XTI&H – Extended Threat Intelligence & Hunting

Collecting intelligence to proactively detect and act on threats.

baseVISION
SECURE & MODERN ENDPOINT MANAGEMENT

Company's Challenges

baseVISION

CHALLENGES

- Ransomware
- Infostealer Malware
- Business Email Compromise
- Phishing
- Account Takeover
- Supply Chain Attack
- Regulations

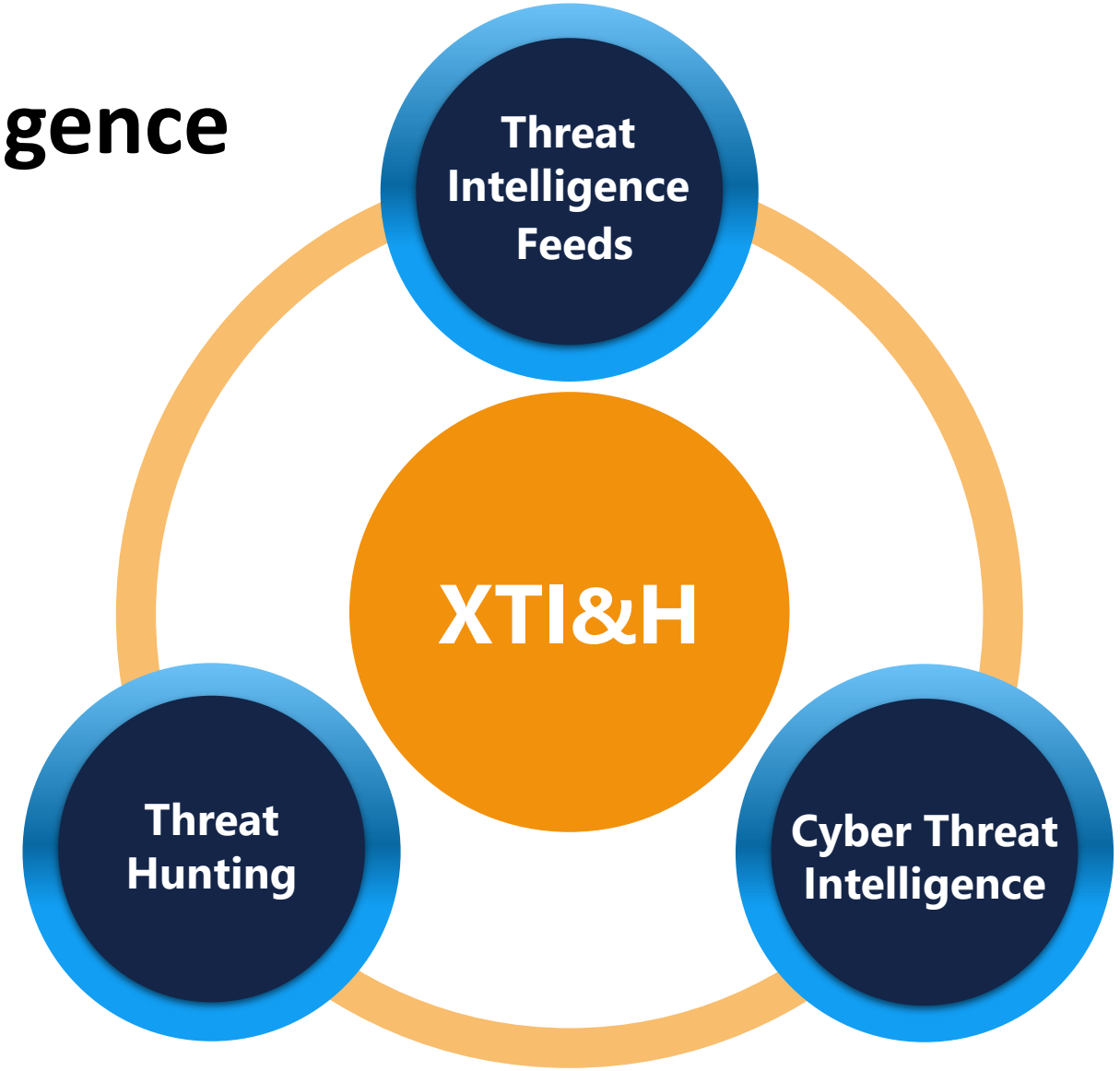
SOLUTIONS

- Automation
- Early Warning System
- Contextualized Intelligence
- Actionable Advice

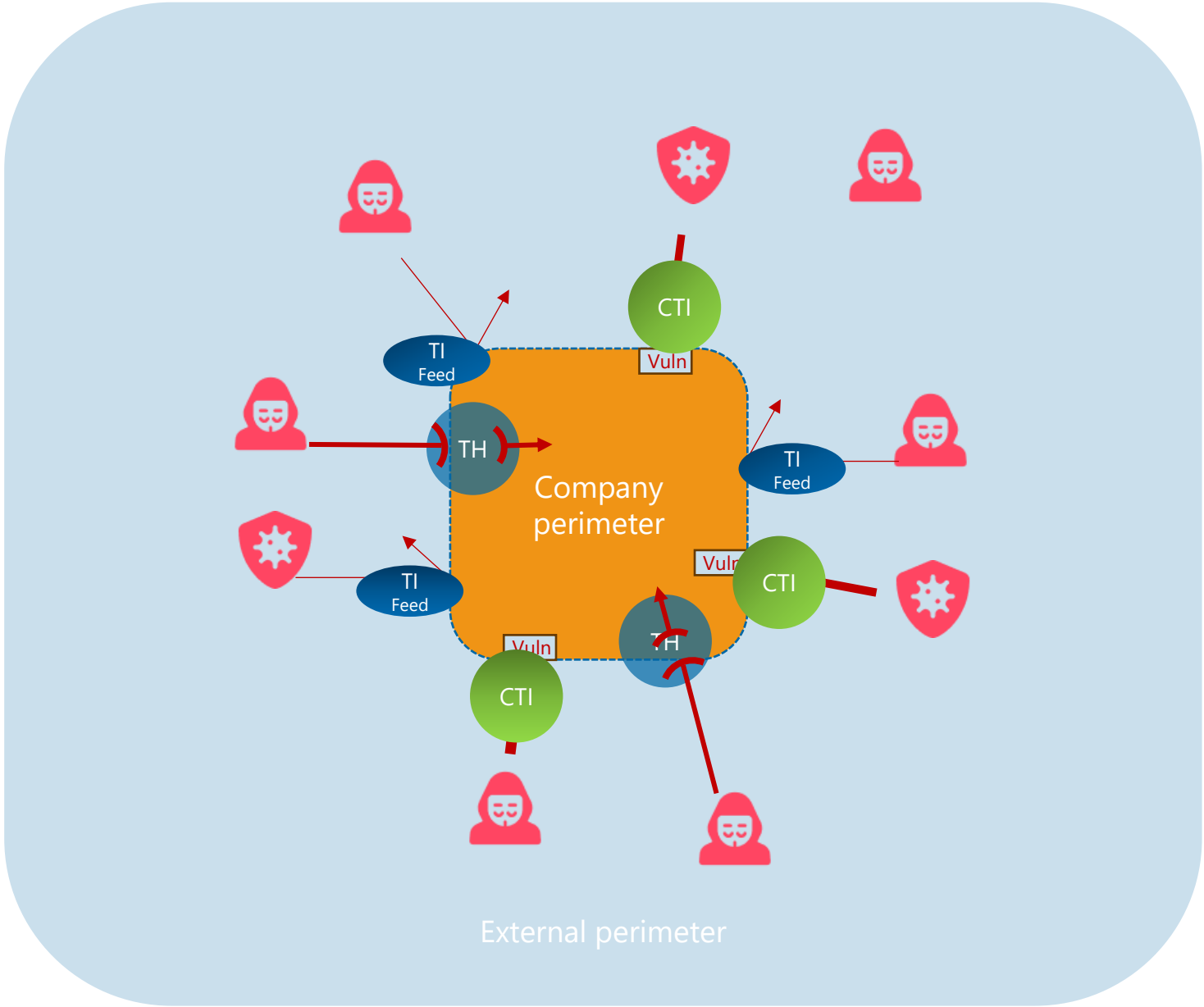
Extended Threat Intelligence & Hunting (XTI&H)

Threat intelligence enriched with A 360° solution integrating Threat Intelligence Feeds, Proactive Threat Hunting, and Cyber Threat Intelligence.

Empower your security with a one-stop shop for actionable insights and preemptive threat mitigation.



XTI&H a 360° Solution



TI Feeds will detect & block IOCs

CTI will proactively monitor and alert on threats & vulnerabilites

TH will identify threat that had bypassed security measures and remove them

What is the Value of baseVISION XTI&H?

baseVISION XTI&H Solution

PROACTIVE SECURITY MEASURES

- Phishing Detection
- VIP & Executive Protection
- Vulnerability Detection
- Deep / Dark Web Monitoring
- Leaked Data / PII Monitoring
- Takedown Service

INFORMED DECISION-MAKING

- Threat Landscape Monitoring
- Supply Chain Monitoring
- Vulnerability Prioritization

ENHANCED INCIDENT RESPONSE

- Actionable Intelligence Dissemination (IOC-IOA)

REGULATORY COMPLIANCE

- Swiss IKT minimal standard 2023
- ISO27001:2022 - New Annex A5.7 Threat Intel

Threat Intel Feeds

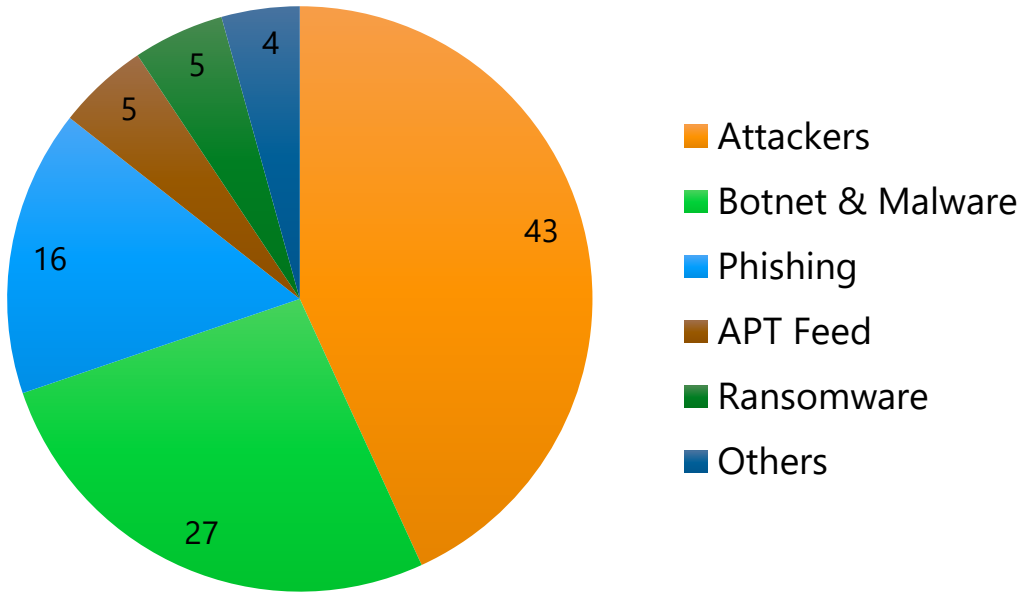
Multiple sources of trust for Threat Intel

baseVISION Threat Intelligence Feeds

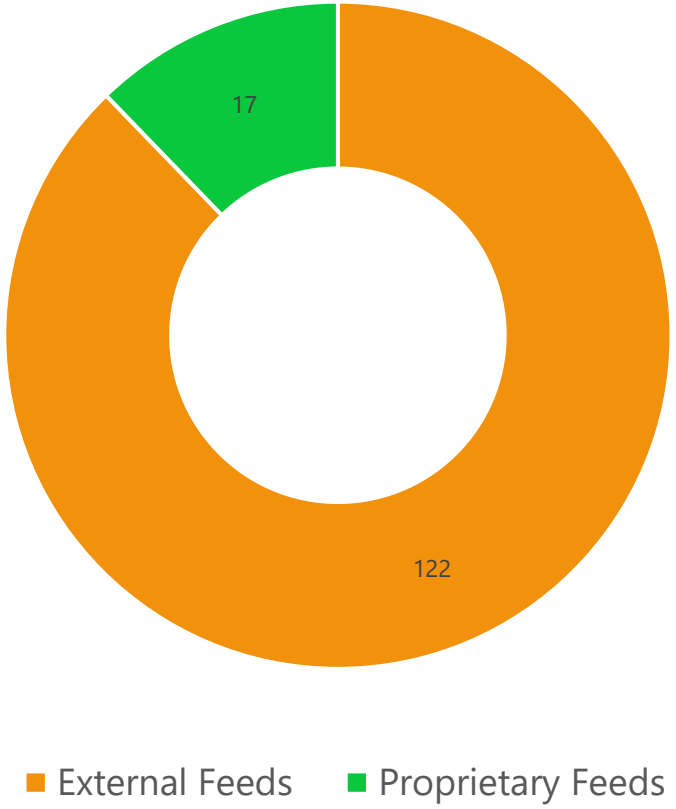
* Only when signed up for CS Hub (NCSC)

Threat Intel Feed Content

Type



Source



Value - baseVISION TI Feeds Service

CHALLENGES

- Evolving Threats
  - Threat groups increase/update their attack strategies.
- One Single Source is unreliable
  - A single source is just a drop in the ocean - true defense requires the full picture

SOLUTION

- Rely on Intelligence Sharing
- Use of multiple sources of intelligence

Proactive Threat Hunting

Identify threats that have bypassed your defenses.

Proactive Threat Hunting Service

Incident and Intelligence-based Hunting:

Leveraging incidents across our client base
Leveraging intelligence to perform hunting for known malicious threats that might be lurking within the perimeter

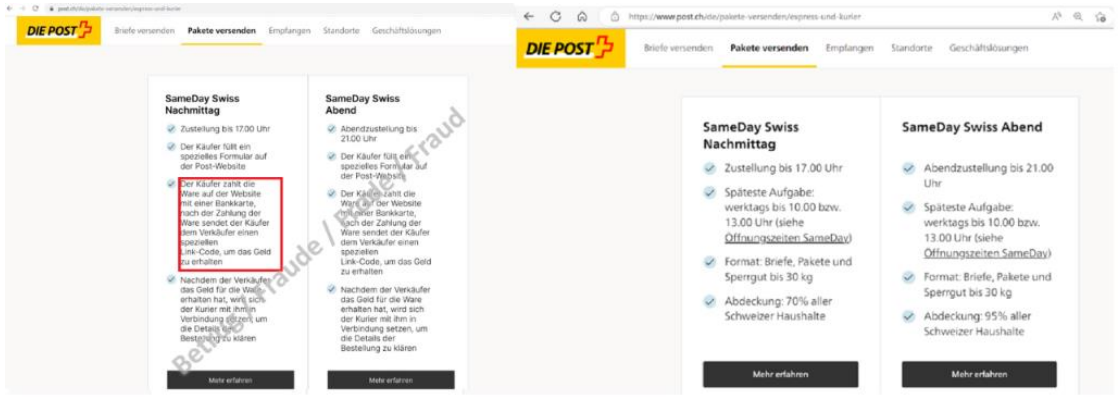
Tactics, Techniques, & Procedures-based Hunting

Standard Hunting Session: Identifying the detection gaps against the MITRE ATT&CK matrix and hunting for evidence of infection

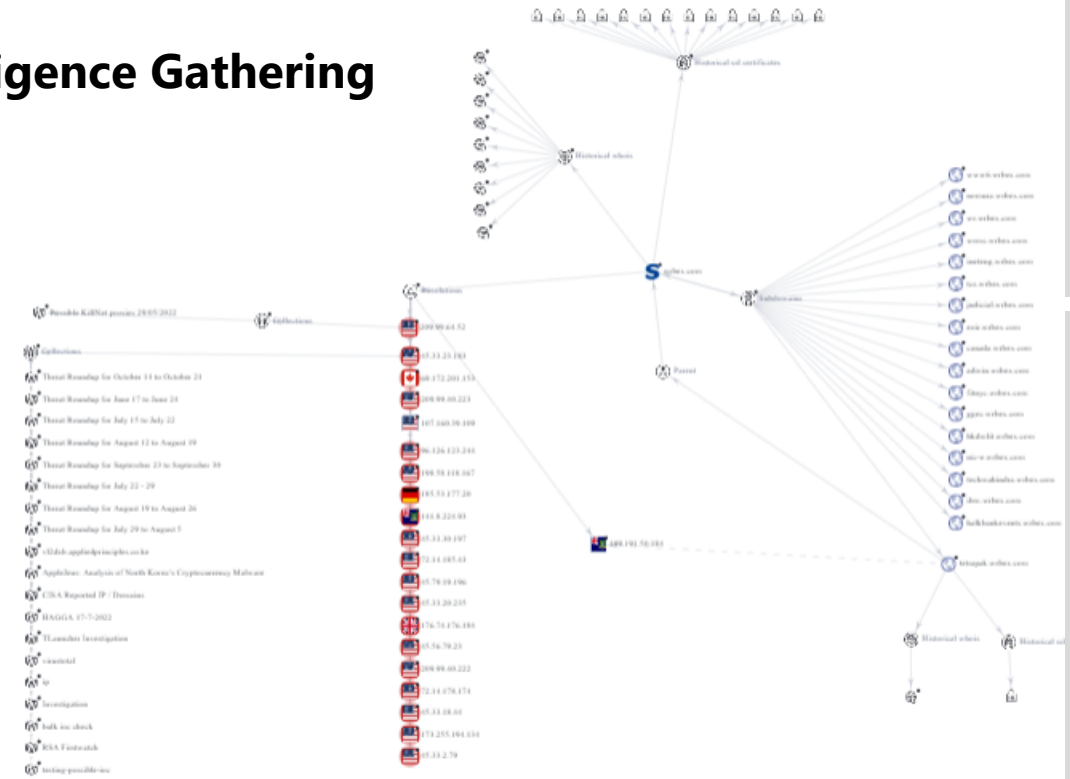
Extended Hunting Session: Threat landscape assessment to generate Hypothesis & use of the Diamond model to hunt for adversarial activities.

Incident & Intelligence-based Threat Hunting

NCSC Alert



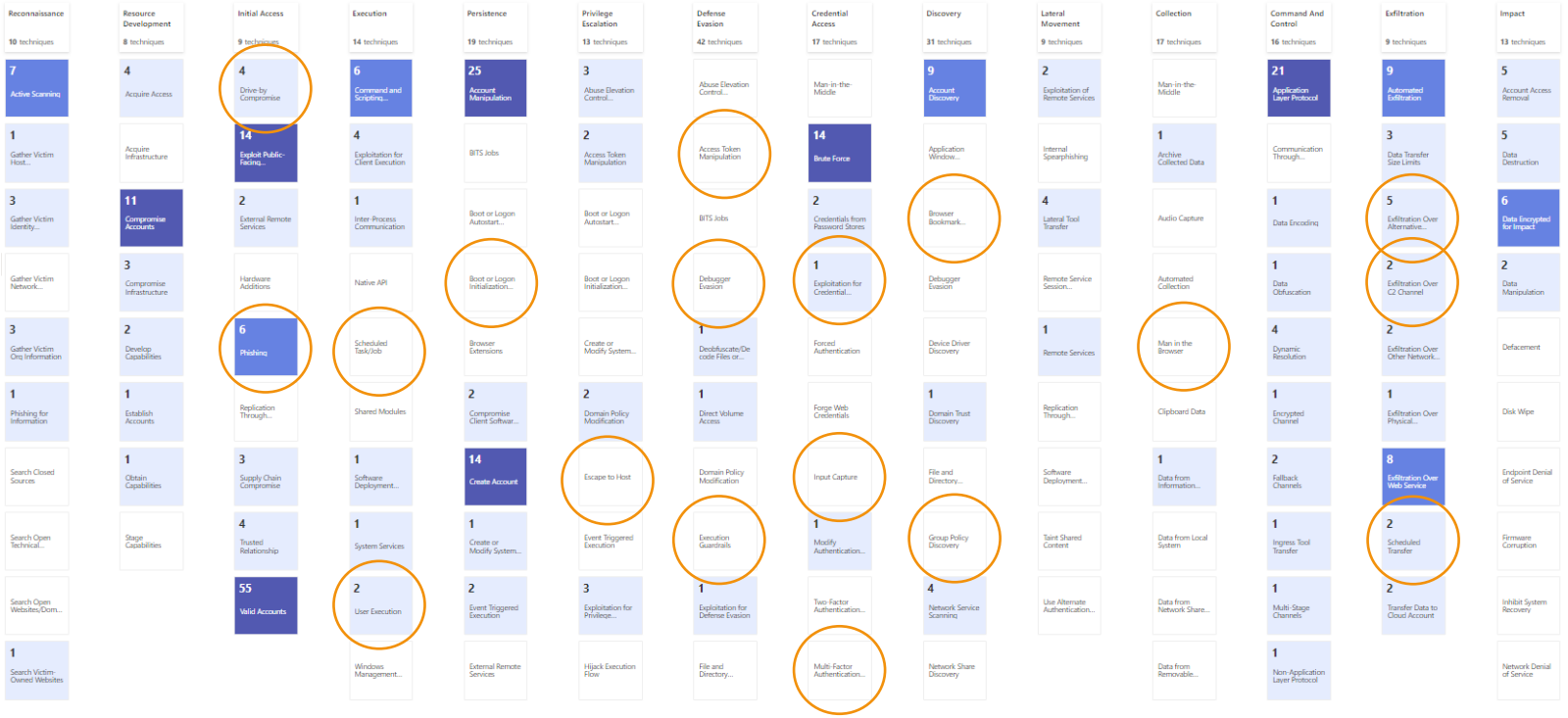
Intelligence Gathering



Threat	Phishing campaign impersonating **Swiss Post**	NCSC Alert
Gather Intelligence	Intel on Campaign: **IOCs/IOAs**	
	Threat Actor	Adversary
	Tactics, Techniques, & Procedures	A. Malware Execution? B. Credential Harvesting?
Response	Block Emails/IOCs	
	A. Remove Malware	
	B. Assume User Compromise	
	Create Detection	

Standard Session: Detection Gaps Against MITRE ATT&CK Matrix

Infostealer Infections:
Lumma Stealer uses 91 Techniques in which 34 are not covered.



Threat

Infostealer Malware Infection: **Lumma Stealer**

Gather Intelligence

Intel on Malware

IOCs IOAs

Lab: Reverse Engineering

Threat Actor

Response

Block IOCs

Hunt & Remove Malware

Assume User Compromise

Create Detection

Standard Session: Vulnerability Intelligence

Critical Vulnerability Identified

CVSSv3

Vectors	Priority
Attack Vector (AV):	NETWORK
Attack Complexity (AC):	LOW
Privileges Required (PR):	NONE
User Interaction (UI):	NONE
Scope (S):	UNCHANGED
Availability Impact (A):	HIGH
Confidentiality Impact (C):	HIGH
Integrity Impact (I):	HIGH

Source: nvd@nist.gov

Ranks

Exploitabil | CVSS | Impact

Exploitability Score : 3.9 CVSS : 9.8 Impact Score: 5.9

Severity (10)

Vector String

CVSS:3.1 AV:N AC:L PR:N UI:N S:U C:H I:H A:H

Intelligence Gathering

★ Rank: 14

UNC5820

UNC5820 is a threat actor group identified by security researchers in October 2024, following a collaboration between Mandiant and Fortinet. This group exploits vulnerabilities in FortiManager appliances, specifically leveraging CVE-2024-47575 / FG-IR-24-423 to gain unauthorized access to devices across various industries. As early as June 27, 2024, UNC5820 was observed staging and exfiltrating configuration data from FortiGate devices managed by compromised FortiManagers. This data includes critical configuration details, user information, and FortiOS256-hashed passwords, which could allow the group to further compromise the FortiManager and move laterally within the enterprise environment.

Threat	**CVE-2024-47575**
Gather Intelligence	Intel on Vulnerability
	Threat Actor Exploit
	IOCs
Response	Block IOCs
	Remove Malware/Persistence
	Create Detection

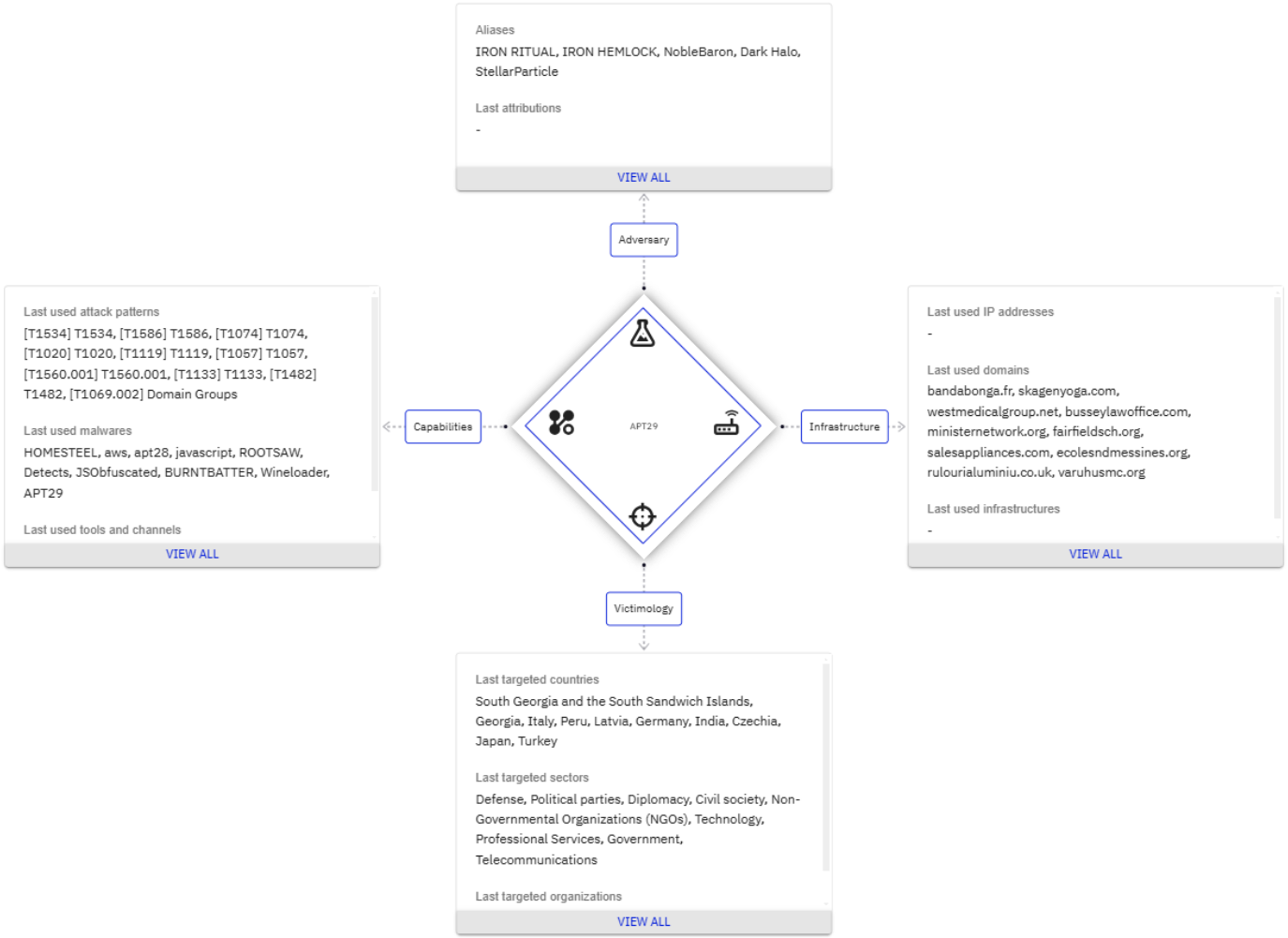
Extended Session - Hypothesis based Threat Hunting

★ Rank 32

APT 29

Summary of Actor:APT 29, also known as Cozy Bear or The Dukes, is a sophisticated cyber espionage group believed to be associated with the Russian intelligence community. They are known for targeting government, diplomatic, think-tank, and healthcare sectors. APT 29 is highly skilled in maintaining a low profile while conducting its operations.

General Features:APT 29 typically uses spear-phishing attacks, custom malware, and exploits to gain access to targeted networks. They are known for their patience and ability to remain undetected for extended periods. The group employs advanced evasion techniques and sophisticated malware to achieve its objectives.

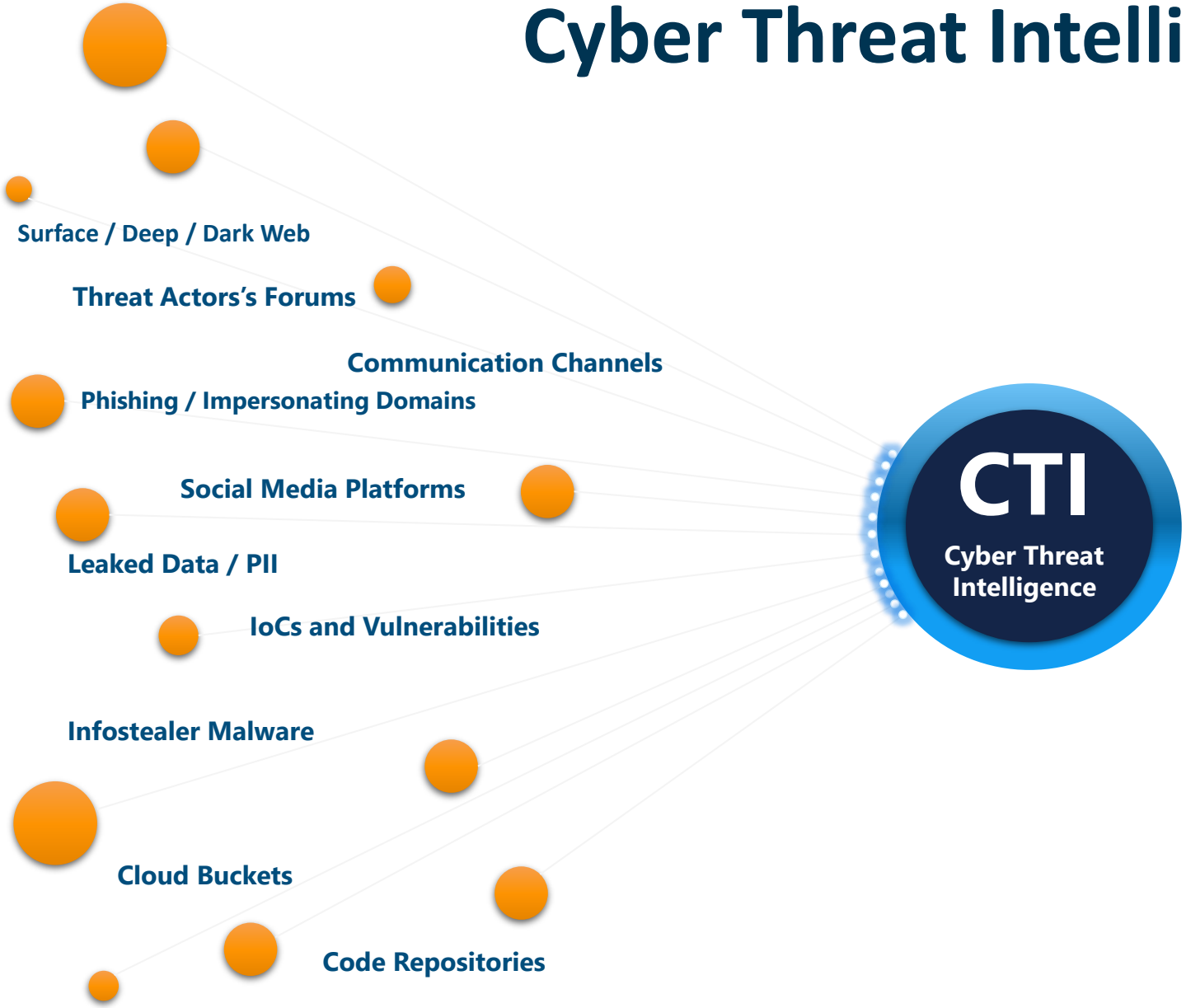


Threat Assessement	Threat Actor, Campaign, Industry/ Country Vertical	Adversary
Diamond Model	Intel on Campaign	Infrastructure: Server, IP, Domain
	Threat Actor's TTP	Capability: Malware, Exploits
	Victimology: Industry, Country	
Response	Hunt & Remove Malware	
	Block IOCs	
	Create Detection	

Cyber Threat Intelligence

Shed some Light to the Darkness

Cyber Threat Intelligence (CTI)



- Attack Surface Management (ASM)
- Digital Risk Protection (DRP)
- Brand Protection
- Threat Landscape Monitoring
- Supply Chain Monitoring
- Takedown Services
- Real-time Infostealer Malware Detection

Cyber Threat Intelligence (CTI)

Threat intelligence enriched with Brand Protection, Digital Risk Protection, External Attack Surface Management, and Threat Landscape Monitoring.

Elevate your company’s security with our false-positive free, actionable, and contextualized threat intelligence service, designed to enhance your SOC team's performance.

- Real-time Infostealer Detection
- Supply Chain Intelligence
- Takedown Services

Cyber Threat Intelligence (CTI)

External Attack Surface Management

Detect unauthorized access points and identify potential vulnerabilities before they are exploited.

- Vulnerabilities / Weaknesses
- Open Ports

Brand Protection

Continuously monitor for phishing attacks and identify impersonating domains before used in phishing attacks.

- Impersonating domains
- VIP & Executive Impersonation

Digital Risk Protection

Detect your company data and employee credentials leaked on the dark web.

- Leaked Credentials / PII
- Pastebin Sites
- Cloud Buckets
- Code Repositories

Takedowns Service

Take down malicious domains and fraudulent social media accounts before they are used in social engineering attacks.

- Impersonating Domain
- Impersonating Social Media Accounts

Threat Landscape Monitoring

Actively monitor and evaluate your country and industry verticals for ongoing and future threats.

- Threat Actors / APT
- Malware / Vulnerability
- Country / Industry Verticals
- Global Trends

Supply Chain Intelligence

Continuously monitor your supply chain for potential breaches and protect your business against attacks originating from third-parties.

- Leaked Data
- Attacks
- Ransomware

Infostealer Malware Detection

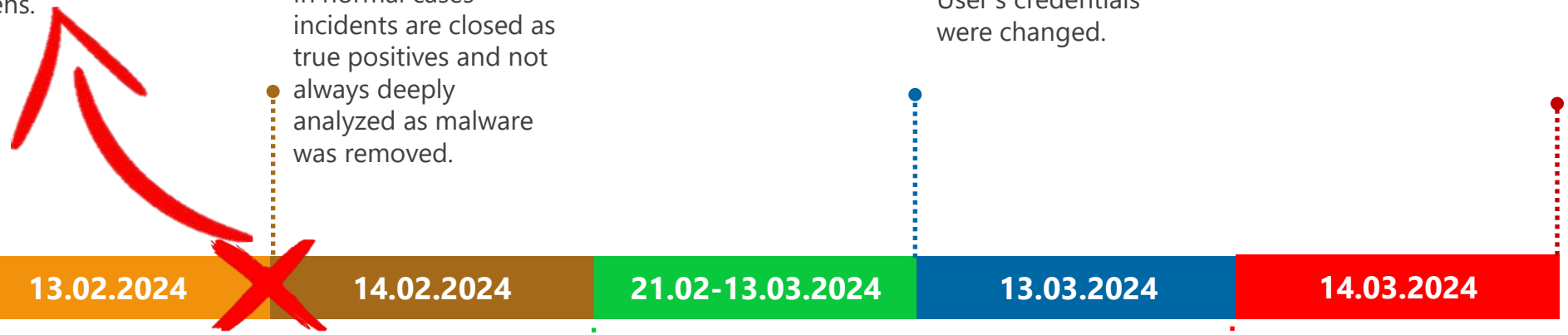
Detect infections from Infostealer malware preventing your employee's credentials and sessions being stolen, enabled to bypass security measures and used in account takeover (ATO) attacks.

- Host infection
- Malware Family
- Private & Company Credentials
- Web Cookie Sessions

Example Infostealer Incident Timeline Use Case

Cyber Threat Intel Service

This is where the incident chain would've stopped with the new Cyber Threat Intelligence Service because of knowledge about stolen cookies/tokens.



Incident creation

User downloaded an HTA file which was detected as malware. The incident was generated at 11:08 AM CEST with events starting at 11:05. The Malware was automatically remediated by MDE.

Incident closure

In normal cases incidents are closed as true positives and not always deeply analyzed as malware was removed.

Suspicious sign-ins

Successful sign-ins from Benin, Ivory Coast, Morocco, Germany, Algeria, United States, Jordan, and Switzerland

Password change

User's credentials were changed.

Further incidents

Some sign-ins failed due to incorrect password. But still successful service usage from random countries.

Sessions revoked

Entra ID Sessions revoked, and user Informed to revoke session in all systems he use.

Timeline with Threat Intel Service

27.03.2024

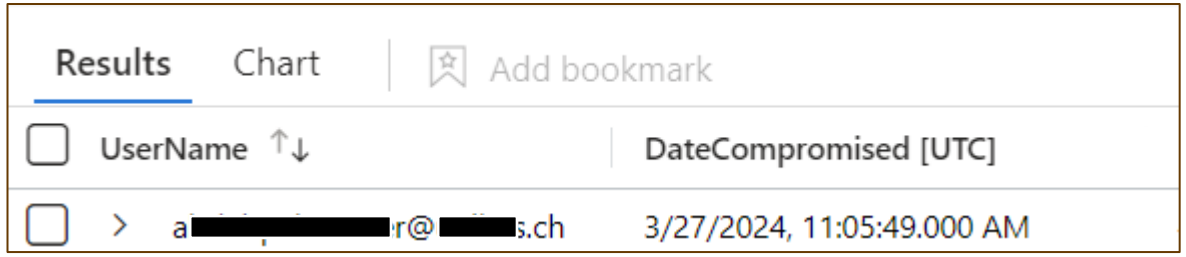
Credentials leaked

User credentials were found in a database with the data regarding compromise matching the incident information: 27.03.2024 at 11:05 CEST

Incident creation

User downloaded an HTA file which compromised the user and ran an infostealer at 11:05 AM CEST and triggered a severity High incident at 11:08

- baseVISION Threat Intel team keeps an **up-to-date table of credentials stolen by infostealers**
- Custom analytic rules monitor for changes in the table to alert the analysts for compromised accounts:



Timeline with Threat Intel Service

baseVISION

Credentials leaked

User credentials were found in a database with the data regarding compromise matching the incident information: 27.03.2024 at 11:05 CEST

Actionable Intelligence

The analyst would ascertain the breach and exfiltration of data and would have provided **Recommendation Actions** to customer

27.03.2024

Incident creation

User downloaded an HTA file which compromised the user and ran an infostealer at 11:05 AM CEST and triggered a severity High incident at 11:08

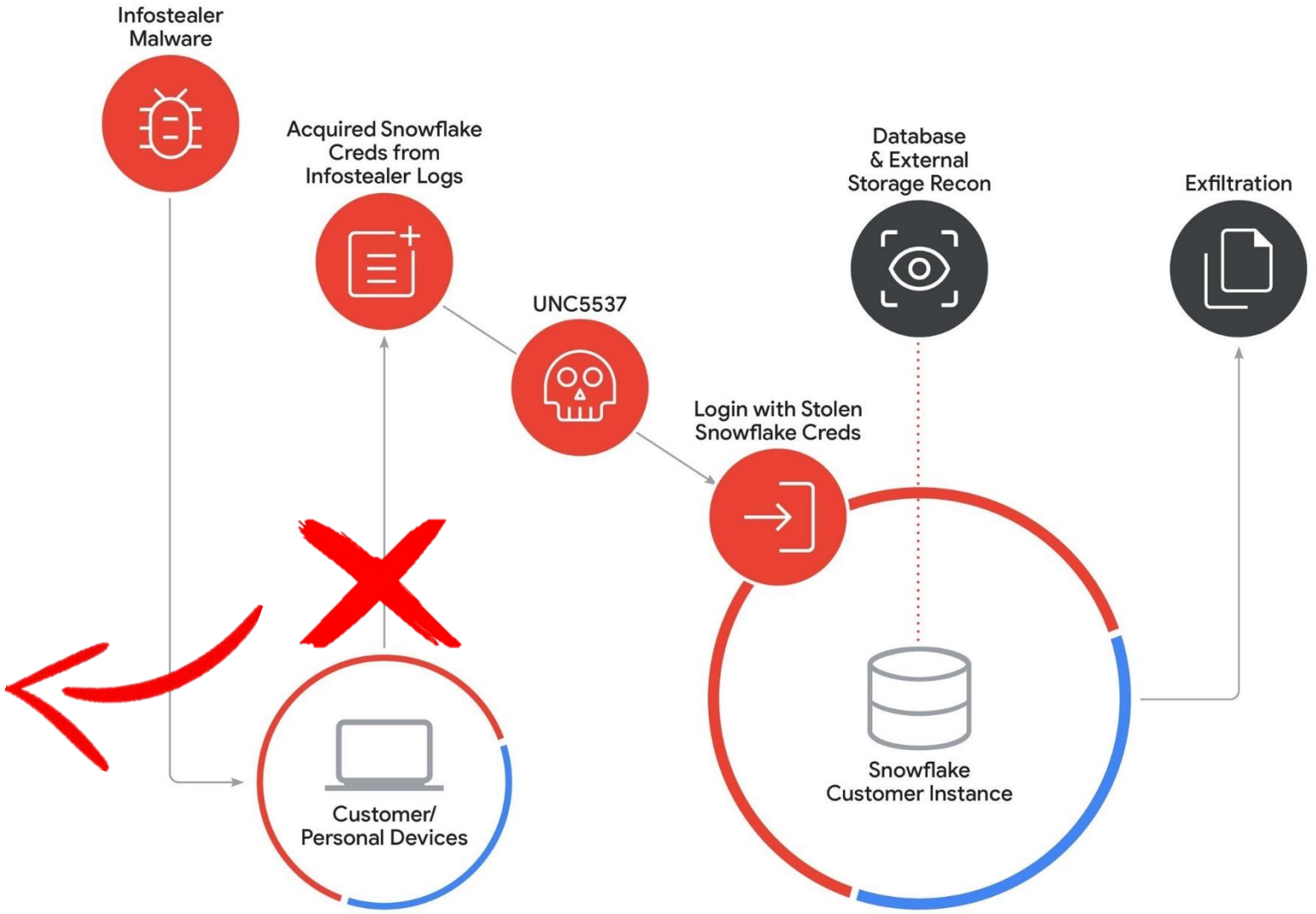
Incident Escalation and Remediation

On the same day as the upload of the credentials, a new High Incident would have triggered alerting the analysts about the credentials and the need for **Immediate Reaction**

Snowflake & CTI + Supply Chain Intelligence

Snowflake Attack Timeline

"To date, Mandiant and Snowflake have notified approximately 165 potentially exposed organizations", the report says.



Cyber Threat Intel & Supply Chain Intelligence

A proper CTI service and Supply Chain Intel service monitoring Real-time Infostealer Infections would have spotted the incident directly at infection. Customer would have been alerted about their third-party being infected.

Source: [UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion | Google Cloud Blog]

XTI&H - Simple and customizable according to your needs

Extended Threat intelligence & Hunting

Threat Intel Feeds

Access to two curated premium feeds:
- Detect
- Protect - with only high-confidence IOC's

Feed sources:
- baseVISION TI
- SOCRadar TI
- BACS TI (Only if Member of CS HUB)
- 140 Open-Source Feeds

Integration:
- Microsoft Sentinel
- Microsoft Defender XDR
- Third Party allowed (Support based on T&M)

Proactive Threat Hunting

Incident and Intelligence-based Hunting
- Leveraging incidents across our client base
- Leveraging IOA and IOC feeds to perform hunting for known malicious threats that might be lurking within the perimeter

Tactics, Techniques, and Procedures-based Hunting
- Standard Hunting Session: Identifying the detection gaps against the MITRE ATT&CK matrix and hunting for evidence of infection (approx. 4h)
- Extended Hunting Session: Hypothesis & Diamond model-based to generate new data points, intelligence insights, and hunting hypotheses. (approx. 8h)

Special Hunting 4 hours inclusive
- Research based on request

Cyber Threat Intel

Brand protection including Fraud Protection and VIP Protection
- Domain and Social Media Account Takedowns

Monitoring
- Supply Chain
- Real time Infostealer and Malware
- Attack Surface
- Threat Landscape
- Threat Event
- Breached/Leaked Credentials/Data (Deep/Dark Web)

Deep/Dark Web Research Jobs
Quarterly Meeting / Digital Report