CYBER THREAT INTELLIGENCE USE CASES

Combining: Theory, Technology and Experience

Jurgen Visser

```
srcip="172.16.160.210" user="root"
caller="root" reason="Too many failures
from client IP, still blocked for 537
seconds"
<54>Jul 5 17:17:43 SymantecServer SEP-
PROD: Virus found,IP Address:
10.235.237.89,Computer name:
A41021,Source: Real Time Scan,Risk name:
Backdoor.IRCBot!win32
<177>Jul  5 14:18:53 SourceFire
snort[10340]: [1:2007933:3] ET EXPLOIT
Microsoft Office Memory Corruption
Vulnerability (CVE-2017-11882)
[Classification: Microsoft Application
Attack] [Priority: 2]: {TCP}
72.246.97.42:80 -> 10.12.1.140:1629
<54>Jul 5 14:05:55 SymantecServer SEP-
PROD: Virus found,IP Address:
10.11.8.78,Computer name:
A372d759,Source: Scheduled Scan,Risk
name: W97M.Melissa.A
<30>Jul 5 19:22-19:16:27 aua[4983]:
id="3005" severity="warn" sys="System"
sub="auth" name="Authentication failed"
srcip="172.16.160.210" user="sysadmin"
caller="root" reason="Too many failures
from client IP, still blocked for 517
seconds"
```

Jurgen Visser

Cyber Defense Specialist

Cyber Defense Specialist passionate about analyzing cyber security risks and strategizing, architecting, building, maturing them into enterprise level cyber security initiatives.

- 3x Threat Intelligence Certified: **GCTI, CTIA, CRTIA**
- Information Security Blogger at **www.correlatedsecurity.com**

Bottom Line Up Front (BLUF)

1. The Cyber Threat Intelligence (CTI) program helps **Senior Business leaders make informed** forward-leaning strategic, operational, and tactical **decisions** on **existing, emerging or predicted cyber threats** to the organization.

2. Cyber Threat Intelligence works best **on top of a already functioning security program** which sits on top of a mature IT organization

Dimension	★ Beginner CTI Program	★★ Intermediate CTI Program	★★★ Advanced CTI Program
Budget	**Low** (below 1-10k USD +/-) Yearly	**Medium** (50k-150k USD) Yearly	**High** (200k-400k USD) Yearly
People	1x Junior CTI analyst	1x Junior CTI analyst 1x Mid-level CTI Lead	1x Junior CTI analyst 1x Mid-level CTI analyst 1x Senior CTI Lead
Products	**CTI USE CASE 0:** Keyword Repository **CTI USE CASE 1:** Intelligence Platform Alerts **CTI USE CASE 2:** Cyber Threat Intelligence Feeds **CTI USE CASE 3:** Vulnerability Intelligence **CTI USE CASE 4:** Infostealer monitoring	**CTI USE CASE 0:** Keyword Repository **CTI USE CASE 1:** Intelligence Platform Alerts **CTI USE CASE 2:** Cyber Threat Intelligence Feeds **CTI USE CASE 3:** Vulnerability Intelligence **CTI USE CASE 4:** Infostealer monitoring **CTI USE CASE 5:** Daily CTI Report **CTI USE CASE 6:** Phishing Intelligence **CTI USE CASE 7:** Threat Hunting	**CTI USE CASE 0:** Keyword Repository **CTI USE CASE 1:** Intelligence Platform Alerts **CTI USE CASE 2:** Cyber Threat Intelligence Feeds **CTI USE CASE 3:** Vulnerability Intelligence **CTI USE CASE 4:** Infostealer monitoring **CTI USE CASE 5:** Daily CTI Report **CTI USE CASE 6:** Phishing Intelligence **CTI USE CASE 7:** Threat Hunting **CTI USE CASE 8:** Internal Strategic Intelligence Report **CTI USE CASE 9:** External Strategic Intelligence Report **CTI USE CASE 10:** Threat Intelligence Sharing

THEORY

Cyber Threat Intelligence: Foundations

1. Cyber Threat Intelligence (CTI) is defined as the **collection and analysis of information about threats and adversaries**. Drawing patterns that **provide an ability to make knowledgeable decisions** for preparedness, prevention, and response actions against various cyber-attacks.

2. The Cyber Threat Intelligence (CTI) program helps **Senior Business leaders make informed** forward-leaning strategic, operational, and tactical **decisions** on **existing, emerging or predicted cyber threats** to the organization.

Cyber Threat Intelligence: Concepts

Actionable Threat Intelligence =
Objectively written + Timely delivery + Accurate facts + Actionable Recommendations

Threat Actor Campaign =
Actor Name + Observed Attacks/Intrusions + Actor TTP's + Key indicators (IOC's or IoA's)

Cyber Threat Intelligence: Distinctions

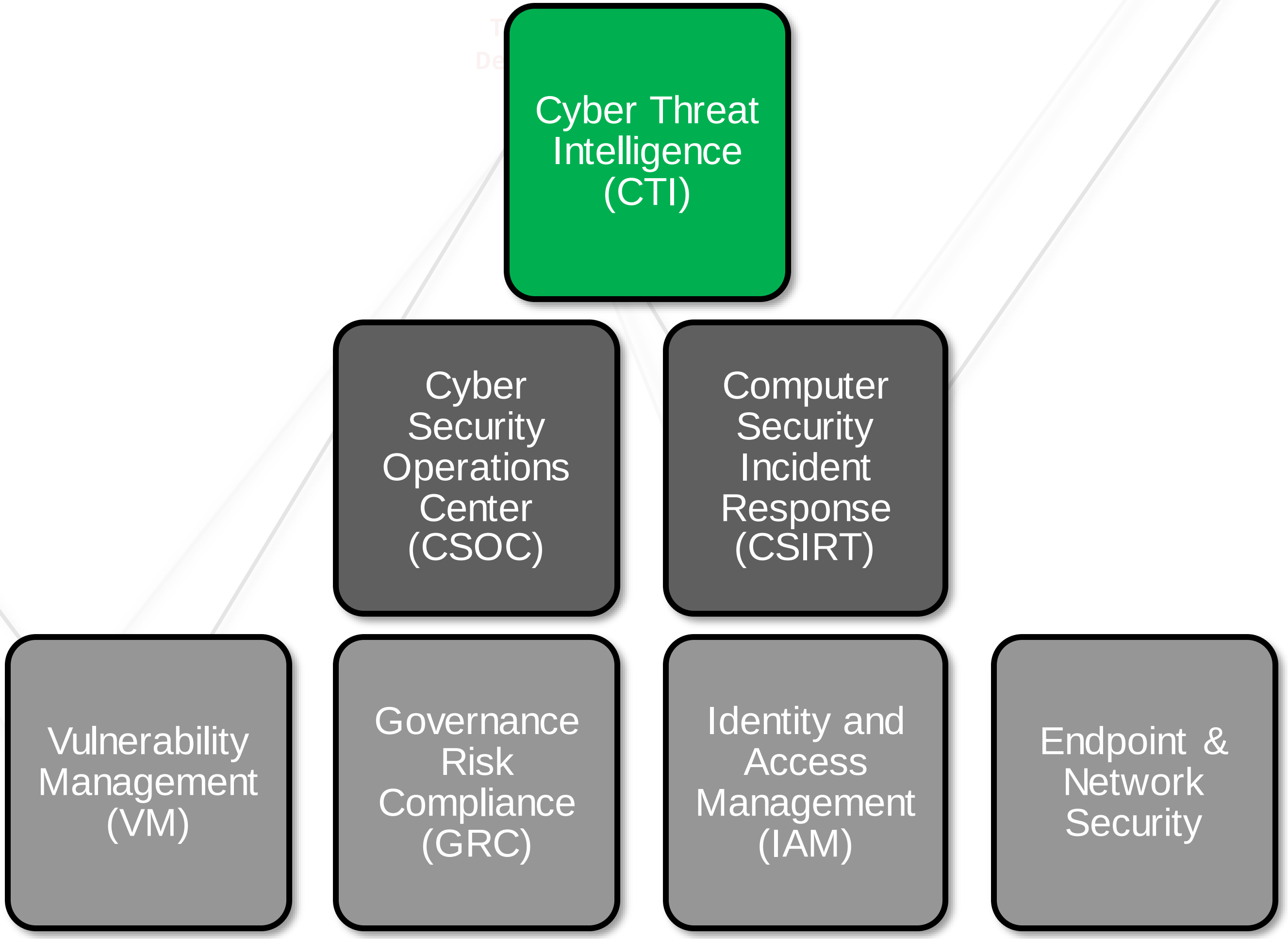
1. **Types of Threat intelligence:** Strategic Threat Intelligence, Tactical Threat Intelligence, Operational Threat Intelligence, Technical Threat Intelligence

2. **Types of Intelligence Sources:** Open-Source Intelligence (OSINT), Human Intelligence (HUMINT), Cyber Counterintelligence (CCI), Technical Intelligence (TECHINT), Social Media Intelligence (SOCMINT)

Cyber Threat Intelligence: Requirements

1. Cyber Threat Intelligence works best **on top of a already functioning security program** which sits on top of a mature IT organization

2. Cyber Threat Intelligence Requirements need to come **top-down NOT bottom-up.**



Cyber Threat Intelligence (CTI)

Cyber Security Operations Center (CSOC)

Computer Security Incident Response (CSIRT)

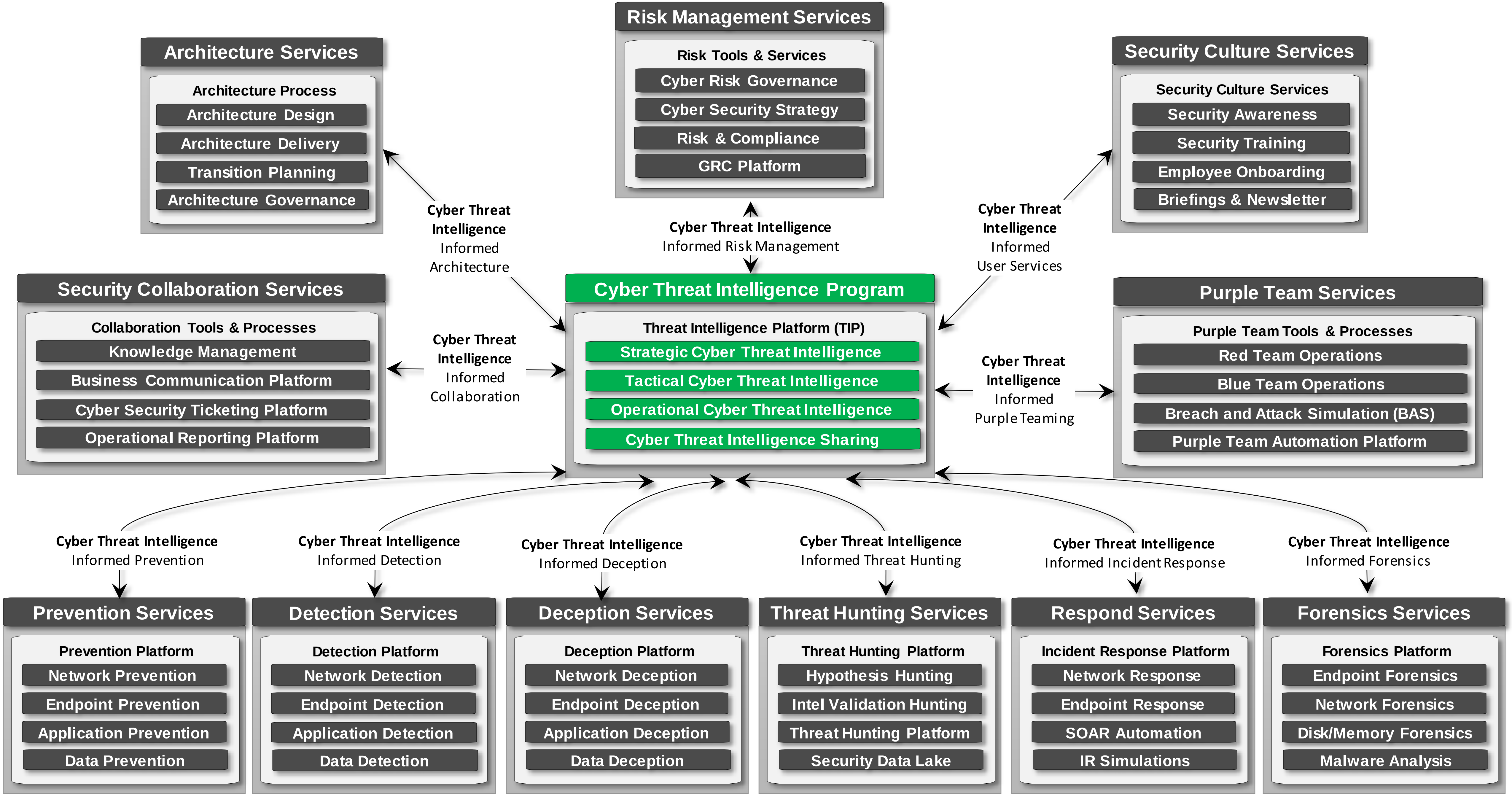
Vulnerability Management (VM)

Governance Risk Compliance (GRC)

Identity and Access Management (IAM)

Endpoint & Network Security

Cyber Threat Intelligence Informed Cyber Security Services



Risk Management Services

Risk Tools & Services
- Cyber Risk Governance
- Cyber Security Strategy
- Risk & Compliance
- GRC Platform

Architecture Services

Architecture Process
- Architecture Design
- Architecture Delivery
- Transition Planning
- Architecture Governance

Security Culture Services

Security Culture Services
- Security Awareness
- Security Training
- Employee Onboarding
- Briefings & Newsletter

Cyber Threat Intelligence Informed Architecture

Cyber Threat Intelligence Informed Risk Management

Cyber Threat Intelligence Informed User Services

Security Collaboration Services

Collaboration Tools & Processes
- Knowledge Management
- Business Communication Platform
- Cyber Security Ticketing Platform
- Operational Reporting Platform

Cyber Threat Intelligence Informed Collaboration

Cyber Threat Intelligence Program

Threat Intelligence Platform (TIP)
- Strategic Cyber Threat Intelligence
- Tactical Cyber Threat Intelligence
- Operational Cyber Threat Intelligence
- Cyber Threat Intelligence Sharing

Cyber Threat Intelligence Informed Purple Teaming

Purple Team Services

Purple Team Tools & Processes
- Red Team Operations
- Blue Team Operations
- Breach and Attack Simulation (BAS)
- Purple Team Automation Platform

Cyber Threat Intelligence Informed Prevention

Cyber Threat Intelligence Informed Detection

Cyber Threat Intelligence Informed Deception

Cyber Threat Intelligence Informed Threat Hunting

Cyber Threat Intelligence Informed Incident Response

Cyber Threat Intelligence Informed Forensics

Prevention Services

Prevention Platform
- Network Prevention
- Endpoint Prevention
- Application Prevention
- Data Prevention

Detection Services

Detection Platform
- Network Detection
- Endpoint Detection
- Application Detection
- Data Detection

Deception Services

Deception Platform
- Network Deception
- Endpoint Deception
- Application Deception
- Data Deception

Threat Hunting Services

Threat Hunting Platform
- Hypothesis Hunting
- Intel Validation Hunting
- Threat Hunting Platform
- Security Data Lake

Respond Services

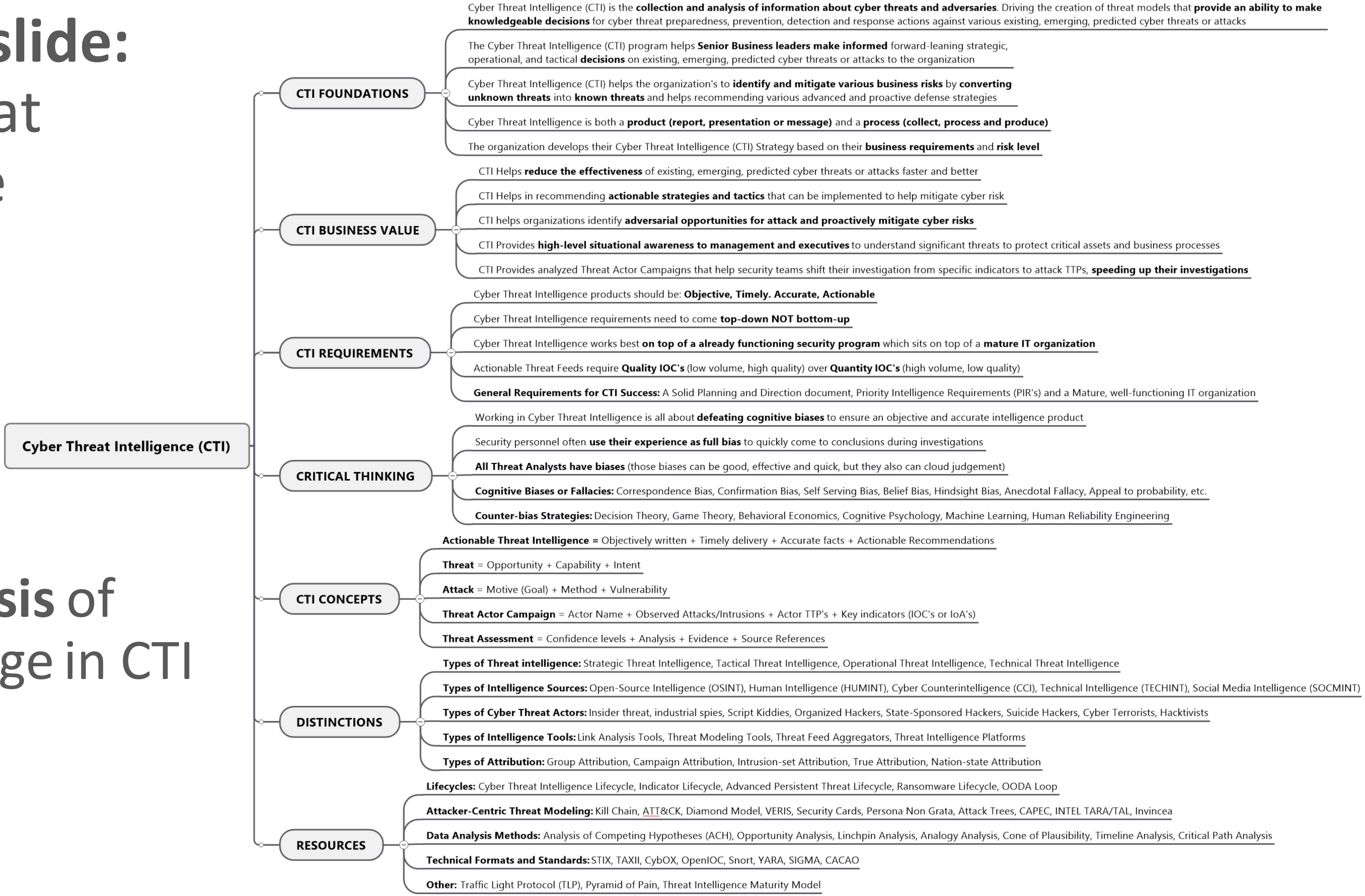
Incident Response Platform
- Network Response
- Endpoint Response
- SOAR Automation
- IR Simulations

Forensics Services

Forensics Platform
- Endpoint Forensics
- Network Forensics
- Disk/Memory Forensics
- Malware Analysis

Reference slide: Cyber Threat Intelligence MindMap

80/20 Analysis of key knowledge in CTI



Cyber Threat Intelligence (CTI)

- **CTI FOUNDATIONS**
  - Cyber Threat Intelligence (CTI) is the **collection and analysis of information about cyber threats and adversaries**. Driving the creation of threat models that **provide an ability to make knowledgeable decisions** for cyber threat preparedness, prevention, detection and response actions against various existing, emerging, predicted cyber threats or attacks
  - The Cyber Threat Intelligence (CTI) program helps **Senior Business leaders make informed** forward-leaning strategic, operational, and tactical **decisions** on existing, emerging, predicted cyber threats or attacks to the organization
  - Cyber Threat Intelligence (CTI) helps the organization's to **identify and mitigate various business risks** by **converting unknown threats** into **known threats** and helps recommending various advanced and proactive defense strategies
  - Cyber Threat Intelligence is both a **product (report, presentation or message)** and a **process (collect, process and produce)**
  - The organization develops their Cyber Threat Intelligence (CTI) Strategy based on their **business requirements** and **risk level**
- **CTI BUSINESS VALUE**
  - CTI Helps **reduce the effectiveness** of existing, emerging, predicted cyber threats or attacks faster and better
  - CTI Helps in recommending **actionable strategies and tactics** that can be implemented to help mitigate cyber risk
  - CTI helps organizations identify **adversarial opportunities for attack and proactively mitigate cyber risks**
  - CTI Provides **high-level situational awareness to management and executives** to understand significant threats to protect critical assets and business processes
  - CTI Provides analyzed Threat Actor Campaigns that help security teams shift their investigation from specific indicators to attack TTPs, **speeding up their investigations**
- **CTI REQUIREMENTS**
  - Cyber Threat Intelligence products should be: **Objective, Timely. Accurate, Actionable**
  - Cyber Threat Intelligence requirements need to come **top-down NOT bottom-up**
  - Cyber Threat Intelligence works best **on top of a already functioning security program** which sits on top of a **mature IT organization**
  - Actionable Threat Feeds require **Quality IOC's** (low volume, high quality) over **Quantity IOC's** (high volume, low quality)
  - **General Requirements for CTI Success:** A Solid Planning and Direction document, Priority Intelligence Requirements (PIR's) and a Mature, well-functioning IT organization
- **CRITICAL THINKING**
  - Working in Cyber Threat Intelligence is all about **defeating cognitive biases** to ensure an objective and accurate intelligence product
  - Security personnel often **use their experience as full bias** to quickly come to conclusions during investigations
  - **All Threat Analysts have biases** (those biases can be good, effective and quick, but they also can cloud judgement)
  - **Cognitive Biases or Fallacies:** Correspondence Bias, Confirmation Bias, Self Serving Bias, Belief Bias, Hindsight Bias, Anecdotal Fallacy, Appeal to probability, etc.
  - **Counter-bias Strategies:** Decision Theory, Game Theory, Behavioral Economics, Cognitive Psychology, Machine Learning, Human Reliability Engineering
- **CTI CONCEPTS**
  - **Actionable Threat Intelligence =** Objectively written + Timely delivery + Accurate facts + Actionable Recommendations
  - **Threat** = Opportunity + Capability + Intent
  - **Attack** = Motive (Goal) + Method + Vulnerability
  - **Threat Actor Campaign** = Actor Name + Observed Attacks/Intrusions + Actor TTP's + Key indicators (IOC's or IoA's)
  - **Threat Assessment** = Confidence levels + Analysis + Evidence + Source References
- **DISTINCTIONS**
  - **Types of Threat intelligence:** Strategic Threat Intelligence, Tactical Threat Intelligence, Operational Threat Intelligence, Technical Threat Intelligence
  - **Types of Intelligence Sources:** Open-Source Intelligence (OSINT), Human Intelligence (HUMINT), Cyber Counterintelligence (CCI), Technical Intelligence (TECHINT), Social Media Intelligence (SOCMINT)
  - **Types of Cyber Threat Actors:** Insider threat, industrial spies, Script Kiddies, Organized Hackers, State-Sponsored Hackers, Suicide Hackers, Cyber Terrorists, Hacktivists
  - **Types of Intelligence Tools:** Link Analysis Tools, Threat Modeling Tools, Threat Feed Aggregators, Threat Intelligence Platforms
  - **Types of Attribution:** Group Attribution, Campaign Attribution, Intrusion-set Attribution, True Attribution, Nation-state Attribution
- **RESOURCES**
  - **Lifecycles:** Cyber Threat Intelligence Lifecycle, Indicator Lifecycle, Advanced Persistent Threat Lifecycle, Ransomware Lifecycle, OODA Loop
  - **Attacker-Centric Threat Modeling:** Kill Chain, ATT&CK, Diamond Model, VERIS, Security Cards, Persona Non Grata, Attack Trees, CAPEC, INTEL TARA/TAL, Invincea
  - **Data Analysis Methods:** Analysis of Competing Hypotheses (ACH), Opportunity Analysis, Linchpin Analysis, Analogy Analysis, Cone of Plausibility, Timeline Analysis, Critical Path Analysis
  - **Technical Formats and Standards:** STIX, TAXII, CybOX, OpenIOC, Snort, YARA, SIGMA, CACAO
  - **Other:** Traffic Light Protocol (TLP), Pyramid of Pain, Threat Intelligence Maturity Model

TECHNOLOGY

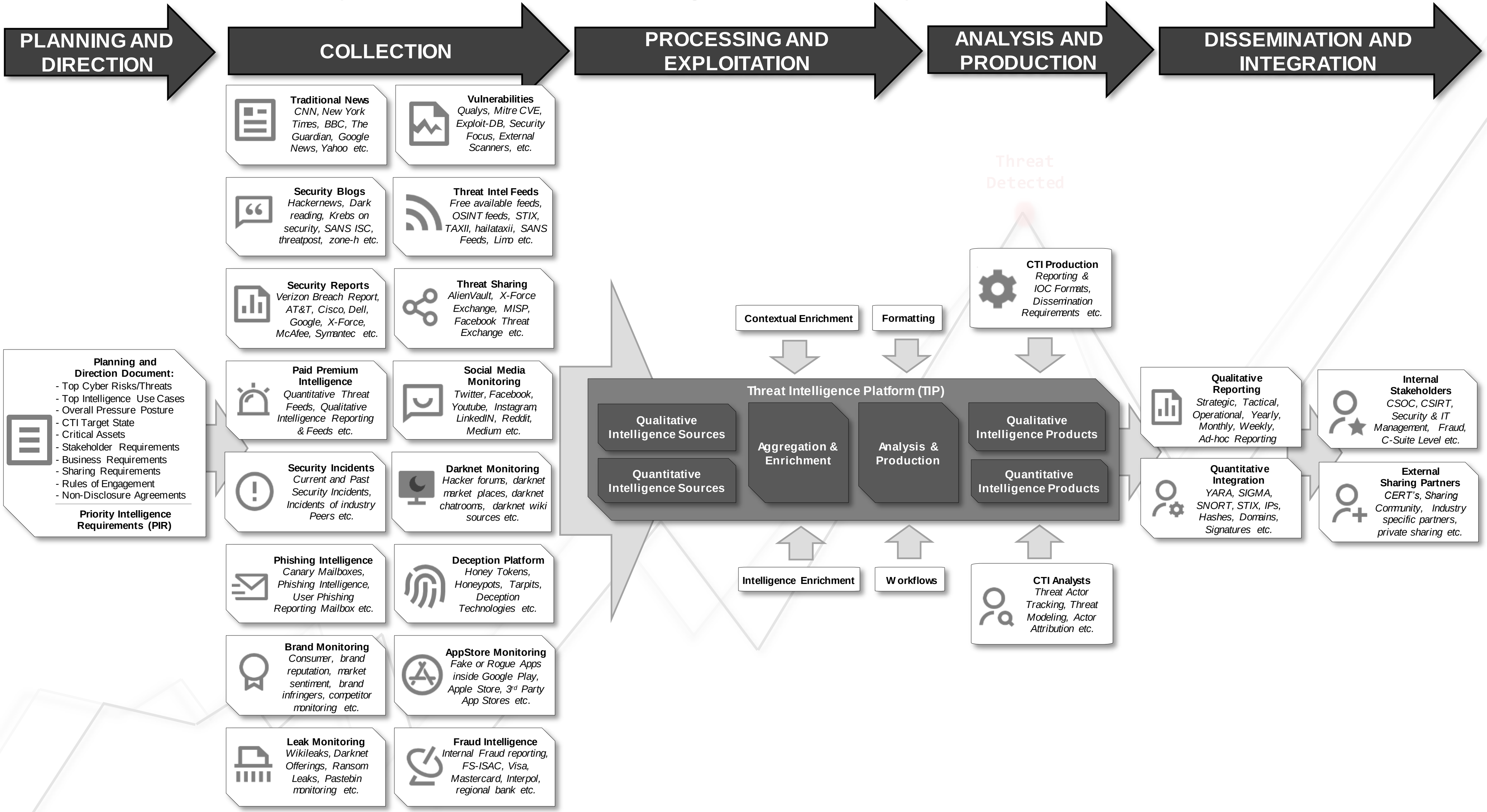
CTI Technological Challenges

1. The CTI vendor industry is in an **early maturity stage** where there are many **different vendors** but all with **different collection scopes**.

2. There is **No single vendor** that does everything on all fronts well.

- OSINT only **vs.** Darkweb only
- APT Focus **vs.** Cybercrime focus
- Threat Enrichment API **vs.** Threat feeds and feed aggregation
- Very specific targeted collection source **vs.** wide array of collection sources
- Where you can put in keywords **vs.** rigid pre-determined collection scope.

Cyber Threat Intelligence Lifecycle Overview



PLANNING AND DIRECTION

COLLECTION

PROCESSING AND EXPLOITATION

ANALYSIS AND PRODUCTION

DISSEMINATION AND INTEGRATION

Planning and Direction Document:
- Top Cyber Risks/Threats
- Top Intelligence Use Cases
- Overall Pressure Posture
- CTI Target State
- Critical Assets
- Stakeholder Requirements
- Business Requirements
- Sharing Requirements
- Rules of Engagement
- Non-Disclosure Agreements

Priority Intelligence Requirements (PIR)

Traditional News *CNN, New York Times, BBC, The Guardian, Google News, Yahoo etc.*

Vulnerabilities *Qualys, Mitre CVE, Exploit-DB, Security Focus, External Scanners, etc.*

Security Blogs *Hackernews, Dark reading, Krebs on security, SANS ISC, threatpost, zone-h etc.*

Threat Intel Feeds *Free available feeds, OSINT feeds, STIX, TAXII, hailataxii, SANS Feeds, Limo etc.*

Security Reports *Verizon Breach Report, AT&T, Cisco, Dell, Google, X-Force, McAfee, Symantec etc.*

Threat Sharing *AlienVault, X-Force Exchange, MISP, Facebook Threat Exchange etc.*

Paid Premium Intelligence *Quantitative Threat Feeds, Qualitative Intelligence Reporting & Feeds etc.*

Social Media Monitoring *Twitter, Facebook, Youtube, Instagram, LinkedIN, Reddit, Medium etc.*

Security Incidents *Current and Past Security Incidents, Incidents of industry Peers etc.*

Darknet Monitoring *Hacker forums, darknet market places, darknet chatrooms, darknet wiki sources etc.*

Phishing Intelligence *Canary Mailboxes, Phishing Intelligence, User Phishing Reporting Mailbox etc.*

Deception Platform *Honey Tokens, Honeypots, Tarpits, Deception Technologies etc.*

Brand Monitoring *Consumer, brand reputation, market sentiment, brand infringers, competitor monitoring etc.*

AppStore Monitoring *Fake or Rogue Apps inside Google Play, Apple Store, 3rd Party App Stores etc.*

Leak Monitoring *Wikileaks, Darknet Offerings, Ransom Leaks, Pastebin monitoring etc.*

Fraud Intelligence *Internal Fraud reporting, FS-ISAC, Visa, Mastercard, Interpol, regional bank etc.*

Contextual Enrichment

Formatting

CTI Production *Reporting & IOC Formats, Dissemination Requirements etc.*

Threat Intelligence Platform (TIP)

Qualitative Intelligence Sources

Quantitative Intelligence Sources

Aggregation & Enrichment

Analysis & Production

Qualitative Intelligence Products

Quantitative Intelligence Products

Intelligence Enrichment

Workflows

CTI Analysts *Threat Actor Tracking, Threat Modeling, Actor Attribution etc.*

Qualitative Reporting *Strategic, Tactical, Operational, Yearly, Monthly, Weekly, Ad-hoc Reporting*

Quantitative Integration *YARA, SIGMA, SNORT, STIX, IPs, Hashes, Domains, Signatures etc.*

Internal Stakeholders *CSOC, CSIRT, Security & IT Management, Fraud, C-Suite Level etc.*

External Sharing Partners *CERT's, Sharing Community, Industry specific partners, private sharing etc.*

Key Take-Aways

1. Expect **intelligence bias** from the intelligence firm country's origin.

2. Product categories like: **Brand Protection, Domain Management, Attack Surface Management, SOAR, Social Media Platforms, Bug Bounty Platforms** can be used for CTI use cases

3. **Defining the Intelligence product first** and match the CTI platform against it.

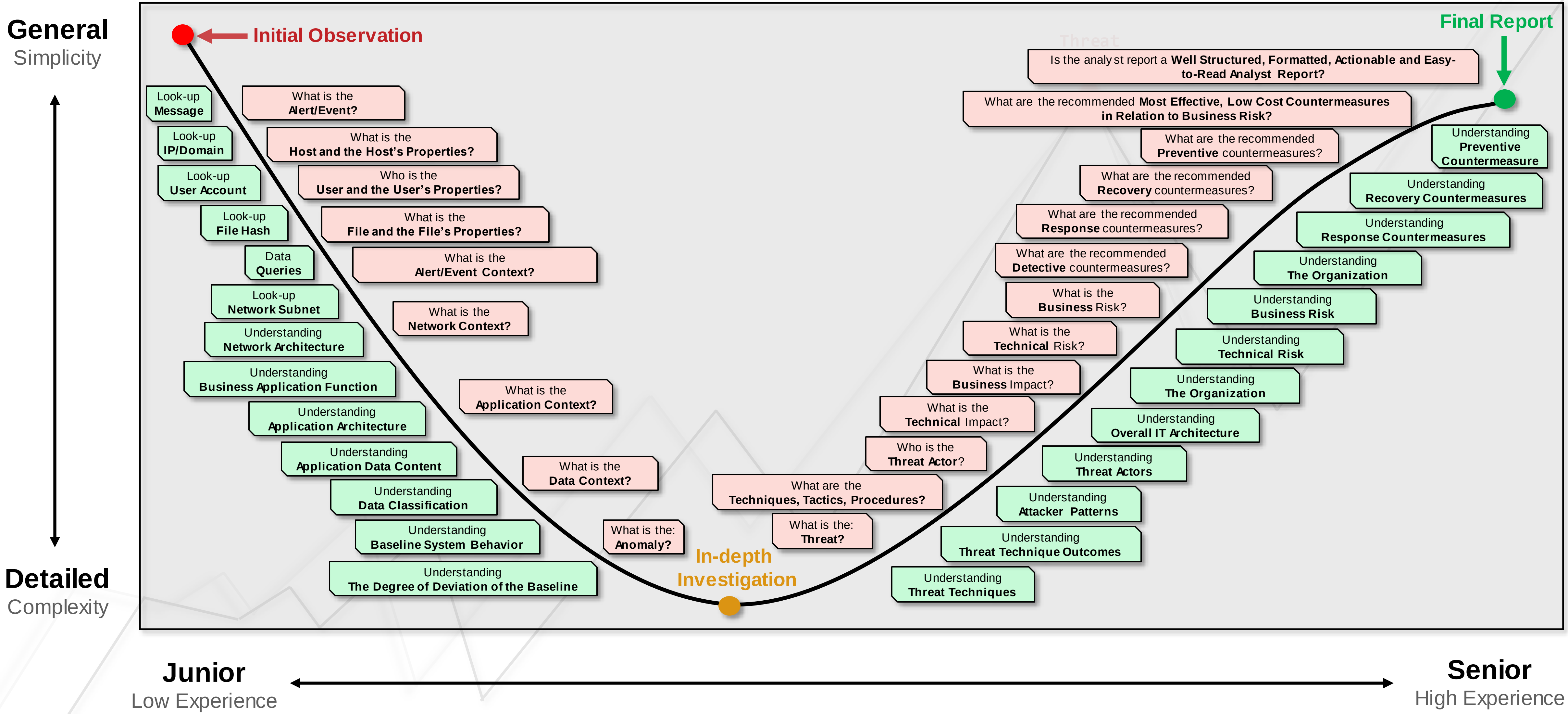
EXPERIENCE

Theory + Experience = Recommendation

Theory	Experience	Recommendation
Cyber Threat Intelligence Requirements need to come **top-down NOT bottom-up.**	Most organizations **won't tell you want they want or need.**	📋 List **mock-up CTI products** and ask stakeholders if they see value in it.
Start with **Priority Intelligence Requirements (PIR)** first.	Vendor requesting for a list of **domains and company brands**.	🧩 **Map** the mock-up CTI products **against the technology platforms**
Tracking threat actors is a very elaborate process that requires in depth details	Only a **few threat actors** are truly relevant, after modeling them tracking them is not hard.	👨‍💼 Once modelled, **do tracking of threat actors using detection rules** on CTI platforms.
Use any of the **15+ different threat modelling techniques** out there.	Only the main phases of **MITRE ATT&CK and Attack Cards** help.	📜 Use only the **MITRE ATT&CK main phases and Attack cards**.
Use elaborate threat actor threat modelling against **Mitre ATT&CK** to drive red teaming	Red Teams are more helped with **tools and entry points.**	🛠 Provide emerging **hack tool and vulnerability intelligence**.
Cyber threat intelligence is **only for cybersecurity purposes**	CTI lends itself to support **brand protection and Fraud as well**.	💰 Ask for additional budget from **Fraud and Branding team**.

Cyber Security Analyst Maturity Curve

*“A senior cyber security analyst should be able to reach the **simplicity at the far side of complexity** and to be able to communicate the cyber security risks, threats and related countermeasures **simply, effectively and actionable.**”*



General
Simplicity

Initial Observation

Look-up **Message**

What is the **Alert/Event?**

Look-up **IP/Domain**

What is the **Host and the Host’s Properties?**

Look-up **User Account**

Who is the **User and the User’s Properties?**

Look-up **File Hash**

What is the **File and the File’s Properties?**

Data **Queries**

What is the **Alert/Event Context?**

Look-up **Network Subnet**

What is the **Network Context?**

Understanding **Network Architecture**

Understanding **Business Application Function**

What is the **Application Context?**

Understanding **Application Architecture**

Understanding **Application Data Content**

What is the **Data Context?**

Understanding **Data Classification**

Understanding **Baseline System Behavior**

What is the: **Anomaly?**

Understanding **The Degree of Deviation of the Baseline**

In-depth Investigation

What is the: **Threat?**

What are the **Techniques, Tactics, Procedures?**

Understanding **Threat Techniques**

Who is the **Threat Actor**?

Understanding **Threat Technique Outcomes**

What is the **Technical** Impact?

Understanding **Attacker Patterns**

What is the **Business** Impact?

Understanding **Threat Actors**

What is the **Technical** Risk?

Understanding **Overall IT Architecture**

What is the **Business** Risk?

Understanding **The Organization**

What are the recommended **Detective** countermeasures?

Understanding **Technical Risk**

What are the recommended **Response** countermeasures?

Understanding **Business Risk**

What are the recommended **Recovery** countermeasures?

Understanding **The Organization**

What are the recommended **Preventive** countermeasures?

Understanding **Response Countermeasures**

Understanding **Recovery Countermeasures**

Understanding **Preventive Countermeasure**

What are the recommended **Most Effective, Low Cost Countermeasures in Relation to Business Risk?**

Threat

Is the analyst report a **Well Structured, Formatted, Actionable and Easy-to-Read Analyst Report?**

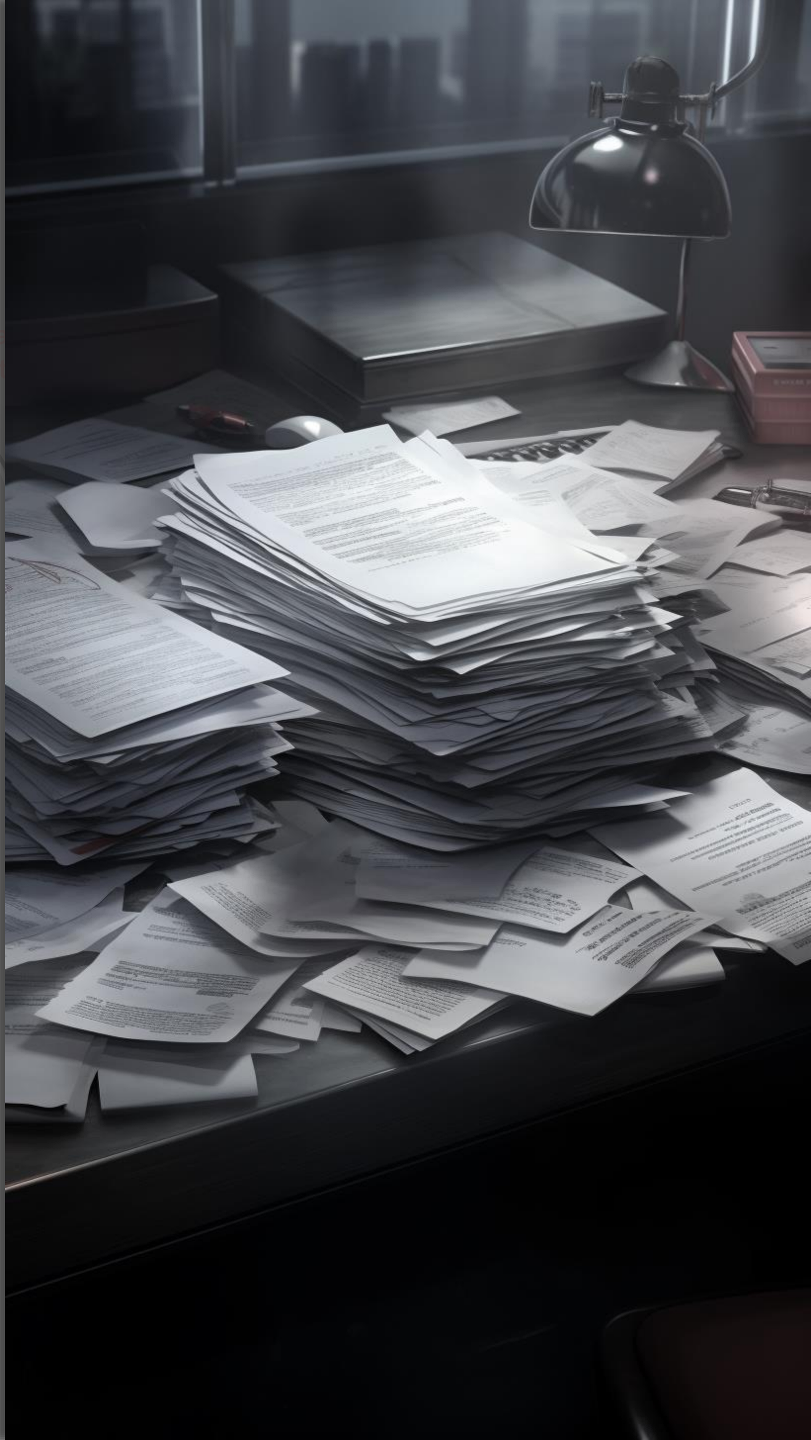
Final Report

Detailed
Complexity

Junior
Low Experience

Senior
High Experience

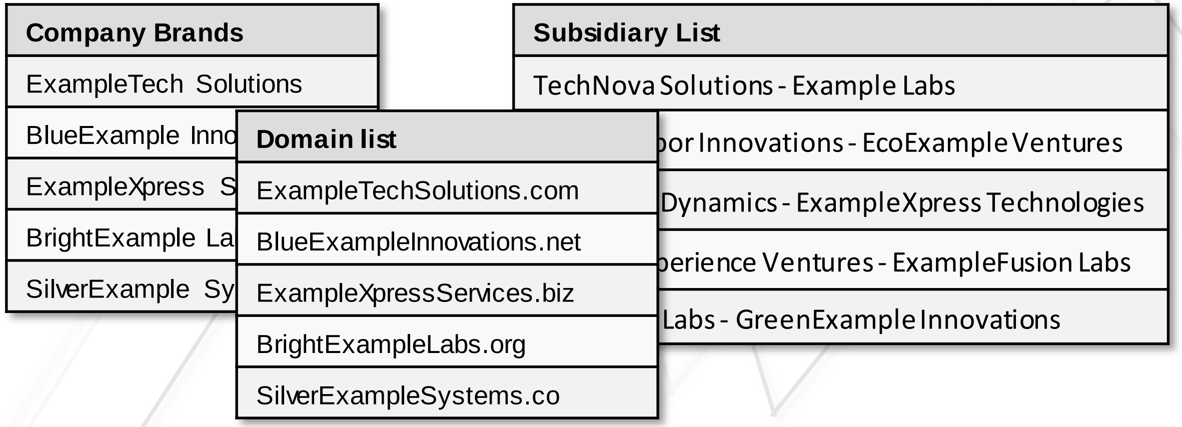
USE CASES



CTI USE CASE 0: Keyword Repository

Create a Series of Lists:

1. Company brand keywords
2. Domain list
3. Subsidiary list
4. Appstore apps list
5. VIP e-mail list
6. Public code repo list
7. Third party list
8. Used Application List



Company Brands
ExampleTech Solutions
BlueExample Inno
ExampleXpress S
BrightExample La
SilverExample Sy

Domain list
ExampleTechSolutions.com
BlueExampleInnovations.net
ExampleXpressServices.biz
BrightExampleLabs.org
SilverExampleSystems.co

Subsidiary List
TechNova Solutions - Example Labs
bor Innovations - EcoExample Ventures
Dynamics - ExampleXpress Technologies
berience Ventures - ExampleFusion Labs
Labs - GreenExample Innovations

Who can benefit from this?

1. The Cyber Threat Intelligence team

What can they do with it?

A. Breach dataset triage keywords

B. Domain look-a-like detection keywords

C. Darkweb mention detection keywords

D. Unsanctioned Appstore keywords

E. VIP infostealer detection keywords

F. Secrets leakage detection keywords

G. Third party breach keywords

H. Vulnerability Intelligence Triage

CTI USE CASE 1: Intelligence Platform Alerts

Take action intelligence platforms generated alerts

1. Look-a-like, fake or impersonation detections
    1. Domain look-a-like, fake or impersonation
    2. Social media look-a-like, fake or impersonation
    3. Mobile app store look-a-like, fake or impersonation
2. Keys or secrets leakage
    1. Code repo/container images secrets detected
    2. Copy paste websites (pastebin etc.)
    3. Specific web services that might contain secrets or keys
3. Attack surface management
    1. Ports opened up
    2. Vulnerable web services
    3. Cloud data bucket exposure
4. Darknet monitoring
    1. Activity involving the organization
5. 3rd Party breach monitoring
    1. Activity involving a third party organizations

Who can benefit from this?

1. Cyber Threat Intelligence Team
2. CSIRT Team
3. Takedown Team

What can they do with it?

A. Initiate a **takedown request** with the respective host (internal or external).

B. Kick-off security investigation to remediate with **CSIRT.**

CTI USE CASE 2: Cyber Threat Intelligence Feeds

Consolidated Feed of Threat Indicators of compromise (IOC):

A. **Risk score** helps filter out high false positive feed entries on the correlation rules.

B. **Related intelligence** column helps the analyst quickly understand the detection context when the alert triggers.

Risk Score	Indicator of Compromise	Type	Related Intelligence
85	192.168.1.100	IP Address	Malware "XYZBot" observed communicating with this IP
70	www.example.com	Domain	Phishing campaign linked to this domain
70	www.malicious-site.com/malware.exe	URL	Malicious executable linked to this URL
80	f4ca5a1b0af60e24a3c1f500f7d69d57	MD5 File Hash	Known malware hash observed on several systems
75	202.54.23.12	IP Address	Multiple intrusion attempts from this IP
55	bad-domain.net	Domain	Suspicious activities reported from this domain
90	45.67.89.123:443	IP	Suspicious behavior on this IP/Port
60	202.54.23.124	IP Address	Unusual traffic patterns associated with this MAC
65	98.76.54.32	IP Address	Potential reconnaissance activity from this IP
45	d41d8cd98f00b204e9800998ecf8427e	MD5 File Hash	Suspicious file hash detected in system logs

Who can benefit from this?

1. The CSOC Team

What can they do with it?

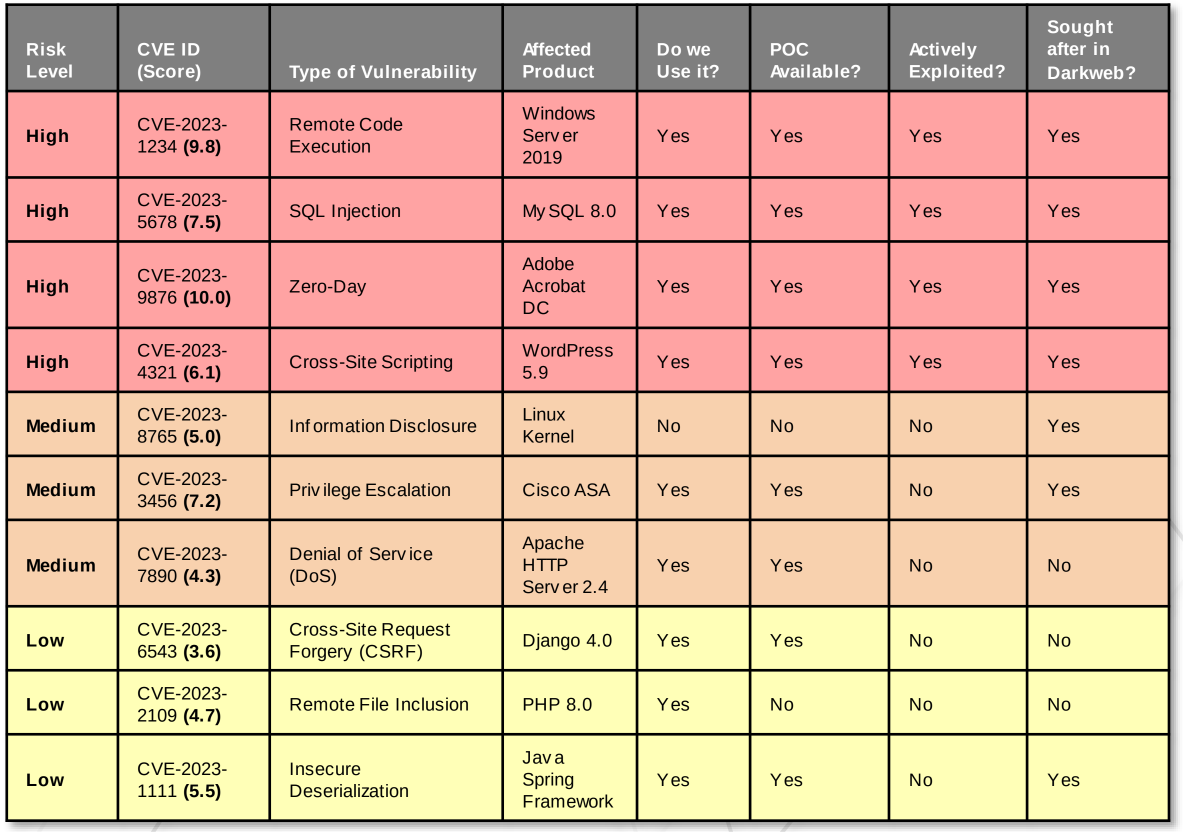
A. Add it to correlation rules such as:

1. Admin user login **AND** match **"Feed IP List"**
2. File Usage **AND** match **"Feed Hash List"**
3. Connection **AND** match **"Feed Domain List"**
4. URL Connect **AND** match **"Feed URL List"**

CTI USE CASE 3: Vulnerability Intelligence

Create a periodically updated vulnerability intelligence table:

1. Send it out to stakeholders frequently.



Risk Level	CVE ID (Score)	Type of Vulnerability	Affected Product	Do we Use it?	POC Available?	Actively Exploited?	Sought after in Darkweb?
High	CVE-2023-1234 **(9.8)**	Remote Code Execution	Windows Server 2019	Yes	Yes	Yes	Yes
High	CVE-2023-5678 **(7.5)**	SQL Injection	MySQL 8.0	Yes	Yes	Yes	Yes
High	CVE-2023-9876 **(10.0)**	Zero-Day	Adobe Acrobat DC	Yes	Yes	Yes	Yes
High	CVE-2023-4321 **(6.1)**	Cross-Site Scripting	WordPress 5.9	Yes	Yes	Yes	Yes
Medium	CVE-2023-8765 **(5.0)**	Information Disclosure	Linux Kernel	No	No	No	Yes
Medium	CVE-2023-3456 **(7.2)**	Privilege Escalation	Cisco ASA	Yes	Yes	No	Yes
Medium	CVE-2023-7890 **(4.3)**	Denial of Service (DoS)	Apache HTTP Server 2.4	Yes	Yes	No	No
Low	CVE-2023-6543 **(3.6)**	Cross-Site Request Forgery (CSRF)	Django 4.0	Yes	Yes	No	No
Low	CVE-2023-2109 **(4.7)**	Remote File Inclusion	PHP 8.0	Yes	No	No	No
Low	CVE-2023-1111 **(5.5)**	Insecure Deserialization	Java Spring Framework	Yes	Yes	No	Yes

Who can benefit from this?

1. The vulnerability management team.
2. The red team/penetration test team.

What can they do with it?

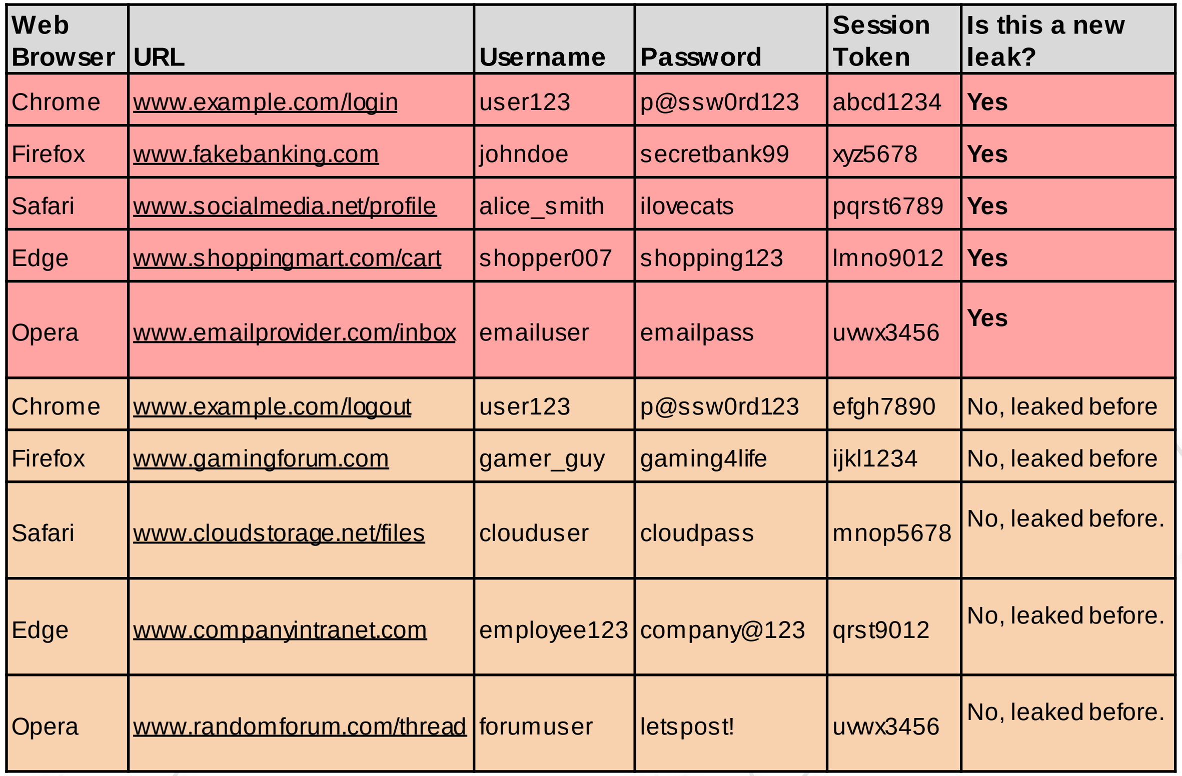
A. Prioritize Patching

B. Exploitation.

CTI USE CASE 4: Infostealer monitoring

Pull infostealers from multiple sources and create a table:

1. Backcheck previously leaked credentials to observe trends and save time.



Web Browser	URL	Username	Password	Session Token	Is this a new leak?
Chrome	www.example.com/login	user123	p@ssw0rd123	abcd1234	**Yes**
Firefox	www.fakebanking.com	johndoe	secretbank99	xyz5678	**Yes**
Safari	www.socialmedia.net/profile	alice_smith	ilovecats	pqrst6789	**Yes**
Edge	www.shoppingmart.com/cart	shopper007	shopping123	lmno9012	**Yes**
Opera	www.emailprovider.com/inbox	emailuser	emailpass	uvwx3456	**Yes**
Chrome	www.example.com/logout	user123	p@ssw0rd123	efgh7890	No, leaked before
Firefox	www.gamingforum.com	gamer_guy	gaming4life	ijkl1234	No, leaked before
Safari	www.cloudstorage.net/files	clouduser	cloudpass	mnop5678	No, leaked before.
Edge	www.companyintranet.com	employee123	company@123	qrst9012	No, leaked before.
Opera	www.randomforum.com/thread	forumuser	letspost!	uvwx3456	No, leaked before.

Who can benefit from this?

1. The Customer Support Team
2. The CSIRT team

What can they do with it?

A. Inform users their credentials are leaked

B. Reset passwords and harden account configurations

C. Eradicate any active malware on the machine.

CTI USE CASE 5: Daily CTI Report

Create a daily Report

1. Maximum of 5 intelligence items
2. Keep the text to the point
3. Answer the following questions
   1. What is the observation?
   2. How is it relevant?
   3. What is the recommendation?
   4. Who can benefit from this intelligence?
4. ChatGPT Prompt example:

```
Act as a cyber threat intelligence analyst read the following article
text and answer the following questions with maximum of 2 sentences
answer and add emojis in bold: 1. what is the observation?, 2. What
are the actionable recommendation? <ARTICLE TEXT>
```

⚠ **Daily Cyber Threat Intelligence Alert** ⚠

1. What is the observation?
The LockBit 3.0 ransomware builder has been leaked, resulting in the creation of new LockBit ransomware variants with altered tactics like unique ransom notes and communication channels. 👾

2. How is it relevant?
Ransomware is considered a high risk to our organization.

3. What is the recommendation?
Strengthen your organization's ransomware defenses by enhancing employee training on phishing and social engineering, regularly updating data backups, and investing in advanced threat detection systems to stay ahead of evolving ransomware techniques. 🔒

4. Who can benefit from this intelligence?
A. Phishing simulation team, B. CSOC C. Data Security Team

Who can benefit from this?

1. Wide array of internal technical or non-technical stakeholders.

What can they do with it?

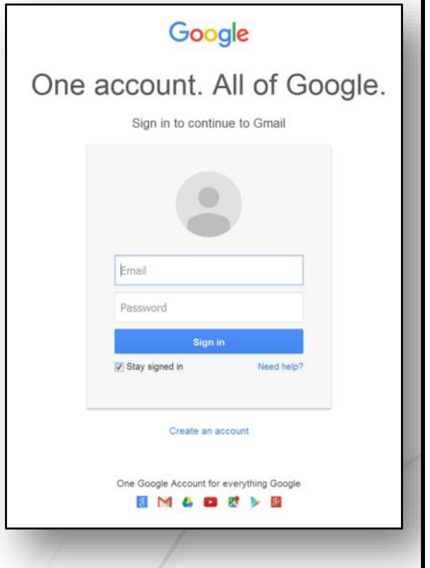
A. External Cyber Situational Awareness Purposes

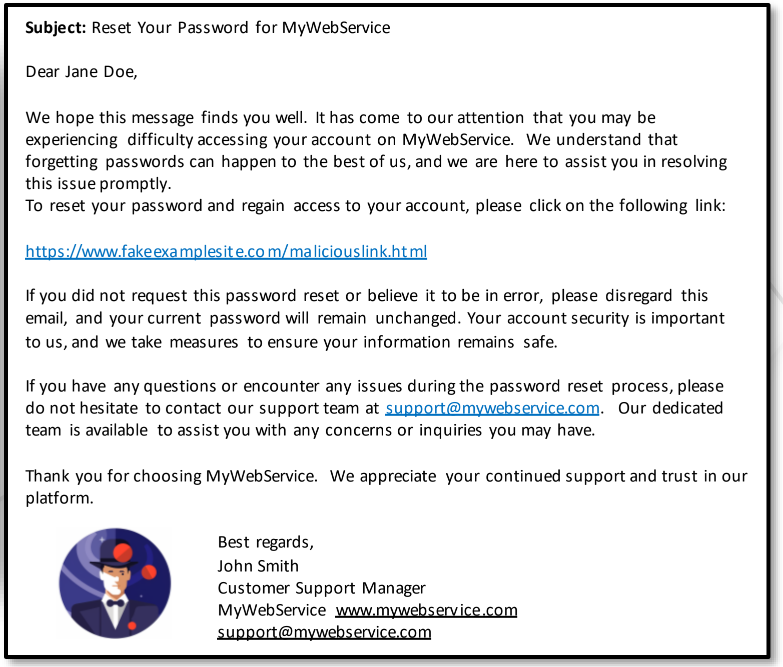
B. Proactive or reactive actionable recommendations to boost the organizations cyber security or compliance levels.

CTI USE CASE 6: Phishing Intelligence

Provide Phishing templates for inspiration internally.

1. Monitor the external web for active phishing campaign examples and send them to the appropriate phishing team and/or the red team.
   - *Pro-active threat hunting for examples is also possible.*


Google
One account. All of Google.
Sign in to continue to Gmail
Email
Password
Sign in
Stay signed in
Need help?
Create an account
One Google Account for everything Google



Subject: Reset Your Password for MyWebService

Dear Jane Doe,

We hope this message finds you well. It has come to our attention that you may be experiencing difficulty accessing your account on MyWebService. We understand that forgetting passwords can happen to the best of us, and we are here to assist you in resolving this issue promptly.
To reset your password and regain access to your account, please click on the following link:

https://www.fakeexamplesite.com/maliciouslink.html

If you did not request this password reset or believe it to be in error, please disregard this email, and your current password will remain unchanged. Your account security is important to us, and we take measures to ensure your information remains safe.

If you have any questions or encounter any issues during the password reset process, please do not hesitate to contact our support team at support@mywebservice.com. Our dedicated team is available to assist you with any concerns or inquiries you may have.

Thank you for choosing MyWebService. We appreciate your continued support and trust in our platform.

Best regards,
John Smith
Customer Support Manager
MyWebService www.mywebservice.com
support@mywebservice.com

Who can benefit from this?

1. The Red Team
2. The Internal Phishing Team
3. The E-Mail Security Team
4. The Security Awareness Team

What can they do with it?

A. Use for the next red team exercise.
B. Use for next phishing exercise.
C. Use for hardening the email filter.
D. Use as recent examples for awareness.

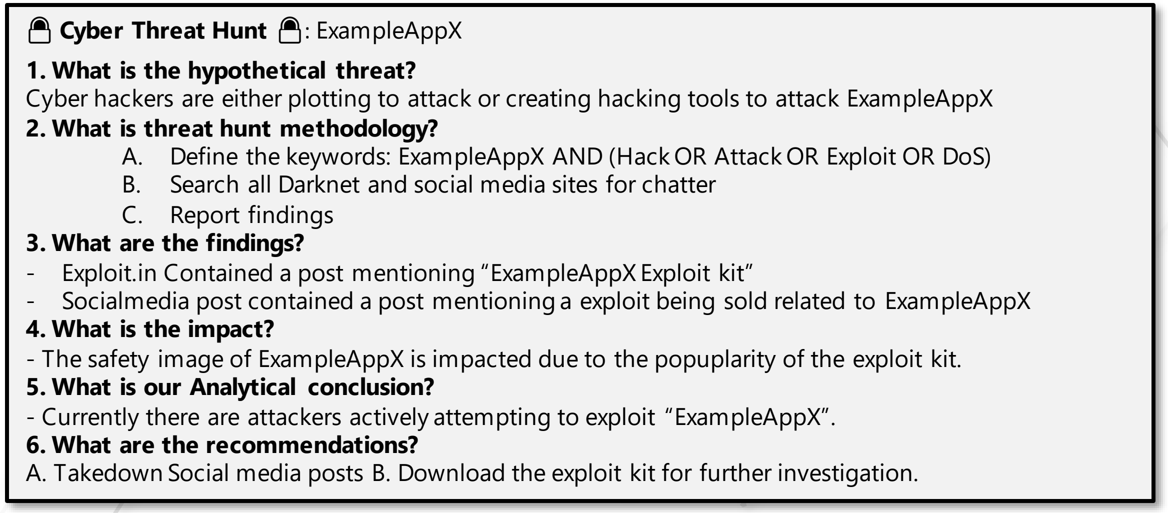
CTI USE CASE 7: Threat Hunting

Threat hunting requests that will proactively search

1. What is the hypothetical threat?
2. What is threat hunt methodology?

   <Execute the threat hunt>

3. What are the findings?
4. What is the impact?
5. What is our analytical conclusion?
6. What are the recommendations?



Cyber Threat Hunt : ExampleAppX

1. What is the hypothetical threat?
Cyber hackers are either plotting to attack or creating hacking tools to attack ExampleAppX

2. What is threat hunt methodology?

A. Define the keywords: ExampleAppX AND (Hack OR Attack OR Exploit OR DoS)
B. Search all Darknet and social media sites for chatter
C. Report findings

3. What are the findings?

- Exploit.in Contained a post mentioning "ExampleAppX Exploit kit"
- Socialmedia post contained a post mentioning a exploit being sold related to ExampleAppX

4. What is the impact?
- The safety image of ExampleAppX is impacted due to the popuplarity of the exploit kit.

5. What is our Analytical conclusion?
- Currently there are attackers actively attempting to exploit "ExampleAppX".

6. What are the recommendations?
A. Takedown Social media posts B. Download the exploit kit for further investigation.

Who can benefit from this?

1. CSIRT, CSOC, CTI
2. Other internal stakeholders can initiate a threat hunt request (RFI).

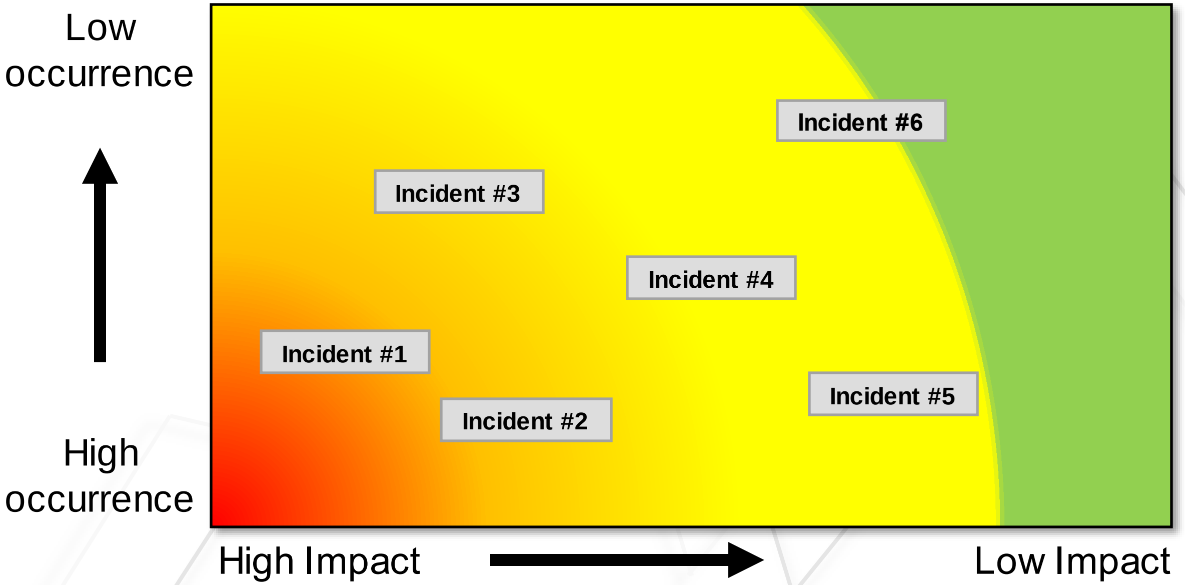
What can they do with it?

1. CSIRT can initiate a hunt during incidents.
2. CSOC can initiate a hunt during triage.
3. CTI can initiate hunts periodically if the intelligence collection cannot be automated.

CTI USE CASE 8: Internal Strategic Intelligence Report

A: Create a threat landscape based on internal incidents.

1. Gather the internal incident registry.
2. Map it to a overall threat table and reflect it in the following diagram style.



Who can benefit from this?

1. Wide array of internal technical or non-technical stakeholders.

What can they do with it?

A. Internal Cyber Situational Awareness Purposes

B. Proactive or reactive actionable recommendations to boost the organizations cyber security or compliance levels.

CTI USE CASE 9: External Strategic Intelligence Report

A: Translate external threat intelligence reports to internal actionable intelligence

1. Monitor external web sources for actionable intelligence reports.
2. Triage those reports that are perceived as "potentially high value"
3. Read and extract key recommendations to a intelligence report with the following table:

Risk Score (after Controls applied)	Report Risk Score	What is the threat	How is it relevant?	What is recommended?	What are we missing?	Recommendation
5	5	**Data Breach**	Unauthorized access to sensitive data	Implement strong access controls and encryption.	Regular security audits	Continuously monitor and update security measures.
4	3	**DDoS Attack**	Disrupts cloud services availability	Employ DDoS mitigation tools and services.	Redundancy planning	Establish backup and failover mechanisms.
4	5	**Insider Threat**	Malicious activities by authorized users	Conduct employee training and implement user behavior analysis.	Insider threat alerts	Enhance monitoring of user activities.
3	4	**Phishing**	Deceptive tactics to steal credentials	Implement email filtering and user awareness training.	Endpoint protection	Enhance endpoint security solutions.
3	5	**Misconfigured Cloud Resources**	Insecure cloud settings lead to vulnerabilities	Utilize cloud security best practices and automated monitoring.	Regular configuration audits	Continuously assess and adjust configurations.
2	3	**API Vulnerabilities**	Weaknesses in API endpoints	Regularly update APIs and apply access controls.	Penetration testing	Perform thorough penetration testing on APIs.
1	3	**Cloud Service Outages**	Interruptions in cloud services	Create a disaster recovery plan and use multiple cloud providers.	Failover planning	Establish failover mechanisms and testing procedures.

Who can benefit from this?

1. Wide array of internal technical or non-technical stakeholders.

What can they do with it?

A. External Cyber Situational Awareness Purposes

B. Proactive or reactive actionable recommendations to boost the organizations cyber security or compliance levels.

CTI USE CASE 10: Threat Intelligence Sharing

A: Cultivate relations, create groupchats and/or sharing platforms with sharing partners

1. Create a **intelligence sharing policy**
2. Determine industry peer relations
3. Determine government peer relations
4. Determine global peer relations
5. Create a common sharing location to exchange intelligence

Intelligence Sharing Partner	Sharing Classification Scope	Do Share	Don't Share
Government Agencies	National Security Threats	- High-confidence indicators of imminent cyberattacks with significant national impact. - Strategic intelligence on threat actors targeting critical infrastructure.	- Raw, unverified data without context or analysis. - Personally identifiable information (PII) or sensitive personal data.
Cybersecurity Vendors	Technical Threat Data	- Specific malware samples, hashes, or signatures. - Vulnerability details with proof-of-concept exploits.	- Customer-specific data or incident reports unless authorized. - Trade secrets or intellectual property.
Information Sharing Groups	Cross-Industry Threats	- Aggregated and anonymized data on common threats and vulnerabilities. - Reports on successful incident response strategies and best practices.	- Detailed internal network diagrams or system architecture. - Internal incident reports without permission.

Who can benefit from this?

1. Wide array of internal technical or non-technical stakeholders.

What can they do with it?

A. External Cyber Situational Awareness Purposes

B. Proactive or reactive actionable recommendations to boost the organizations cyber security or compliance levels.

CONCLUSION

Conclusion

1. The Cyber Threat Intelligence (CTI) program helps **Senior Business leaders make informed** forward-leaning strategic, operational, and tactical **decisions** on **existing, emerging or predicted cyber threats** to the organization.

2. Cyber Threat Intelligence works best **on top of a already functioning security program** which sits on top of a mature IT organization

Dimension	★ Beginner CTI Program	★★ Intermediate CTI Program	★★★ Advanced CTI Program
Budget	**Low** (below 1-10k USD +/-) Yearly	**Medium** (50k-150k USD) Yearly	**High** (200k-400k USD) Yearly
People	1x Junior CTI analyst	1x Junior CTI analyst 1x Mid-level CTI Lead	1x Junior CTI analyst 1x Mid-level CTI analyst 1x Senior CTI Lead
Products	**CTI USE CASE 0:** Keyword Repository **CTI USE CASE 1:** Intelligence Platform Alerts **CTI USE CASE 2:** Cyber Threat Intelligence Feeds **CTI USE CASE 3:** Vulnerability Intelligence **CTI USE CASE 4:** Infostealer monitoring	**CTI USE CASE 0:** Keyword Repository **CTI USE CASE 1:** Intelligence Platform Alerts **CTI USE CASE 2:** Cyber Threat Intelligence Feeds **CTI USE CASE 3:** Vulnerability Intelligence **CTI USE CASE 4:** Infostealer monitoring **CTI USE CASE 5:** Daily CTI Report **CTI USE CASE 6:** Phishing Intelligence **CTI USE CASE 7:** Threat Hunting	**CTI USE CASE 0:** Keyword Repository **CTI USE CASE 1:** Intelligence Platform Alerts **CTI USE CASE 2:** Cyber Threat Intelligence Feeds **CTI USE CASE 3:** Vulnerability Intelligence **CTI USE CASE 4:** Infostealer monitoring **CTI USE CASE 5:** Daily CTI Report **CTI USE CASE 6:** Phishing Intelligence **CTI USE CASE 7:** Threat Hunting **CTI USE CASE 8:** Internal Strategic Intelligence Report **CTI USE CASE 9:** External Strategic Intelligence Report **CTI USE CASE 10:** Threat Intelligence Sharing