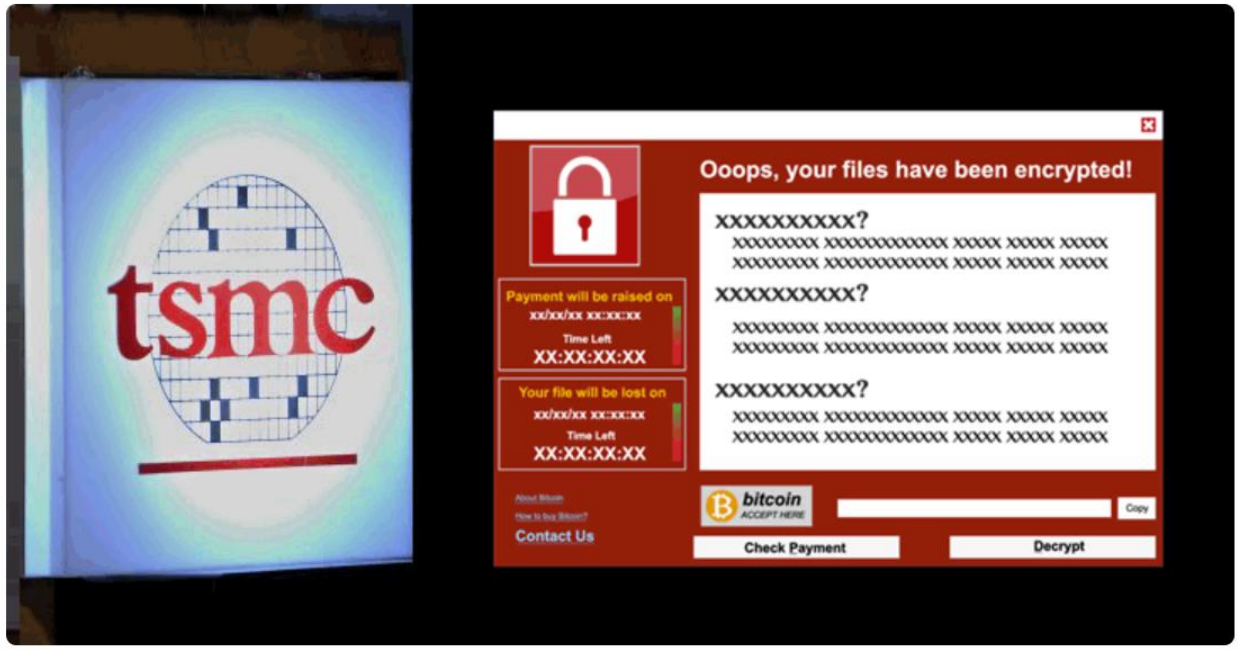
Storytime: APT, Ransomware, and cyberattacks

A wake-up call for TSMC and its suppliers

- The virus outbreak on August 3, 2018.
- The virus infected 10,000 machines within 3 days.
- The total cost was $170 million due to the production halt.

- The misoperation occurred during the software installation of new tools.
- There was no virus-free check before moving into the Fab.
- EoS OS(Win7) is still being used in Fab tools and automated materials handling systems.

Aug 07, 2018 Mohit Kumar



TSMC Details Impact of Computer Virus Incident

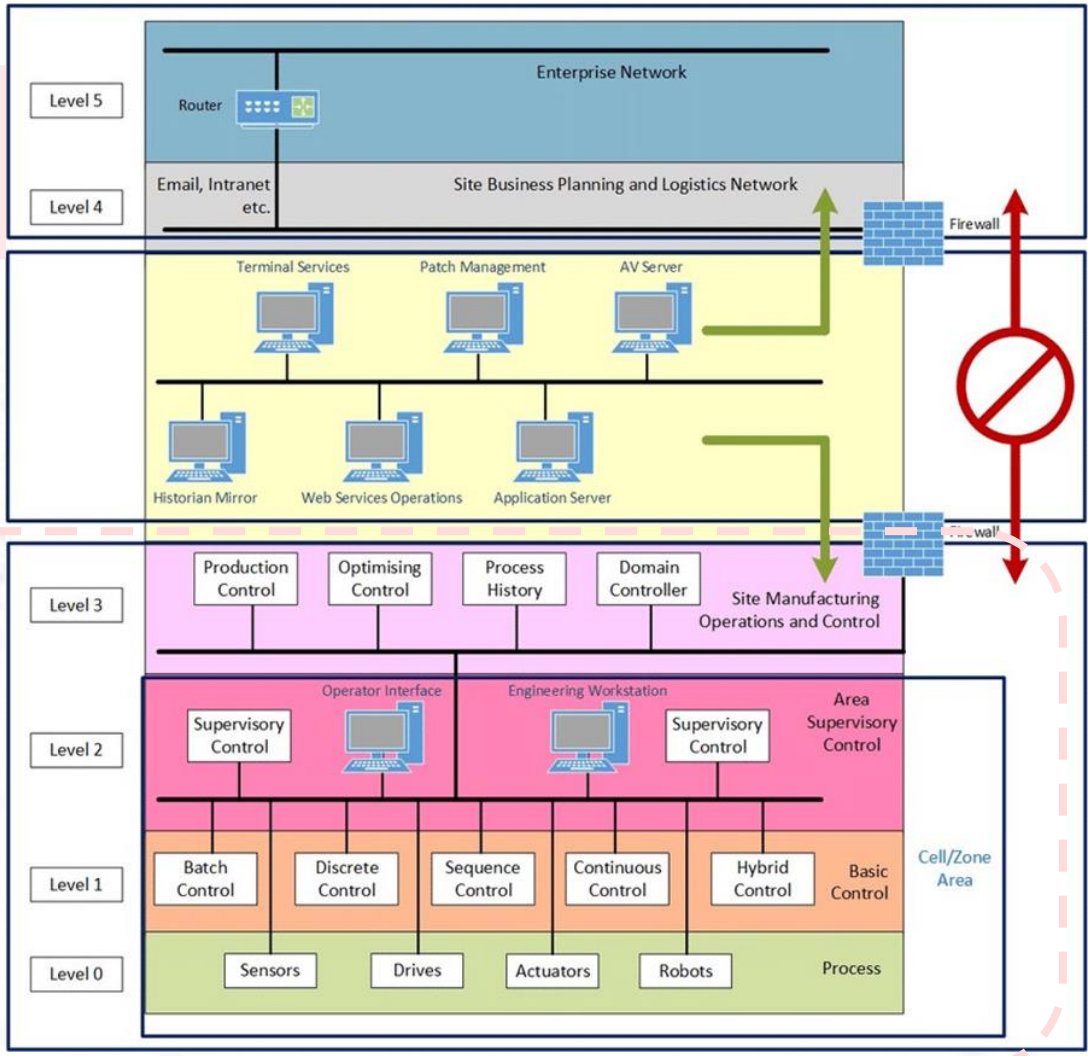
Hsinchu, Taiwan, R.O.C., Aug 5, 2018 – TSMC today provided an update on the Company's computer virus outbreak on the evening of August 3, which affected a number of computer systems and fab tools in Taiwan. The degree of infection varied by fab. TSMC contained the problem and found a solution, and as of 14:00 Taiwan time, about 80% of the company's impacted tools have been recovered, and the Company expects full recovery on August 6.

The call points out the Pain Points in SEMI industries

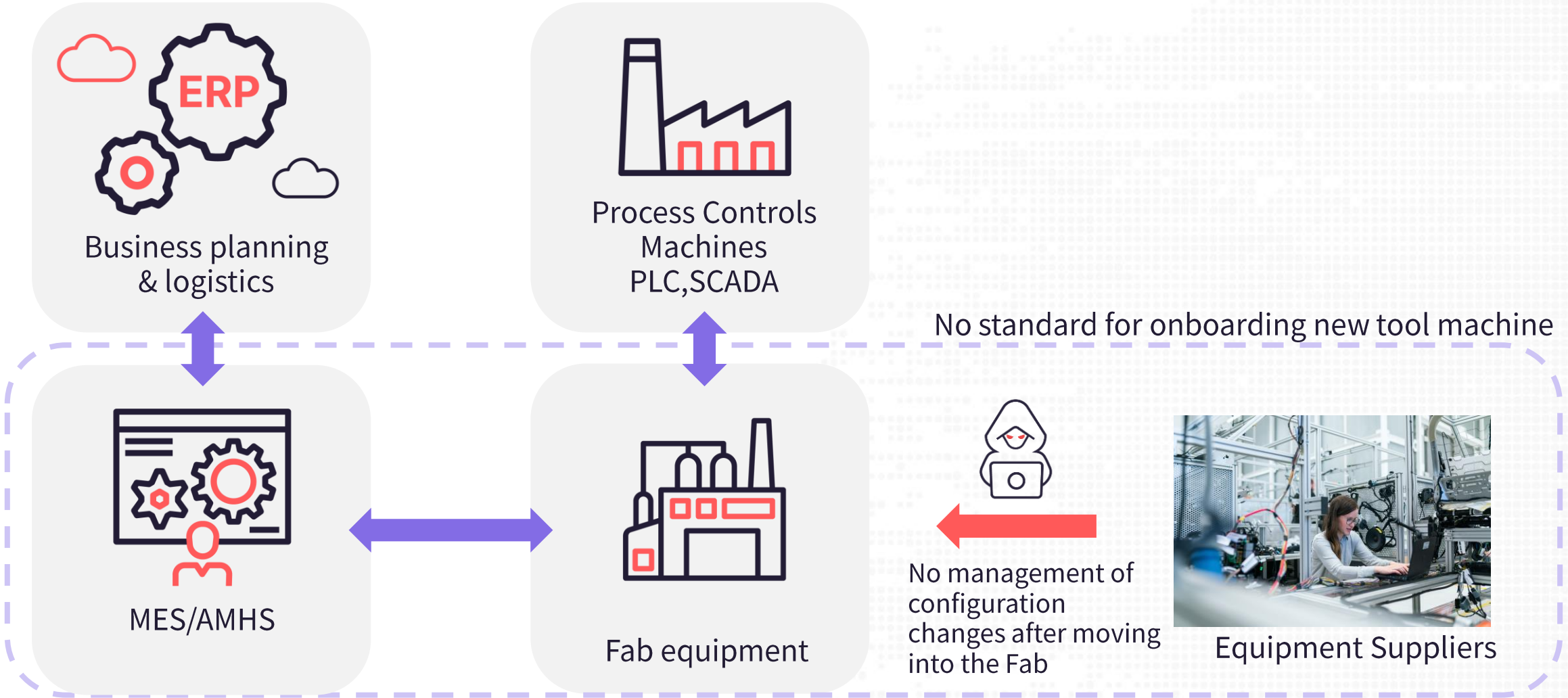
Assume those equipment are well segregated.
Assume no security patch is needed at L0 to L3.
Assume no vulnerability scanning is needed at L0 to L3.

There is too much implicit trust behind OT use cases.

- **Focus on production, not security monitoring**
- **No EDR or AV for real-time protection**
- **IT / OT infrastructure overlaps with low visibility**
- **EoL or Vulnerable systems remain unpatched in the fabric**



Equipment acts like a Trojan horse for foundry



From Task force to SEMI Committee

2018: Fab & Equipment Information Security Task Force

2021: SEMI Taiwan Semiconductor Cybersecurity Committee

2022: E187 Specification for cybersecurity for Fab equipment

2023: E187 Reference Practice

- The SEMI Taiwan Semiconductor Cybersecurity Committee has been established through the initiative of ITRI and TSMC in 2021. CyCraft is also a founding member of the committee.

The committee will meet every quarter to discuss supply chain security.

- 2022 SEMI E187
- 2023 SEMI E187 Reference Practice

New SEMI Standard E187 for Fab equipment

SEMI E187 defines the fundamental cybersecurity baseline requirements to secure semiconductor fab equipment by design and support security protection in both operation and maintenance.

This new baseline standard affects entities who provide equipment or services to semiconductor fabrication plants such as equipment suppliers and system integrators.

Assume Breach: Conduct a compromise assessment before entering FAB
Multi Access Control: Account management and tiered administration
Never Trust, Always Verify: Continuous monitoring and validation is required

https://www.semi.org/zh/technology_and_trends/quick_start_guide_to_new_cybersecurity_standard_e187

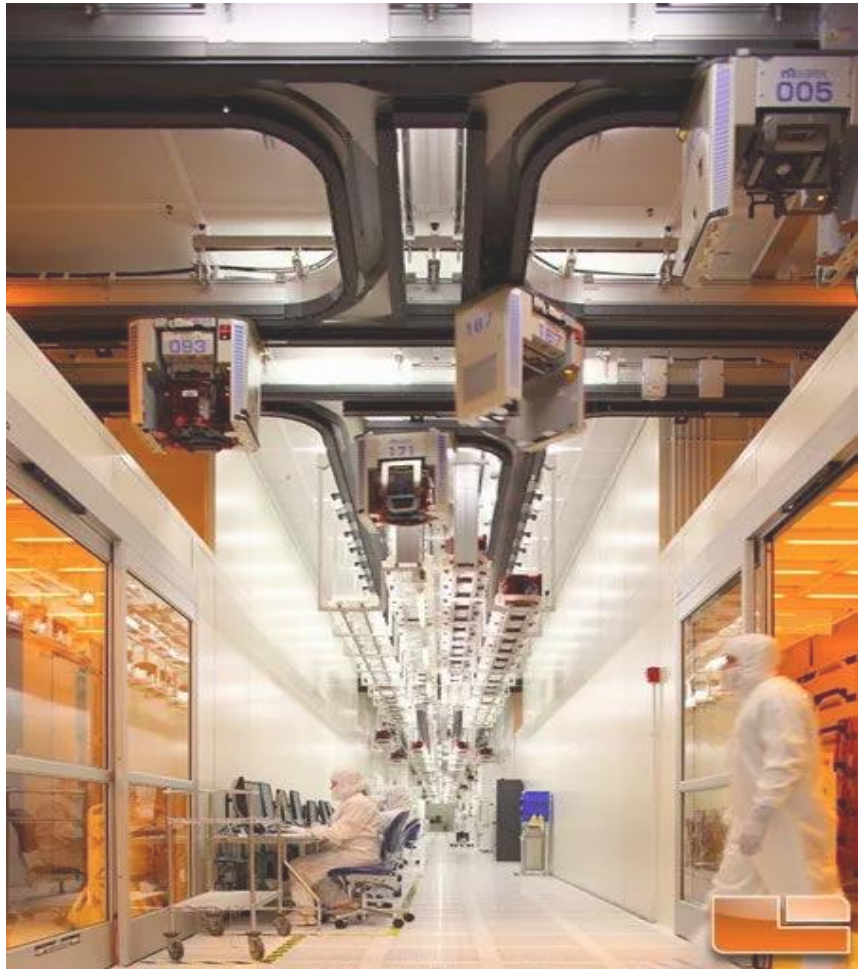
CYCRAFT

E187: the baseline of Fab equipment

E187 Requirements	Essential for S manufacturing	Advanced for M,L manufacturing
Security monitoring	• Logs management and export	• Application Logs • Data Access Logs • Backup and Restore • Configuration management
Endpoint Security	• Vulnerability mitigation • Malware scanning • Harden of used apps and services • Access control mechanism	• EDR Protection • Identity Protection
Network Security	• Secure transmission protocols • Harden of network services	• Independent firewall • Advance Authentication • Application network behaviors • Remote control • Intranet Segmentation
Operation System	• Non-EoL Operating Systems • Patch management procedure	• Virtual Patch

The above verification items can pass testing through Verification of Conformity (VoC) services.

TSMC utilizing the Power of Procurement Contracts to accelerate the adoption of new standard



List in Procurement Specification

Utilizing the power of procurement contracts, TSMC requires suppliers to implement the semiconductor equipment cybersecurity standard

Establish Verification Mechanism

Creating a verification checklist based on four dimensions to ensure compliance before introducing new equipment

Lead SEMI Cybersecurity Standard Working Group

Developing and promoting supply chain adoption standards, receiving the "2023 SEMI International Standards Excellence Award"

Promote SEMI Cybersecurity Risk Rating Service

Assisting semiconductor companies in identifying security vulnerabilities and enhancing protection effectiveness, benefiting over a thousand enterprises

Establish Cybersecurity Reference Architecture for Semiconductor Manufacturing Environment

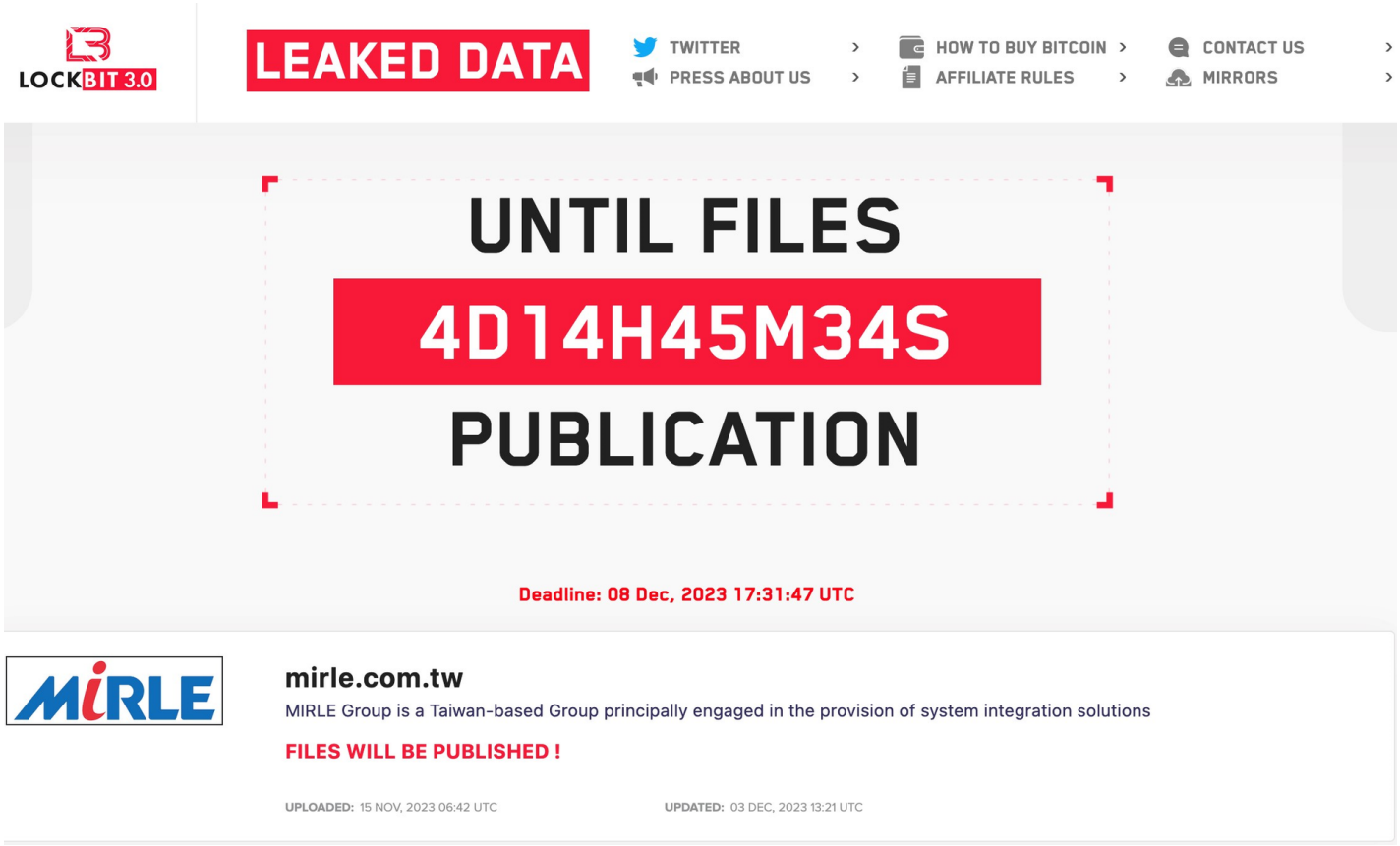
Defining the Cybersecurity Reference Architecture for Semiconductor Manufacturing Environment in partnership with SEMI to accelerate system integration and networking efficiency

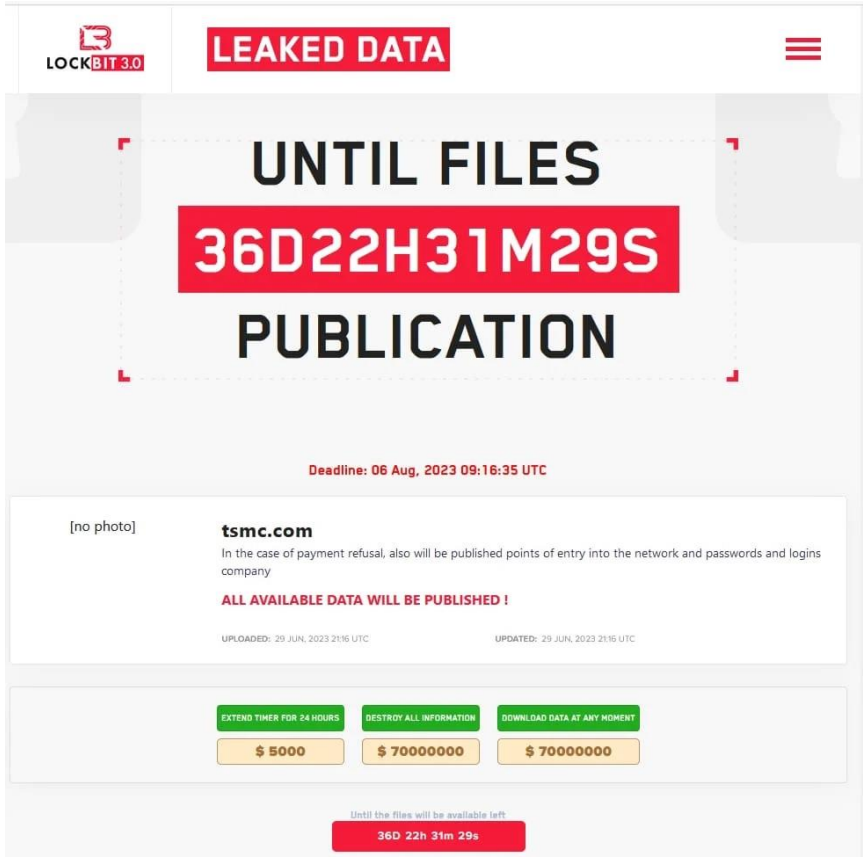
Ref. https://esg.tsmc.com/en/update/responsibleSupplyChain/caseStudy/43/index.html

The E187 is not applicable for suppliers who do not have a tool machine

The IT security of suppliers can still become an attack surface in the SEMI industry

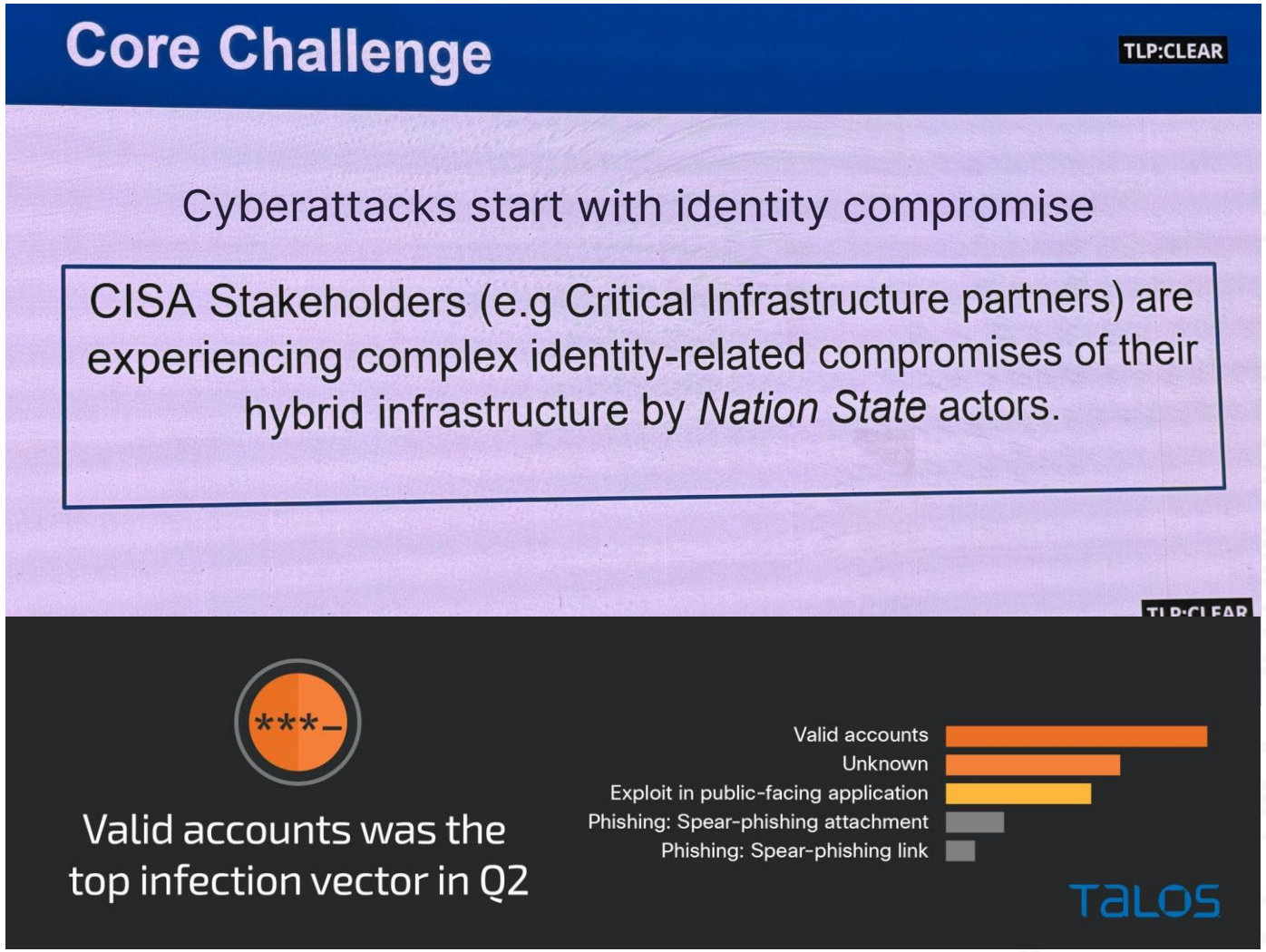
The LockBit hack on the breached supplier also targeted TSMC with a ransom demand

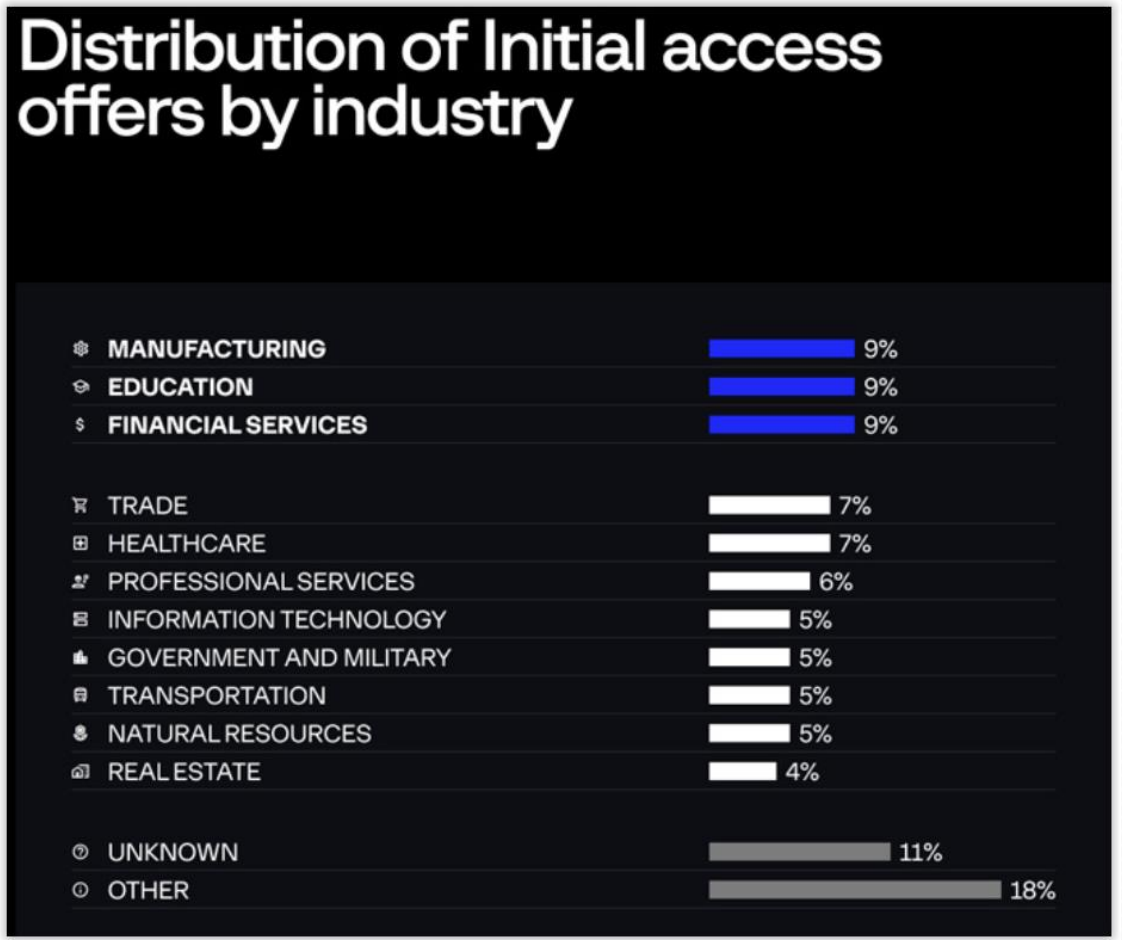




If something happens to the supplier, it means something may happen to the customer.

Attackers don’t break in, they log in





Ref. https://www.group-ib.com/media-center/press-releases/gib-2021-2022-report/
https://blog.talosintelligence.com/talos-ir-q2-2023-quarterly-recap/

Initial Access Brokers (IAB) are like locksmiths who provide door keys for attackers.

However, attacker take 60 minutes to reach their target from initial access

MITRE | ATT&CK

Matrices | Tactics | Techniques | Mitigations | Groups | Software | Resources | Blog | Contribute | Search

MATRICES

- Enterprise
  - PRE
  - Windows
  - macOS
  - Linux
  - Cloud
    - AWS
    - GCP
    - Azure
    - Office 365
    - Azure AD
    - SaaS
  - Network
- Mobile
  - Android
  - iOS
- ICS

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	6 techniques	9 techniques	10 techniques	18 techniques	12 techniques	37 techniques	15 techniques	25 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter	Boot or Logon Autostart Execution (12)	Access Token Manipulation (5)	Abuse Elevation Control Mechanism (4)	Brute Force	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	BITS Jobs	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)	Browser Extensions	Build Image on Host	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Native API	Compromise Client Software Binary	Debugger Evasion	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Scheduled Task/Job (6)	Create Account (3)	Deobfuscate/Decode Files or Information	Debugger Evasion	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Shared Modules	Create or Modify System Process (4)	Deploy Container	Deobfuscate/Decode Files or Information	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)		Supply Chain Compromise (3)	Software Deployment Tools	Event Triggered Execution (15)	Direct Volume Access	Deploy Container	Man-in-the-Middle (2)	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories (2)	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	System Services (2)	External Remote Services	Domain Policy Modification (2)	Direct Volume Access	Modify Authentication Process (4)	File and Directory Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	User Execution (2)	Hijack Execution Flow (11)	Escape to Host	Domain Policy Modification (2)	Network Sniffing	Network Service Scanning	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Windows Management Instrumentation	Implant Container Image	Event Triggered Execution (15)	Execution Guardrails (1)	OS Credential Dumping (8)	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (2)
				Office Application Startup (6)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Steal Application Access Token	Network Sniffing		Data Staged (2)	Non-Standard Port		Resource Hijacking
				Pre-OS Boot (5)	Hijack Execution Flow (11)	File and Directory Permissions Modification (2)	Steal or Forge Kerberos Tickets (4)	Password Policy Discovery		Email Collection (3)	Protocol Tunneling		Service Stop
				Scheduled Task/Job (6)	Process Injection (11)	Hide Artifacts (6)	Steal Web Session Cookie	Peripheral Device Discovery		Input Capture (4)	Proxy (4)		System Shutdown/Reboot
				Server Software Component (3)	Scheduled Task/Job (6)	Hijack Execution Flow (11)	Two-Factor Authentication Interception	Permission Groups Discovery (3)		Man-in-the-Middle (2)	Remote Access Software		
				Traffic Signaling (1)	Valid Accounts (4)	Impair Defenses (6)	Unsecured Credentials (6)	Process Discovery		Screen Capture	Web Service (3)		
				Valid Accounts (4)		Indicator Removal on Host (6)		Query Registry		Video Capture			
						Indirect Command Execution		Remote System Discovery					
						Masquerading (6)		Software Discovery (1)					
						Modify Authentication Process (4)		System Information Discovery					
						Modify Registry		System Network Configuration Discovery					
						Modify System Image (2)		System Network Connections Discovery					
						Network Boundary Bridging (1)		System Owner/User Discovery					
						Obfuscated Files or Information (5)		System Service Discovery					
						Pre-OS Boot (5)		System Time Discovery					
						Process Injection (11)		Virtualization/Sandbox Evasion (3)					
						Rogue Domain Controller							
						Rootkit							
						Signed Binary Proxy Execution (11)							
						Signed Script Proxy Execution (1)							
						Subvert Trust Controls (4)							
						Template Injection							

(Initial Access)

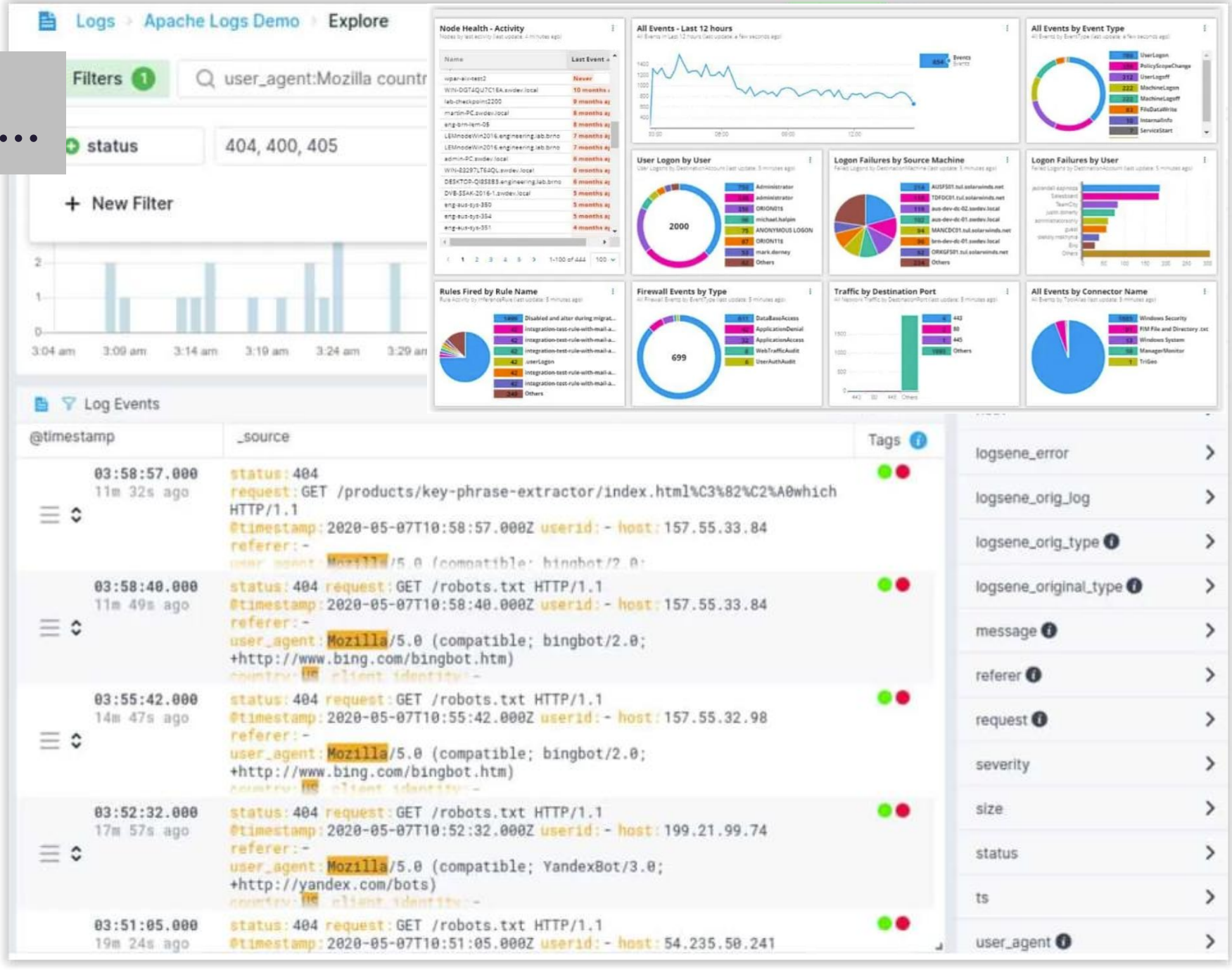
(Lateral Movement)

(Defense Evasion)

Good statistical charts with truly raw data, but …

Lack of Key Risk Indicators (KRI)
Lack of Key Performance Indicators (KPI)
Lack of Mean Time to Respond (MTTR)
Lack of Mean Time to Detect (MTTD)

XXX Security Report

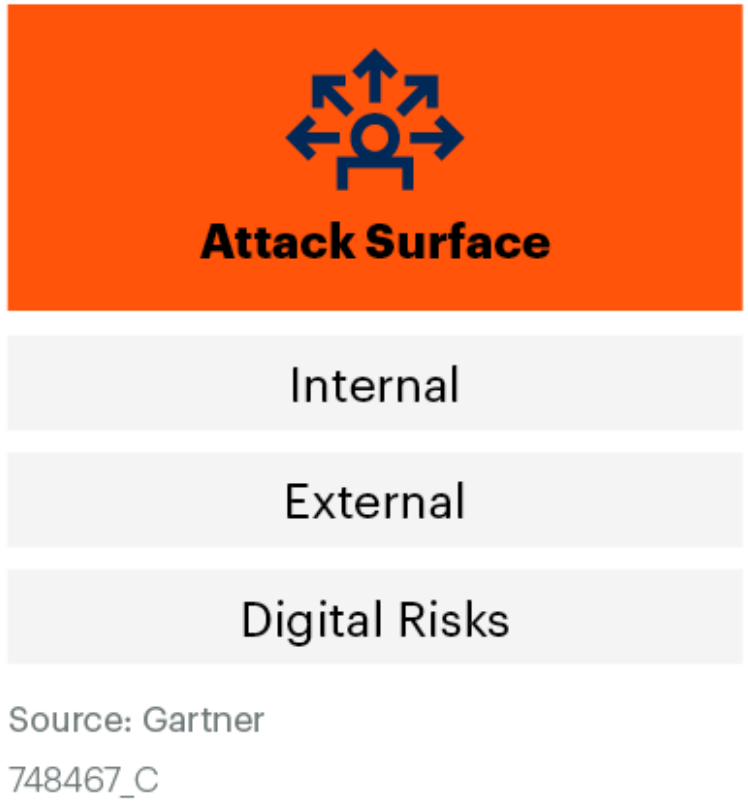


TW SEMI promotes unified supplier assessment with threat exposure rating services

Cyber Security Assessment (Questionnaire)

Ref. https://www.semi.org/zh

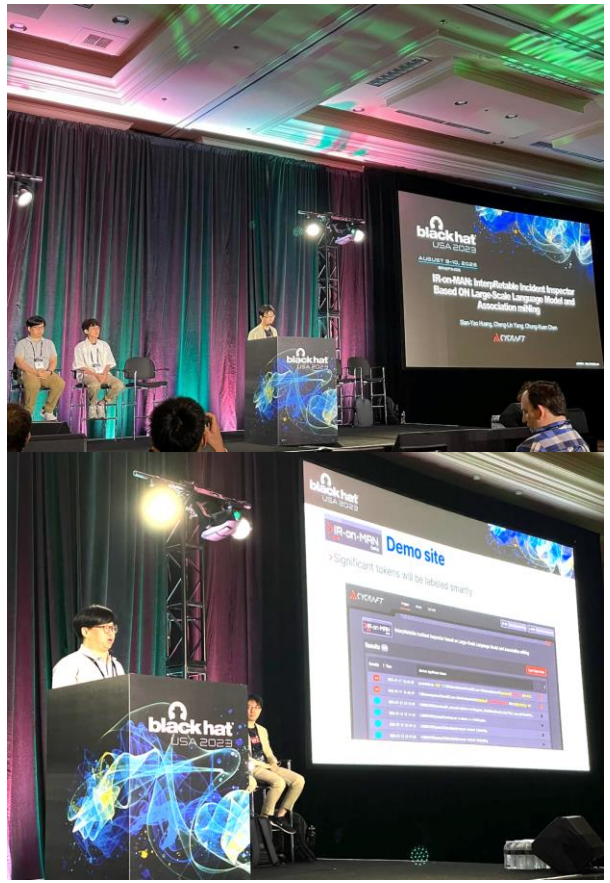
Attack Surface Management

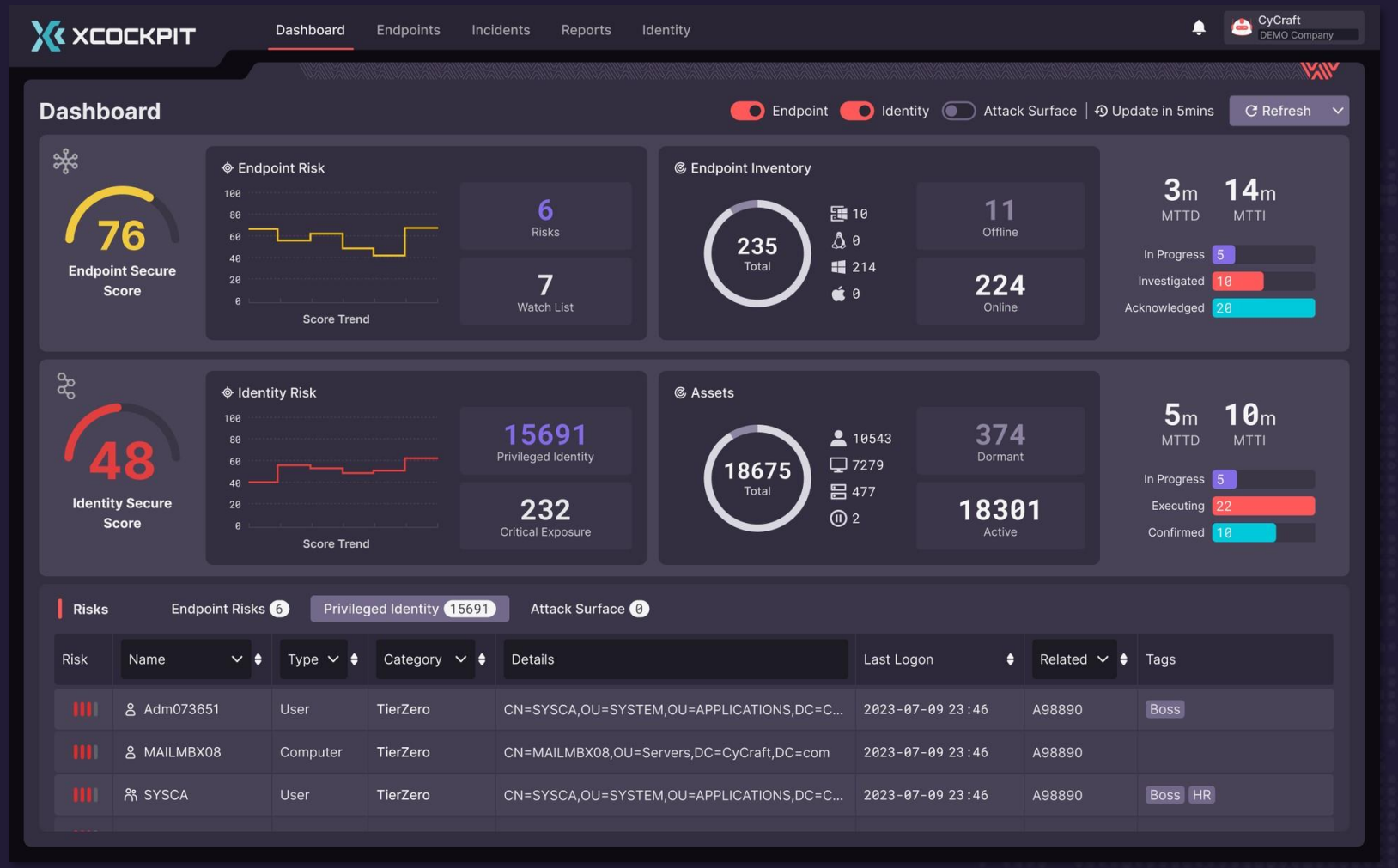


See what an adversary sees from the outside in


Continuous Threat Exposure Management is a new trend
What can AI help with?

The first similarity analysis for CmdLog using LLM





必要な情報はすべて可視化

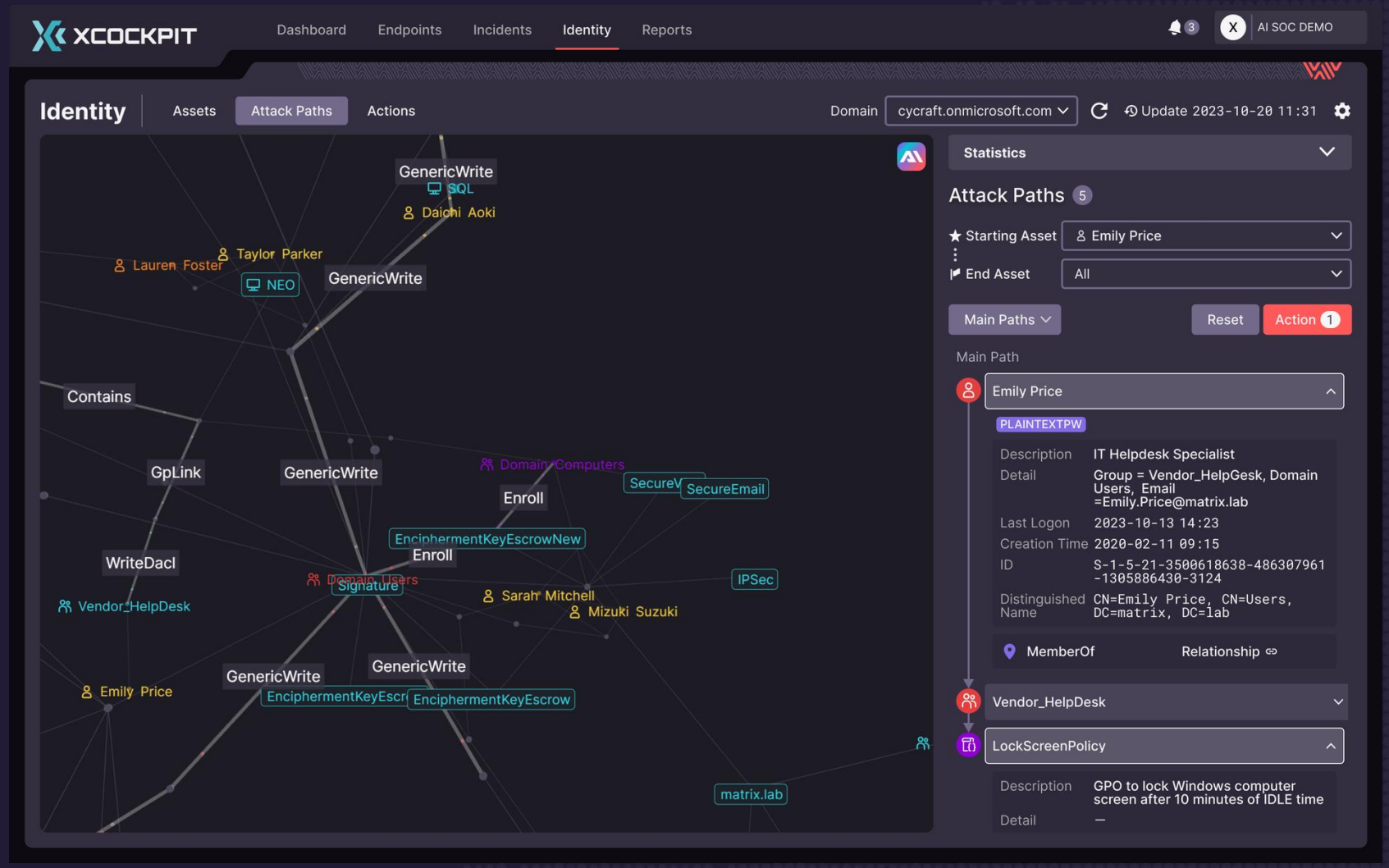
オンプレミス環境、クラウド環境を問わず、
XCockpitはすべての資産、サービス、
エンドポイント、グループ、アカウントの
隠れた関係性を調査し、
それらがどこにさらされているかを把握し、
リスクを定量化します。

CYCRAFT


XCOCKPIT
Dashboard
Endpoints
Incidents
Reports
Management
AIバーチャル・アナリストは、ケース全体の概要説明を作成し、セキュリティ担当者のケースに対する理解を助けるとともに、対応効率を高めます。
2023-0504-Malware (ja) - Incident Viewer
Event Graph
Incident Briefing
Note
Switch to 2D Graph
要約：
2023年5月4日の12:06:20から12:16:21までの約10分間に、オペレーティングシステムが「Windows Server 2019 Datacenter 1809」で、エンドポイント名が「CREEPER」、グループが「CYCORP」であるコンピュータ上で、以下の高いリスクのイベントが発生しました。
- 2023年5月4日の12:06:20、「C:\WINDOWS\System32\rundll32.exe」が実行されました。（テクニックID：T1055.000、プロセスインジェクション；T1550.000、代替認証素材の使用；T1003.000、OS資格情報ダンプ。悪意のあるソフトウェア名：COBALTSTRIKE.1; METASPLOIT.SH1; CobaltStrike、ポストエクスプロイトおよび横方向移動ツール。）
- 2023年5月4日の12:15:49、「C:\Windows\System32\WindowsPowershell\v1.0\powershell」が実行されました。（テクニックID：T1027.000、難読化されたファイルまたは情報；T1105.000、入り口ツールの転送。）
- 2023年5月4日の12:16:21、「C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe」が実行されました。（テクニックID：T1003.002、OS資格情報ダンプ：セキュリティアカウントマネージャー；T1027.000、難読化されたファイルまたは情報；T1003.005、OS資格情報ダンプ：キャッシュされたドメイン資格情報。）
- 2023年5月4日の12:16:21、「C:\WINDOWS\system32\reg.exe」が実行されました。（テクニックID：T1003.002、OS資格情報ダンプ：セキュリティアカウントマネージャー；T1003.005、OS資格情報ダンプ：キャッシュされたドメイン資格情報。）
エンドポイントフォレンジックレポートに対する対策として、サイバーセキュリティチームが注視すべき点と緊急対応策については、以下の通りです。悪意のあ
9 Execution
2023-05-04 13:16:21
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Details
"C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -noP -sta -w 1 -enc UgBIAGcALgBlAHgAZQAgAHMAYQB2AGUAIABIAEsATABNAFwAUwBBAE0AIABzAGEAbQAuAGgAaQB2AA==
PID 900
SID S-1-5-21-3188494444-2937684683-888728269-500
Information • Parent Process: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe (PID:4332)
MITRE ATT&CK®
T1003.002 OS Credential Dumping: Security Account Manager
T1003.005 OS Credential Dumping: Cached Domain Credentials
T1027.000 Obfuscated Files or Information
T1059.001 Command and Scripting Interpreter: PowerShell
AIバーチャル・アナリストは、最新の攻撃手法に対応
Close
Change State
CREEPER
CYCORP
Windows Server 2019 Datacenter
192.168.41.14
6 Incidents
0 Confirmed
0 Closed
Incidents
INVESTIGATED
2023-0504-Malware
2023-05-04 12:06:20 (14m)
Malware
Attacker Activity
Suspicious Activity
27
Total Events
INVESTIGATED
2023-0504-Malware (en)
2023-05-04 12:06:20 (14m)
INVESTIGATED
2023-0504-Malware (ja)
2023-05-04 12:06:20 (14m)
3
12:16:21 "C:\WINDOWS\System32\WindowsPowerS… UwBBAE0AIABzAGEAbQAuAGgAaQB2AA==
12:16:27 "C:\WINDOWS\system32\cmd.exe" /c echo T1145-1 start
2023-05-04 12:16:21
T1003.005 OS Credential Dumping: Cached Domain Credentials
T1059.001 Command and Scripting Interpreter: PowerShell

高リスクアカウントの影響分析

Identity LandscapeのAI技術により、組織内のアカウント権限の相関関係を把握し、攻撃経路をシミュレーションして予測します。
また、従来のアカウントインベントリに代わり、高権限アカウントの影響度分析を実行します。



CYCRAFT

CyCraftGPT

次世代言語モデルAIが分析レポートを
生成し、要約説明を提供。
企業内の複雑なアカウント構造を
処理するための方向性を提案します。

2023 年 10月 6日 11:01:57，CyCraft AI仮想アナリストは、MATRIX.LAB AD ドメインのアカウント分析をして、特権アカウント他への攻撃経路分析をしました。結果、総合セキュリティ評価スコアは42点でした。この分析では、合計で 2374のオブジェクトが検査され、12のユーザーアカウント、6のコンピューターアカウント、68のグループ、およびその他の 2288のオブジェクトが含まれていました。アカウント関係を分析した結果、62の特権アカウントが存在することが判明し、その中には 15のTierZero アカウントと 47の管理アカウントが含まれていました。最小権限の原則に基づいて、アカウント全体とリソースの関係や構造を分析することで、次項のアカウントセキュリティの強化提案がまとめられました：

＜アカウントセキュリティの強化提案＞

アセット権限の調整：潜在的な脅威を減らすための権限の変更

オブジェクトのフォルダリダイレクション（GPO）、デフォルトドメインコントローラーポリシー（GPO）、暗号化キーエスクロー（AD CSテンプレート）、Internet Explorer Setting（GPO）、matrix.lab（DOMAIN）、IPSec、パスワードポリシー（GPO）、SecureEmail（AD CS Template）、EnciphermentKeyEscrowNew（AD CS Template）、デフォルトドメインポリシー（GPO）、SecureVPN（AD CS Template）、署名、Tainan-ADMIN、アカウントロックアウトポリシー（GPO）、Office 365設定、Windowsファイアウォール設定（GPO）、ソフトウェアインストール（GPO）の権限設定を確認してください。これらのオブジェクトには明らかな設定エラーが存在し、多数の低特権アカウントに特権アセットを制御させており、セキュリティポリシーに違反しています。特に特別な理由がない限り、関連する権限設定を変更して、最小限の権限原則に合致するようにすることをお勧めします。

アカウント Mei Ishikawa（USER）の必要性を確認してください。アカウントMei Ishikawa（USER）は特権アセットを直接または間接的に制御できます。これらのアカウントが長期間使用されていない場合および使用されなくなった場合、アクセス権の範囲を制限するために無効にすることをお勧めします。

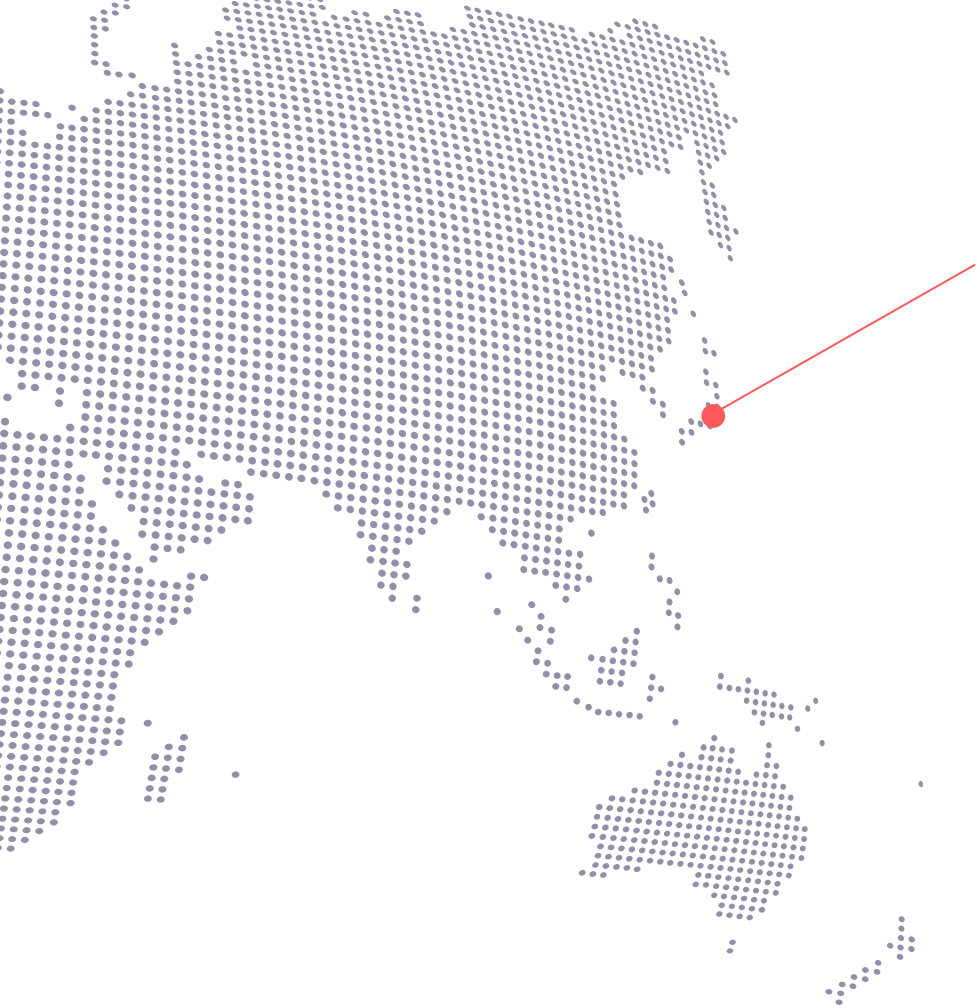
アイデンティティの強化：ネットワークセキュリティポリシーに基づいたアカウントセキュリティの向上

アカウント Daniel Cooper（USER）のパスワード設定を確認してセキュリティを強化してください。アカウントDaniel Cooper（USER）には現在、直接的なリスクはないかもしれませんが、パスワードが簡単に破られる可能性があるため、セキュリティを強化する必要があります。パスワードポリシーを強化するか、破られるリスクを回避するために Microsoft MSA メカニズムを検討してください。

アカウント matrix.lab（DOMAIN）、EnciphermentKeyEscrow（AD CS Template）、EnciphermentKeyEscrowNew（AD CS Template）、SecureVPN（AD CS Template）のアクセス権限や設定が過度に高いかどうかを確認してください。これらは他の一般的な特権アカウントに比べてセキュリティリスクがある可能性があります。これらは管理要件の専用アカウントかもしれません。これらのアカウントの目的を確認し、必要に応じてアクセス権限の範囲を調整してセキュリティを向上させてください。

Takeaways

- **To solve the four pain points, the entire SEMI industry needs to cooperate with each other, and awareness should be trained so that they can use standard or guidelines to improve the maturity of cybersecurity.**
- **The E187 standard serves as a baseline; its purpose is to encourage tool machine vendors to pay more attention to security during the design phase.**
- **Credentials and identities remain a vulnerable aspect and have become the most targeted attack vector for ransomware groups. Assessing identity attack paths and conducting Continuous Threat Exposure Management (CTEM) should be considered essential daily activities.**
- **SecOps should not exist solely for experts to serve the security solution; instead, the solution should serve and empower the security team.**



CyCraft Japan

担当者：Renata （れなた）Chang

renata.chang@cycraft.com

CyCraft Japan

〒100-0004　東京都千代田区大手町一丁目９番２号
大手町フィナンシャルシティグランキューブ３階

Global Business Hub Tokyo 81-03-6378-1053

奧義智慧 台北辦公室

新北市板橋區遠東路3號6樓

02-7739-0077

奧義智慧 台南辦公室

台南市歸仁區歸仁十三路一段6號
(資安暨智慧科技研發大樓)3樓323室

0972-285-216

CYCRAFT

Thanks!

EVERYTHING
STARTS
FROM
SECURITY