Intelligence in Threat Hunting

Orval Roller

Cybersecurity Professional

Key Concepts

+ **The Intelligence Lifecycle**

+ **Types of Threat Intelligence**

+ **Integration into Cyber Defense**

MAJOR TOPICS

- Role of Threat Intelligence in Cybersecurity
- Types & Levels of Modern Cybersecurity
- Core Processes
- Tools, Frameworks, & Collaborative Sharing

LEARNING OUTCOMES

+ Explain purpose and phases of CTI Lifecycle
+ Differentiate between types of CTI
+ Enrich and correlate IoCs
+ Integrate CTI into detection and defense workflows
+ Apply frameworks such as MITRE ATT&CK and STIX/TAXII
+ Evaluate CTI quality and assess its role in cyber defense

PREREQUISITES

- Foundational understanding of cybersecurity principles
- Familiarity with common cybersecurity tools and terminology
- Exposure to SecOps and IR concepts
- Curiosity and willingness to think like an analyst

Let’s Get Started!

Intelligence in Threat Hunting

- Keep your brain open
- Think critically
- Connect the dots
- And most of all – get ready to make threat intelligence actionable.

The Role of Threat Intelligence in Cyber Defense

Cyber Threat Intelligence

- What is Threat Intelligence?
  - Indicators of Compromise (IoCs)
  - Tactics, Techniques, and Procedures (TTPs)
  - Attribution Information
  - Contextual Data

Integration into Cyber Defense

Prevention

- Vulnerability Prioritization
- Policy Hardening
- Threat Modeling
- Blacklisting (Disallow Listing)

Detection

- IOC Matching
- TTP Detection
- Alert Enrichment
- Threat Hunting Guides

Response

- Adversary Playbooks
- Contextual Response
- Attribution Support

Recovery

- Post Incident Review
- Lessons Learned
- Improvement Planning

Planning

- Risk Assessments
- Security Roadmaps
- Simulations and Tabletop Exercises
- Regulatory Compliance

Why Threat Intelligence Matters

- Reduce Breach Costs
- Speeds Up Detection and Response
- Improves SOC Efficiency
- Enables Proactive Defense
- Real-World Relevance

Types of Threat Intelligence

- Strategic
- Operational
- Tactical
- Technical

Integration Points in the Stack

- Where does threat intelligence fit into existing infrastructure?
  - SIEM
  - Endpoint Detection and Response
  - Firewall/WAF
  - SOAR (Security Orchestration, Automation, and Response)
  - Threat Intelligence Platform

Common Sources of Threat Intelligence

- OSINT
- Government feeds (e.g., CISA KEV, NVD)
- ISACs
- Commercial feeds
- Dark web monitoring

Benefits of a Mature CTI Program

+ Faster incident response
+ Reduced risk exposure
+ Better investment decisions
+ More effective threat hunting

Challenges and Pitfalls

- Information overload
- Poor relevance to the organization
- Lack of trained analysts
- Failure to operationalize threat intelligence

Takeaways

- Force multiplier
- Adds value across the Cyber Defense Lifecycle
- Don’t Just Collect – Operationalize
- Quality Over Quantity
- Requires People, Process, and Technology

Strategic, Operational, Tactical, and Technical Intelligence

Threat Intelligence Levels

Strategic Threat Intelligence

Strategic Intelligence in Action

- Examples
  - Nation-state targeting specific sectors
  - Long-term ransomware trends
  - Supply chain geopolitical risks
- Sources
  - Government threat bulletins
  - Commercial threat reports
  - Sector ISACs
- Outputs
  - Risk assessments
  - Executive briefings
  - Policy recommendations

Operational Threat Intelligence

Operational Intelligence in Action

- Examples
  - Ransomware affiliate mapping
  - Phishing campaign timeline
  - MITRE ATT&CK heat maps
- Sources
  - Threat actor tracking reports
  - ISAC updates
  - Dark web monitoring
- Outputs
  - Adversary profiles
  - Campaign briefs
  - Threat intelligence requirements

Tactical Threat Intelligence

Tactical Threat Intelligence in Action

- Examples
  - Credential dumping techniques
  - Fileless malware execution
  - Lateral movement via PSExec
- Sources
  - Internal IR reports
  - Threat emulation results
  - Red team engagements
- Outputs
  - Hunt queries
  - Sigma/YARA detection rules
  - Response playbooks

Tactical Threat Intelligence

Technical Intelligence in Action

- Examples
  - IP addresses, file hashes
  - Malicious domains or URLs
  - Malware samples/hashes
- Sources
  - VirusTotal
  - Honeypots and spam traps
  - Sandboxes
- Outputs
  - Blocklists
  - IOC feeds for SIEM
  - EDR/FW rule integrations

The Levels Working Together

Pitfalls of Siloed Intelligence

- Strategic goals don’t match real threats
- SOC drowns in IoCs without context
- Detection rules lack campaign awareness
- Missed opportunities for prioritization

Takeaways

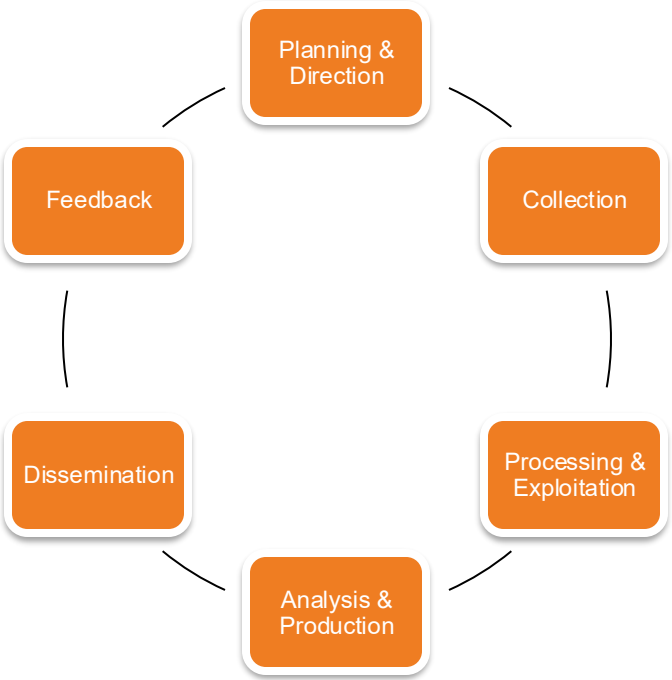
- Each level of intel answers a different question
- Actionable intelligence must match its audience
- Best programs integrate all four levels
- Feedback loops turn noise into insight

Intelligence Lifecycle: From Planning to Dissemination

Cyber Threat Intelligence Lifecycle

- CTI Lifecycle is Iterative
- Each Phase Builds on the Last
- Actionable Intelligence is the Goal

Cyber Threat Intelligence Lifecycle Overview



Planning & Direction

- Define the Hunt
  - What threats matter to us now?
  - Who are we hunting and why?
  - What are our Priority Intelligence Requirements (PIRs)?
  - Which MITRE TTPs should we focus on?

- Example:
  - “We’ve seen TA577 abusing DLL search order hijacking in our sector. Let’s hunt for T1574.001 across legacy systems.”

Collection

- Gather the Right Telemetry
  - Pull EDR, Netflow, Windows Logs, Authentication Logs
  - Integrate CTI: IOCs, TTPs, actor profiles
  - Align with hunt scope and assets
- Example:
  - “Collected DNS logs after CTI warned of APT28 using ‘cdn-assets-update[.]com’.”

Processing & Exploitation

- Normalize and Enrich Data
  - Normalize logs into a common format
  - De-dupe and filter irrelevant data
  - Enrich with context (GeoIP, WHOIS, MITRE tags)

- Example:
  - “Used a script to tag base64 PowerShell commands with T1059.001 and flag unsigned scripts.”

Analysis & Production

- Test the Hypothesis
  - Look for anomalous behavior
  - Correlate events across systems
  - Validate adversary TTPs in your environment
  - Document findings with context and severity

- Example:
  - “Lateral movement via PSExec discovered after matching IR evidence to Lazarus TTPs”

Dissemination

- Get the Intel to the Right Hands
  - Alert SOC for detection engineering
  - Share with IR and leadership
  - Document in knowledgebases or playbooks

- Example:
  - “IOC list delivered to firewall team; Sigma rule deployed in SIEM to catch reuse.”

Feedback

- Improve the Next Hunt
  - Review what worked, what didn't
  - Collect feedback from IR, SOC, CTI teams
  - Update PIRs, scope, and detection logic
- Example:
  - "SOC reported false positives on the PowerShell rule; we refined it using baseline logic."

Prioritizing Intelligence

- Why Prioritization Matters
  - **The Flood of Intel:** You can't act on everything
  - **The Cost of Distraction:** Wasted effort vs. focused response
  - **The Goal:** Relevance + Urgency + Impact

Key Dimensions of Prioritization

- Relevance
  - Aligned with industry, assets, geography, threat model
- Actionability
  - Can it be used to inform detection/prevention?
- Criticality
  - What is the risk if left unmitigated?

Understanding Relevance

- What makes intelligence relevant?
  - Does it match your organization's attack surface?
  - Is the threat actor known to target your sector?
  - Does it apply to your software stack, geolocation, or business processes?

Indicator	Sector	Technology	Region	Relevance Score
10.1.100.133	✅ Financial	✅ Uses Citrix	❌ Asia Only	Medium
Malware[.]com	❌ Healthcare	✅ Microsoft 365	✅ US-Based	Low

Evaluating Actionability

- Can you use the intel to detect, block, or investigate a threat?
  - Actionable Indicators
    - IPs/domains with rich context (first seen, campaign link, threat actor)
    - TTPs tied to detections in your EDR/SIEM
    - Snort/YARA rules or Sigma format

Indicator	IOC Type	Detection Method Exists?	Mitigation Possible?	Actionable?
Hash 1a2b3c	File	❌	❌	❌
10.1.20.37	Network	✅ via firewall rules	✅	✅

Measuring Criticality

- If the threat is real and affects us, how bad is it?
- Factors
  - Potential Impact (financial, operational, reputational)
  - Data at risk
  - Threat actor sophistication

RISK = LIKELIHOOD X IMPACT

Scoring Models and Frameworks

- Admiralty Code (NATO Rating System)
  - Source Reliability (A-F)
  - Information Credibility (1-6)
  - Used to rate incoming intel
- Diamond Model
  - Evaluate **Adversary, Infrastructure, Victim, Capability**
  - Scored based on proximity to your assets or operations
- Risk-Based Scoring
  - Formula: Likelihood x Impact x Exposure
  - Ties intelligence directly to risk posture

Prioritization Matrix

	Low Actionability	High Actionability
Low Relevance	Ignore	Watch
High Relevance	Investigate	PRIORITIZE

Automation vs Analyst Judgement

- SIEMs and TIPs can automate prioritization:
  - STIX tags
  - Scoring feeds
  - Expiration dates
- Analysts are still needed for:
  - Campaign tie-ins
  - Understanding nuanced TTPs
  - Applying internal organizational knowledge

Takeaways

- Not all intelligence is equal
- Prioritize based on Relevance, Actionability, and Criticality
- Use scoring frameworks to stay consistent
- Human analysis adds needed nuance

Applying the Intelligence Cycle in Real-World Operations

Quick Recap of the Intelligence Cycle

- Planning & Direction
- Collection
- Processing & Exploitation
- Analysis & Production
- Dissemination
- Feedback

Real-World Use Case Introduction

- **Example Case:** Ransomware Attack on a Healthcare Provider
  - **Date:** January 2024
  - **Threat Actor:** Suspected APT28-affiliated group
  - **Impact:** Critical systems locked, patient data encrypted

Direction (Setting the Stage)

- Who gives direction?
  - CISO, Threat Intel Lead, Incident Commander
- Focus:
  - Identify what we need to know (IoCs, threat actor TTPs, infrastructure at risk)
- Example:
  - “Determine if this is part of a broader campaign targeting the health sector.”

Collection (Gathering the Data)

- **Internal:** logs, SIEM events, EDR telemetry
- **External:** OSINT, ISAC reports, CTI vendors, dark web

```
{
  "indicator": "h3x-tunnel.duckdns.org",
  "type": "domain",
  "threat_actor": "APT28",
  "confidence": "high",
  "description": "Domain associated with recent ransomware campaigns targeting healthcare sector",
  "first_seen": "2023-12-30T13:45:00Z",
  "related_hashes": ["a4f0b1e2f2cb9e2d3b3a1180c1e9cd29b3c003..."]
}
```

Processing & Exploitation

- **Normalize data:** timestamps, IPs, domain names, log formats
- De-duplicate, enrich with GeoIP, WHOIS, and MITRE mappings

Analysis & Production

- What's happening?
- Who's behind it?
- What's the objective?
- How can we stop it?

- **Example Output:** Threat actor profile, IOC set, kill chain stage

Dissemination

- **Format:** Flash report, Threat Bulletin, Briefing, Slack/Ticket System
- **Audience:** SOC, Executives, IR, Law Enforcement

Feedback Loop

- Did the intel help detection or response?
- Were there gaps in collection?
- What should we do differently next time?

Analyst Roles at Each Stage

Stage	Typical Roles Involved
Direction	CISO, IR Lead, CTI Lead
Collection	CTI Analysts, Threat Hunters
Processing & Exploitation	Automation Engineers, Intel Techs
Analysis & Production	Intel Analysts, Hunt Team
Dissemination	CTI Lead, Report Writers
Feedback	All Stakeholders

Tactical vs Strategic Applications

- **Tactical:** Enriching SOC alerts, blocking malicious IPs
- **Operational:** Campaign tracking, adversary TTP monitoring
- **Strategic:** Budgeting, long-term security priorities

Takeaways

- The intelligence cycle is iterative and flexible
- Direction and feedback are crucial bookends
- Real-world ops require fast but accurate intelligence flows
- Integrating the cycle in IR and detection makes teams proactive

Using MITRE ATT&CK for Adversary Analysis

Introduction

- Adversary Analysis
  - Tracking, profiling, and understanding threat actors
- MITRE ATT&CK
  - Knowledgebase of tactics and techniques observed in the real-world
  - Maps observed behaviors of known threat actors or campaigns

What is MITRE ATT&CK?

- MITRE Adversarial Tactics, Techniques, and Common Knowledge
- Tactics
  - Adversary goals
- Techniques/Sub-techniques
  - How are the goals achieved?
- Mitigations and relationships
  - How do we respond?
- Data sources and detections
  - Which logs and signals can detect behaviors?

How ATT&CK Supports Adversary Analysis

- How analysts use ATT&CK
  - Map threat group behavior
  - Compare behaviors across incidents
  - Hunt for activity using TTPs
  - Prioritize detection engineering
- Threat Actor pages
  - Lists known techniques, tools, software, references

Mapping a Real Incident with ATT&CK Navigator

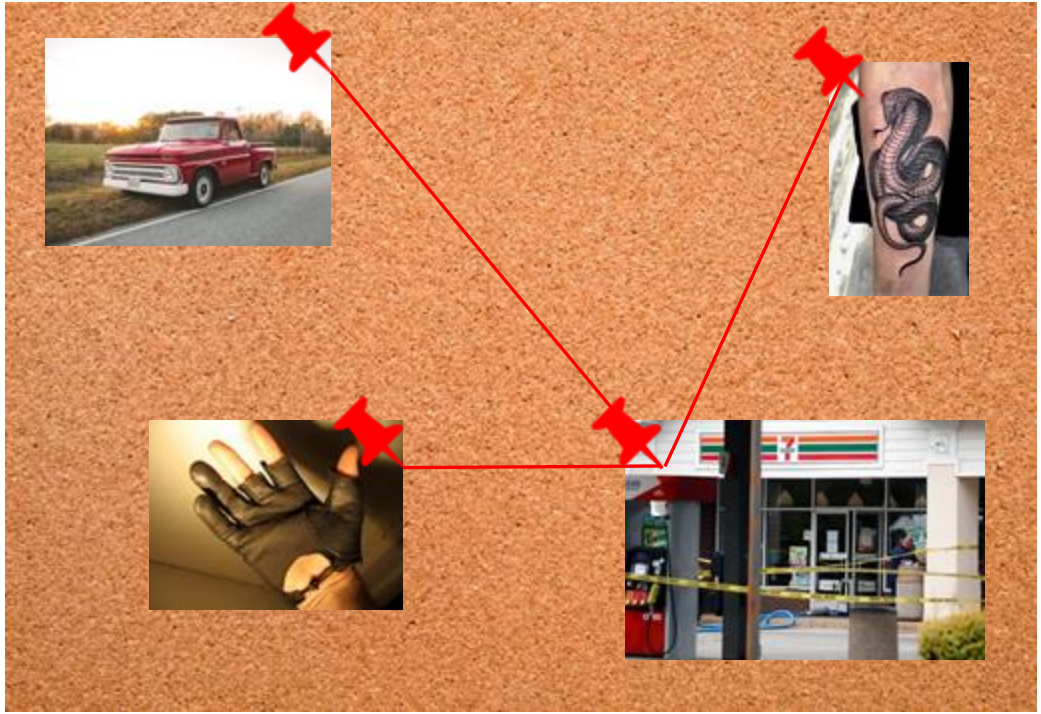
- Indicators from analysts
  - Use of PowerShell (T1059.001)
  - Use of Web Protocols (T1071.001)
- Does this activity match other known threat actor activity?
- Guide incident response
- Assess adversary objectives

Takeaways

- ATT&CK is not a silver bullet
- Map behaviors, no just indicators
- Use ATT&CK for:
  - Threat Hunting
  - Detection Engineering
  - Threat emulation/red teaming
  - Attribution support

Correlating IoCs Across Sources

Detective Analogy



What is IOC Correlation?

- Correlation links IoCs across time, tools, and sources.
- Transforms isolated data points into an intelligence picture.
- Enables detection, attribution, and response.

What are IoCs?

- Digital clues tied to malicious activity
- Can be atomic (IP, hash value) or behavioral (process tree)
- Used to detect, track, and stop threats

Where Do IoCs Come From?

- Internal telemetry (SIEM, EDR, DNS, proxy)
- External intel (MISP, OSINT, vendor feeds)
- Government/ISACs (CISA, sector-specific ISACS)
- Historical incidents and ticketing systems

Why Correlate IoCs?

- Validate threats using multiple sources.
- Enhance context and actor attribution.
- Detect low signal or stealthy threats.
- Link infrastructure and uncover campaigns.

Correlation Techniques

- Exact Matching
- Infrastructure Pivoting
- Fuzzy Matching
- Time-Base Analysis
- TTP and Campaign Linking

Exact Matching

- Direct one-to-one matching of IOCs across datasets
  - Most basic form of correlation
  - Compares identical values (IPs, hashes, domains, etc.)
  - Confirms credibility and increases priority
  - Often automated in SIEMs, TIPs, and other feeds

- Example:
  - IP ‘192.0.2.45’ have been seen in both the organization’s SIEM and in their subscribed threat intel feed.

Infrastructure Pivoting

- Use one IoC to discover related indicators via shared infrastructure
  - Pivot from a domain to its IP => find all domains on that IP.
  - Use WHOIS, passive DNS, SSL cert reuse, ASN data.
  - Expands visibility into the adversary's digital footprint.

- Example:
  - The domain name 'evil-login[.]net' => host on '45.66.123.9' => hosts 5 other known malicious domains.

Fuzzy Matching

- Identify indicators that are similar but not exact
  - Detect typosquatting or lookalike domains.
  - Use fuzzy hashing (ssdeep) for near-identical malware.
  - Identify minor code or filename variations.
- Example:
  - ‘dropbox[.]com’ vs ‘dropb0x-secure[.]com’
  - Malware hashes with a 93% similarity

Time-Based Correlation

- Correlate IoCs based on event timing to reconstruct incidents.
  - Link events across logs by timestamps.
  - Reveals attack progression and lateral movement.
  - Supports timeline-based threat hunting and IR.

- Example:

Timestamp	Source/System	Indicator Type	IoC Value	Observed Activity	Correlation Note
10:03 AM	Email Gateway	Hash	a1b2c3…	Phishing email	Matches known malware
10:05 AM	DNS Logs	Domain	login-secure[.]com	DNS lookup initiated	Same C2 as malware
10:06 AM	EDR	Process	powershell.exe	Obfuscated script	Follows known TTP
10:07 AM	Proxy Logs	IP Address	203.0.113.25	Outbound C2 Connection	Matches threat feed

TTP & Campaign Correlation

- Match IoCs to known tactics, techniques, and threat actor patterns.
  - Align IoCs with MITRE ATT&CK techniques.
  - Identify repeat tool sets or scripting behaviors.
  - Map to historical campaigns or APT profiles.
- Examples:
  - PowerShell command => T1059.001 (MITRE)
  - Infrastructure overlaps with APT28 campaign
  - Confirms behavioral linkage to known adversary

Tools for Correlation

- TIPs – threat sharing and event correlation
- MITRE ATT&CK Navigator
- Maltego – infrastructure graphing
- Elastic/Splunk – internal log correlation
- Python scripts + enrichment APIs

Correlation Best Practices

- Normalize and enrich data before correlation
- Use STIX/TAXII for standardization
- Always verify external IoCs with internal logs
- Tag by time, actor, confidence
- Avoid correlation overload (don’t link everything!)

The Power of Connection

- IoCs are valuable alone, but powerful when linked
- Correlation reveals intent, infrastructure, and actor behavior
- Use tools and context to go beyond surface indicators
- Good correlation is the difference between alerts and insight

Integrating CTI into SIEMS and Detection Pipelines

Why Integration Matters

- Faster detection of known bad
- Improved context for analysis
- Better alert triage and fewer false positives
- Automation possibilities

CTI Feeds and Sources

- Open Source (OSINT): AlienVault OTX, Abuse.ch, etc.
- Commercial: Recorded Future, ThreatConnect
- ISACs/GOV: FS-ISAC, CISA
- Internal: Honeypots, IR reports

Integration Points in the Pipeline

- Collection TIP SIEM
- SIEM Enrichment: Adds CTI data to raw logs
- Detection Logic: IOC/TTP matches trigger alerts
- SOAR: Uses CTI to prioritize & automate response

IoC Use Cases

- IP/URL/Hash matching
- GeoIP & ASN-based risk scoring
- Expiry and context-based IOC filtering

Beyond IoCs: TTP Detection

- Use ATT&CK-aligned rules (e.g., detecting credential dumping)
- Threat behaviors tied to known adversaries
- Mapping detection coverage to ATT&CK

SIEM Rule Enrichment Example

- Before:
  - ‘IF src_ip == x.x.x.x THEN alert’

- After:
  - ‘IF src_ip IN [Threat Feed] AND Threat_Level >= 7 AND NOT PreviouslySeen THEN alert with context’

Automation with SOAR

- Enrich alerts with threat actor data
- Automate blocking in firewall
- Prioritize incidents based on threat scoring

Metrics for Success

- Reduction in false positives
- Mean Time to Detection (MTTD)
- Coverage of known threats
- Analyst feedback

Challenges & Pitfalls

- Too much noise from low-quality feeds
- Stale IoCs
- Over reliance on atomic indicators
- Poor correlation with local environment

Best Practices

- Use vetted, high-confidence feeds
- Apply context (e.g., malware family, campaign)
- Regularly tune detection rules
- Automate IoC expiration
- Feed CTI back from IR teams (Closed Loops)

Maturity Model

- Five Progressive Stages of CTI Maturity
  - Ad hoc CTI lookup
  - IoC ingestion into SIEM
  - Detection rule tuning
  - Behavioral analytics
  - Full SOAR-based response

Takeaways

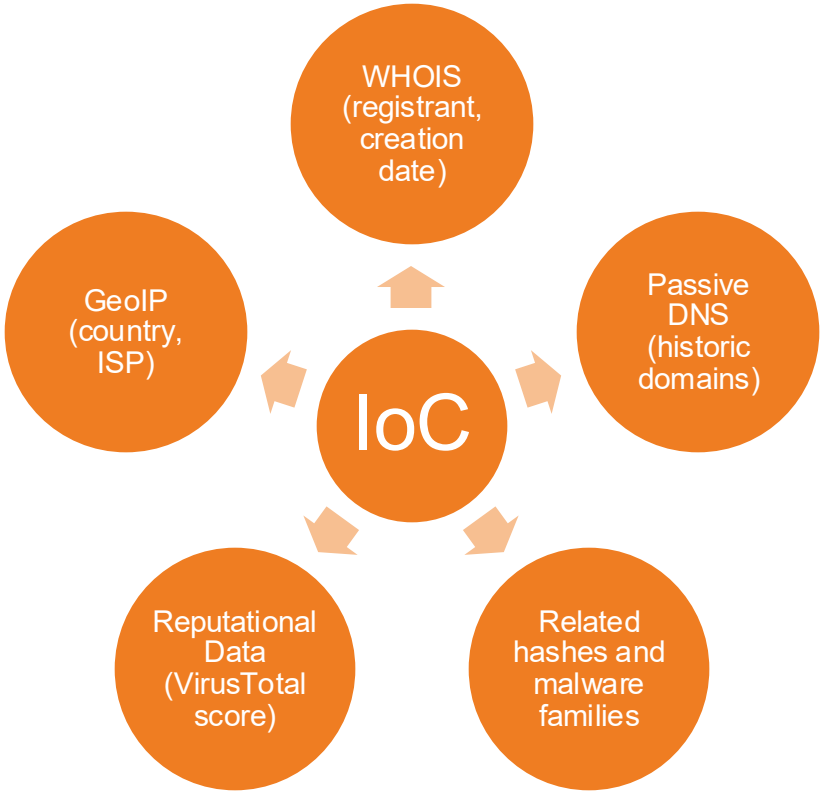
- Integration is key to making CTI actionable
- SIEMs benefit from high-quality intel + context
- Automation supercharges response
- CTI is not just IoC matching – think behavior, context, threat actor

IoC Enrichment & Contextualization

Why Raw Data Isn’t Enough

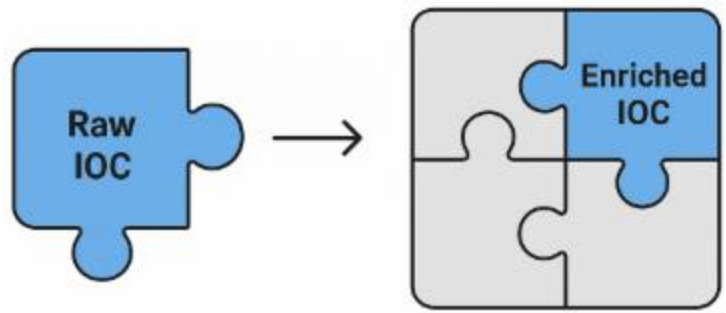
- Lack of Context
- High False Positives
- No Prioritization
- Blind Spots in Response

What is Enrichment?



Contextualization

- Is this part of a known campaign?
- What stage of the attack does it relate to?
- Does this affect my industry?



Walkthrough

- Your SOC receives an alert for outbound traffic to ‘34.117.59.81.’
- You enrich it and find:
  - WHOIS: Belongs to Google Cloud
  - GreyNoise: Seen scanning SSH globally
  - VirusTotal: Flagged as malicious in 3 engines
  - Passive DNS: Previously resolved from ‘akudate.evilcorp[.]com
  - Sandbox: Dropped Emotet payload
- You contextualize:
  - Likely C2 infrastructure
  - Previously used by Emotet variant
  - Seen in phishing campaigns in past 7 days
  - Associated with TTPs linked to TA542

How It All Connects

- IoC → Enrichment Layer → Context Layer → Outputs
  - Detection Engineering
  - Threat hunting
  - Reporting/Intel feeds
  - Incident response

Common Tools & Data Sources

- Internal: SIEM, IR logs, sandbox detonation
- External: VirusTotal, PassiveTotal, MISP, AbuseIPDB, AlienVault OXT, Shodan

Mapping IoCs to MITRE ATT&CK

Tactic	Technique (ID)	Associated IoC Types	Example IoC
Initial Access	Phishing (T1566)	Email address, subject line, sender IP, file hash	billing@secure-paypal.com
Execution	Command and Scripting Interpreter (T1059)	Script hash, file path, process name, parent-child process correlation	C:\Users\user\AppData\Roaming\run.ps1
Privilege Escalation	Exploitation for Privilege Escalation (T1068)	CVE references, unusual process activity, exploit toolkit hashes	CVE-2021-1732exploit hash: a7e45bcf92...
Credential Access	Credential Dumping (T1003)	LSASS memory access, mimikatz hash, hash dumps	C:\Windows\Temp\lsass.dmp
Exfiltration	Exfiltration Over HTTPS (T1041)	Outbound data patterns, domain names, SSL cert fingerprints	Large POSTs to cdn-dropbox[.]com, cert: SHA256:abcd...

Pitfalls & False Confidence

- Reputation doesn’t equal attribution
- Shared infrastructure ≠ shared actor
- Data staleness is real (last seen ≠ still active)

Practical Use Cases

- **SOC Analyst:** Enriched IoCs drive correlation rules
- **Threat Hunter:** Use context to guide hypothesis driven hunts
- **CTI Analyst:** Add actor info and ATT&CK mapping for reporting

Takeaways

- **Enrichment** = Data about the IoC
- **Contextualization** = Meaning around the IoC
- **Together** = Actionable intelligence

Intelligence-Driven Threat Hunting Methodologies

Why Intelligence Should Drive the Hunt

- Raw data ≠ meaningful detection – intelligence provides direction
- Focused hunts reduce wasted effort and blind spots
- Brings hunting in line with real-world threats (APT groups, malware campaigns)
- Supports prioritization based on likelihood, relevance, and potential impact.

Core Intelligence Inputs

- Strategic to Tactical : Use all levels of threat intel but prioritize technical and TTP-based indicators.
- Sources:
  - OSINT feeds
  - Commercial feeds
  - Sector ISACs / CISA alerts
  - Internal telemetry (previous IR cases, phishing reports)

From Intelligence to Hypothesis

- Use intelligence to build testable, scoped hypotheses:
  - “If [actor/tool] targets organizations like ours, we might see [behavior] in [data source].”
- Example:
  - “If Volt Typhoon is targeting ICS systems, are there WMI events in the Windows IT system logs?
- Reinforces proactive, analytical mindset.

Aligning with MITRE ATT&CK

- Convert intel to behaviors via ATT&CK techniques.
- Benefits:
  - TTP-based hunting scales better than IOC-based
  - Reusable detection content across environments
- Tools:
  - ATT&CK Navigator, Unfetter, ThreatMapper

Telemetry and Hunting Tools

- What you need visibility into:
  - Endpoints (EDR, Logs, AV)
  - Authentication (Windows Events, AD logs)
  - Network (Netflow data, Proxy, DNS)
  - Cloud (CloudTrail, GCP logs)
- Tool Examples:
  - Splunk, ELK, Velociraptor, Sigma rules, EQL

Methodology

- Step-by-step:
  1. Ingest and contextualize threat intel
  2. Create hypothesis from relevant actor/tool
  3. Map to ATT&CK techniques
  4. Build hunt queries/detections
  5. Validate with real data
  6. Feed results into IR/SIEM/detection

Case Study – Targeted Email Compromise

- **Intel:** TA551 uses Excel macros => RDP => Cobalt Strike
- **Hypothesis:** Look for Excel spawning unusual child processes
- **TTP Mapping:**
  - T1204.002 (User Execution)
  - T1059.005 (VBScript)
  - T1219 (Remote Access Software)
- **Action:** Hunt EDR logs for ‘excel.exe’ spawning ‘powershell.exe’, followed by outbound C2

Post-Hunt Actions

- Refine detections & SIEM rules
- Share TTP observations with SOC/IR
- Feed context back into TIP or wiki
- Update adversary playbooks or threat models

Intelligence-Driven vs Traditional Hunting

Feature	Traditional	Intelligence-Driven
Scope	Broad, unfocused	Scoped to threats
Drivers	Gut feeling, anomalies	Adversary behaviors, intel
Outputs	Alerts, anomalies	Detections, context, enrichment
Efficiency	Varies	High (targeted effort)

Operationalizing the Process

- Build repeatable workflows:
  - Templates for hypothesis generation
  - ATT&CK-mapped detection libraries
  - Threat actor tagging in logs
- Integrate with SOC/IR feedback loops
  - Make hunting part of daily ops, not a side project

Takeaways

- Intelligence gives purpose to the hunt.
- Hypotheses and TTPs bridge gaps between CTI and detection
- Continuous improvement depends on feedback loops

- Threat Hunting Maturity for an organization:
  - Progress from IOC-based reactive hunts (Level 1)
  - Behaviorally focused TTP hunts (Level 2)
  - Fully integrated, intelligence-driven, adversary-informed hunting cycles (Level 3)

OSINT, Commercial Feeds, and Closed Sources

The Intelligence Source Spectrum

- OSINT (Open-Source Intelligence)
  - GitHub, Twitter/X, Reddit, VirusTotal, blogs, Pastebin, etc.
- Commercial Feeds
  - Mandiant, Recorded Future, Flashpoint, Palo Alto Unit 42, etc.
- Closed Sources
  - Government Agencies
  - Sector Specific ISACS

OSINT (Open-Source Intelligence)

- Strengths
  - Free and abundant
  - Diverse: social media, public malware repositories, blogs
  - Real-time & community-driven
- Weaknesses
  - High noise-to-signal ratio
  - Often unauthenticated or unverified
  - Susceptible to disinformation or manipulation

Commercial Feeds

- Strengths:
  - Curated, enriched, and usually vetted
  - Often come with support or threat actor tracking
  - SLAs and integrations with SIEM/TIP/SOAR
- Weaknesses:
  - Expensive – may overlap with OSINT.
  - Risk of “vendor echo chamber” where everyone has the same indicators.

Closed Sources

- Strengths:
  - Highly exclusive – e.g., government intel, industry-specific trust groups, dark web infiltrations
  - Can provide early warning or high-confidence intelligence
- Weaknesses:
  - Hard to access (clearance, trust, vetting)
  - Little transparency into collection methods

Source Convergence & Validation

- The best intelligence comes from correlating across sources.
- Example:
  - OSINT detects a new phishing domain.
  - Commercial feed matches infrastructure to a known APT.
  - Closed source confirms campaign targeting via classified alerts.

Operational Considerations

- Questions to ask:
  - What's the source's collection methodology?
  - Can it be actioned?
  - Is it redundant or unique?

Case Study – Log4Shell

OSINT	COMMERCIAL FEEDS	CLOSED SOURCES
Dec 9: • Tweets leak exploit • GitHub PoCs drop • Minecraft servers tested	**Dec 10:** • YARA/Sigma rules released • Initial TTP attribution • Endpoint detection guidance	**Dec 11:** • Alerts to critical infrastructure organizations • Early ransomware warnings • Nation-state actor reports
Impact: Fast, noisy alerts Crowd-sourced awareness	**Impact:** Structured detections Context from experts	**Impact:** Strategic response Trusted sector coordination

"Speed + Structure + Strategy = Resilience"

Feed Management Strategy

- Build vs Buy vs Borrow
- TIPs and automation to reduce overload.
- Creating internal policies for validation and usage.

STIX, TAXII, & the Traffic Light Protocol

Foundations of Threat Intelligence Sharing

- Understand STIX, TAXII, and TLP
- Learn how they work together in CTI sharing
- See how they are used in real-world tools and platforms

STIX: Structured Threat Information Expression

- Structured
  - Defined schema for consistency
- Descriptive
  - Captures indicators, actors, malware
- Relational
  - Links objects like “Malware used by Actor”
- Machine Readable
  - Written in JSON for automated parsing

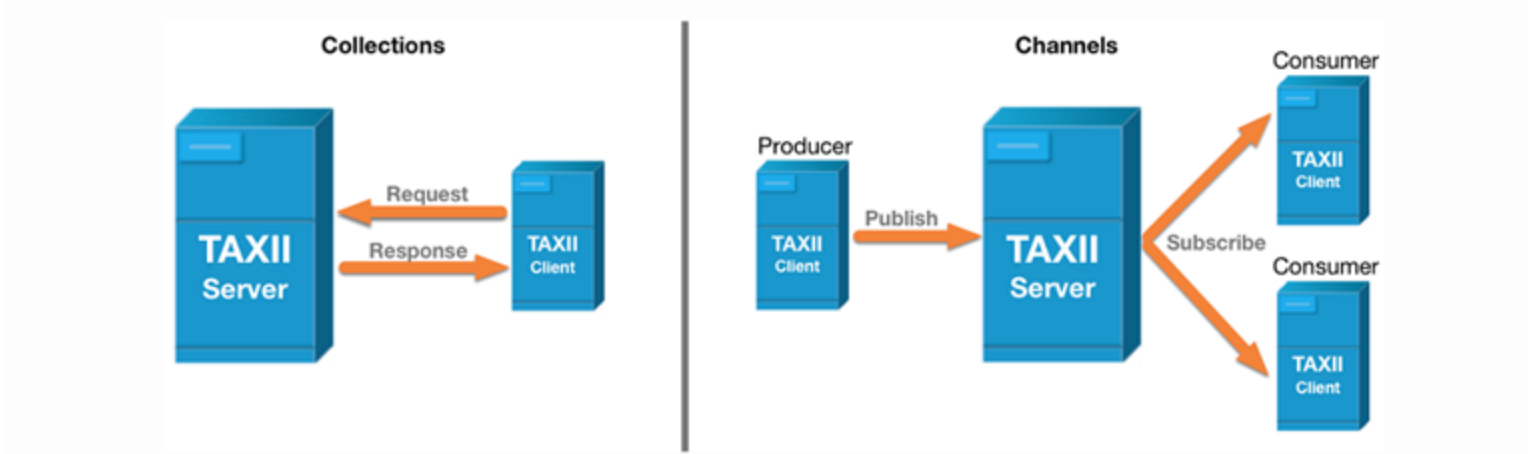
STIX Example

```
{
  "type": "indicator",
  "pattern": "[file:hashes.'SHA-256' = '...']",
  "labels": ["ransomware", "healthcare-targeting"],
  "created_by_ref": "identity--1234",
  "tlp_color": "amber"
}
```

TAXII: Trusted Automated Exchange

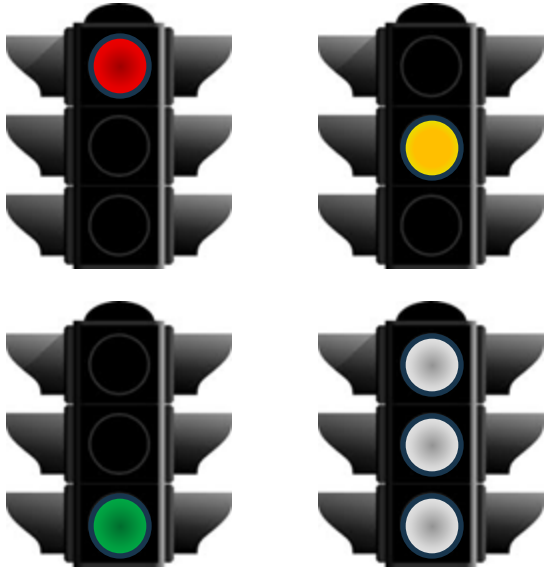
- Transport Protocol
  - Moves STIX data between systems securely and reliably
- Standardized API
  - Uses HTTP/S and RESTful endpoints for easy integration
- Push & Pull Support
  - Can push data to subscribers or let consumers pull when needed
- Collections & Channels
  - Organizes shared intel into topic-based containers
- Designed for Automation
  - Supports machine-to-machine sharing in real time or on schedule

TAXII Example



TLP: Traffic Light Protocol

- TLP:RED
  - For named recipients only; do not share
- TLP:AMBER
  - Limited disclosure; only to those who need to know within your organization
- TLP:GREEN
  - Share with peers and partners within your community
- TLP:CLEAR
  - No restrictions; may be shared publicly



Putting It All Together

- STIX provides the data format.
- TAXII provides the transport mechanism.
- TLP provides the handling and dissemination guidance.

Takeaways

- STIX
  - What is shared
- TAXII
  - How it's shared
- TLP
  - Who it's shared with

Structured Analytical Techniques for CTI

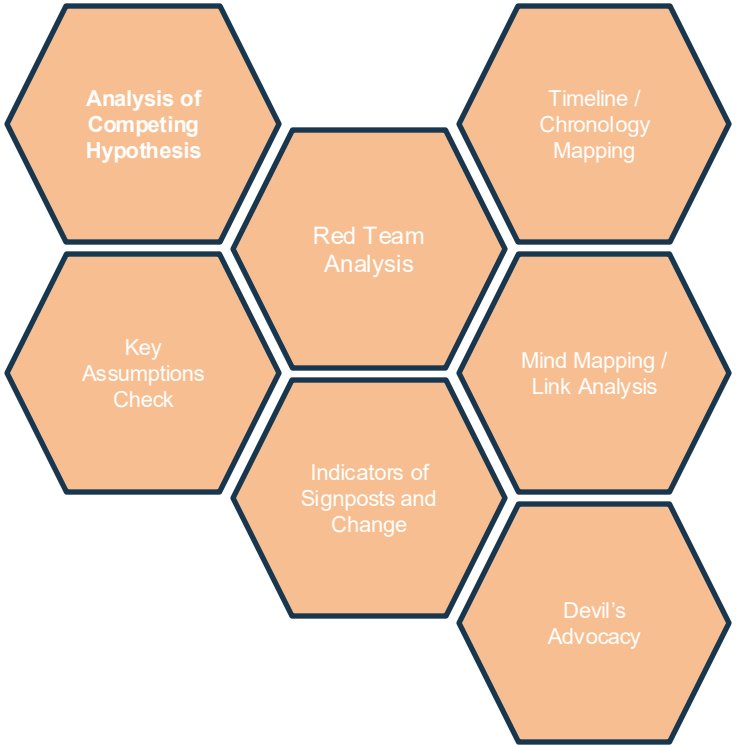
Structured Analytical Techniques

- What are SATs?
  - Formalized methods used to improve critical thinking and analysis
- Purpose
  - Examine assumptions
  - Identify gaps and contradictions
  - Minimize biases
  - Consider alternative hypotheses
- Examples
  - Analysis of Competing Hypotheses
  - Devil's Advocate
  - Chronology
  - Red Team Analysis

SATs in Cyber Threat Intelligence

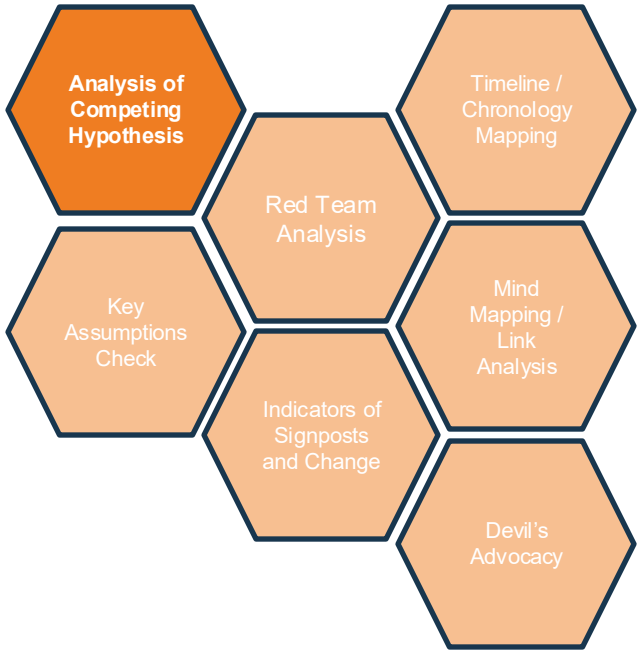
- Importance of SATs in CTI
  - Deception
  - Confirmation bias
  - Time pressure
  - Financial risk

Core Techniques



Analysis of Competing Hypothesis

- What is it?
  - Matrix based technique for comparing multiple hypotheses against evidence to see which hypothesis is most consistent

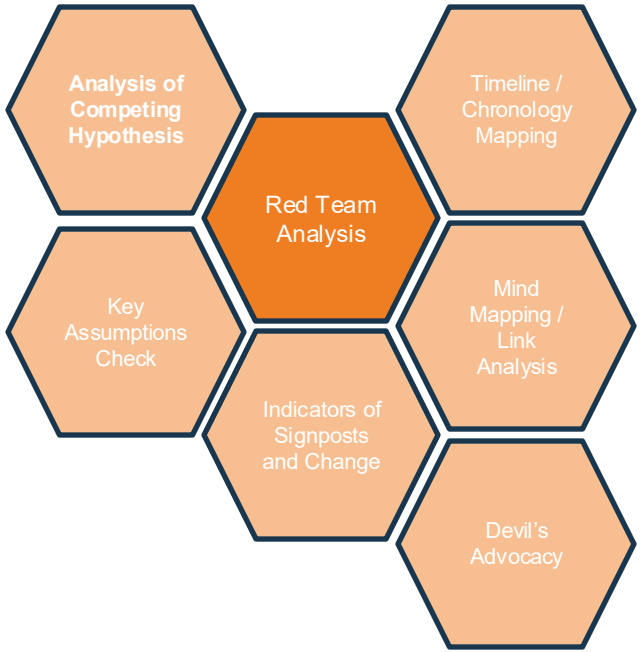


Key Assumptions Check

- What is it?
  - Technique to identify and challenge the assumptions that underpin your analysis

Red Team Analysis

- What is it?
  - Analysts take on the role of the adversary to understand their objectives, constraints, and likely next moves.

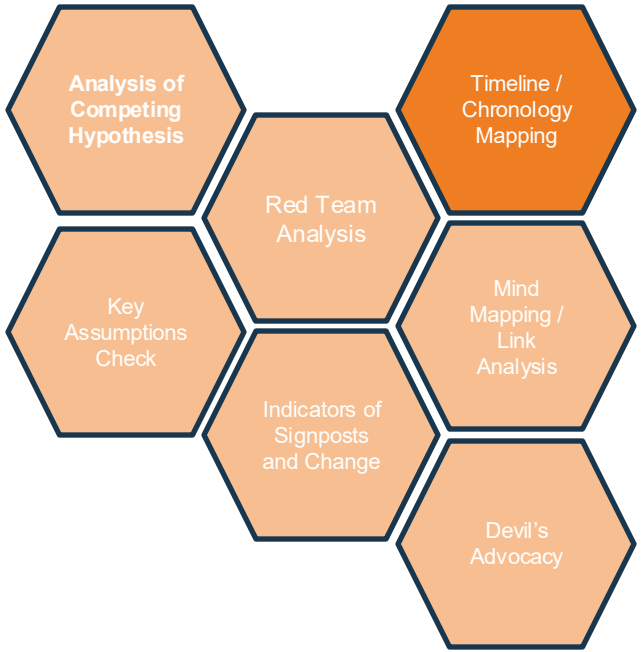


Indicators of Signposts & Change

- What is it?
  - A method to monitor whether your hypothesis continues to be supported over time.

Timeline / Chronology Mapping

- What is it?
  - Organizes events in time to find gaps, triggers, or patterns that suggest causality or coordinated activity.



Mind Mapping / Link Analysis

- What is it?
  - Visually connects people, infrastructure, malware, behaviors, and events.

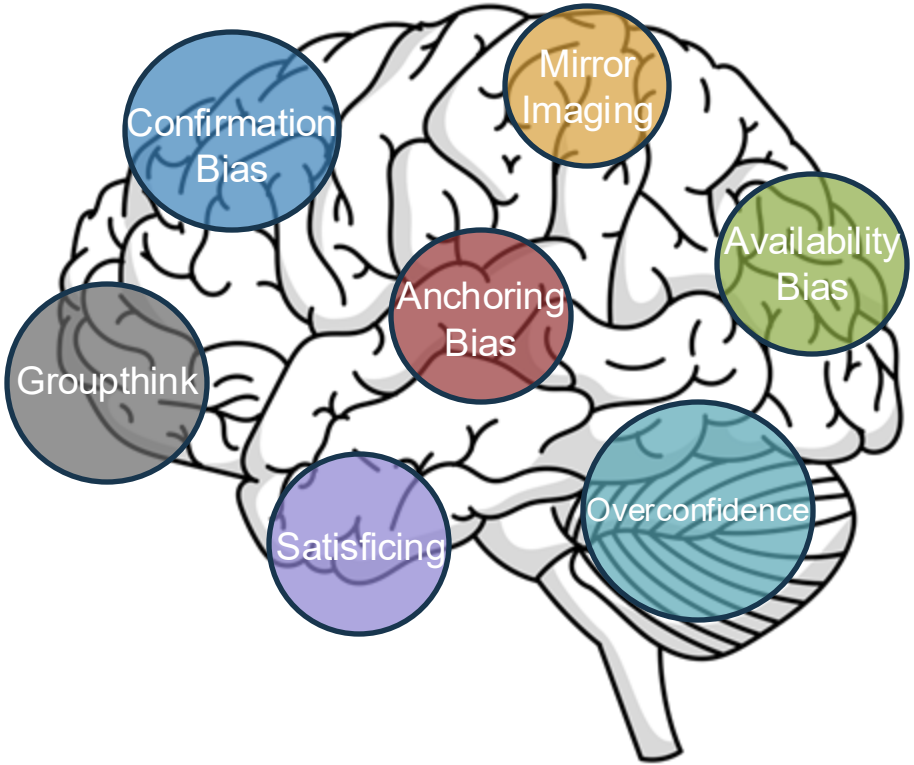
Devil's Advocacy

- What is it?
  - Arguing against the prevailing analysis to find weaknesses.

Bias Is Inevitable

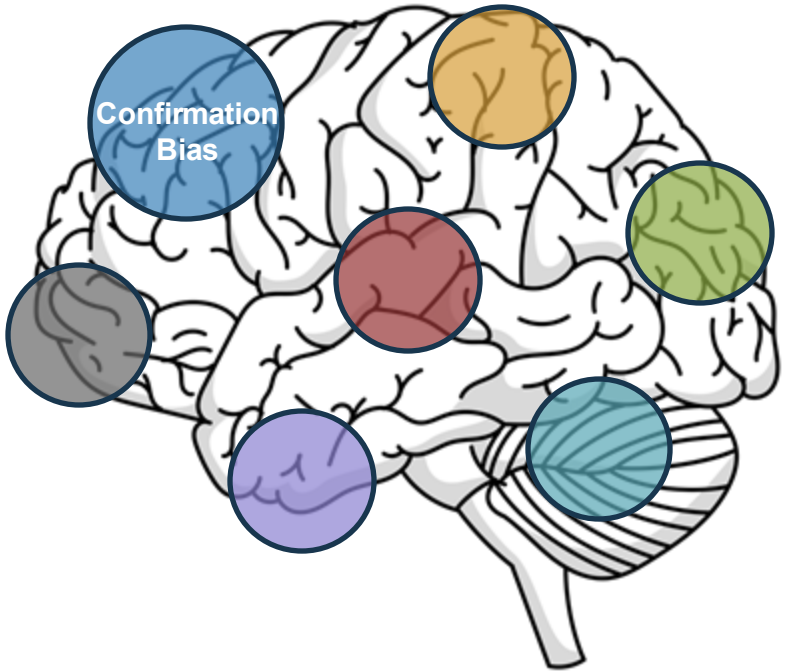
- What causes bias?
- What are the different kinds of biases?
- How do we overcome bias?

Bias & Cognitive Traps



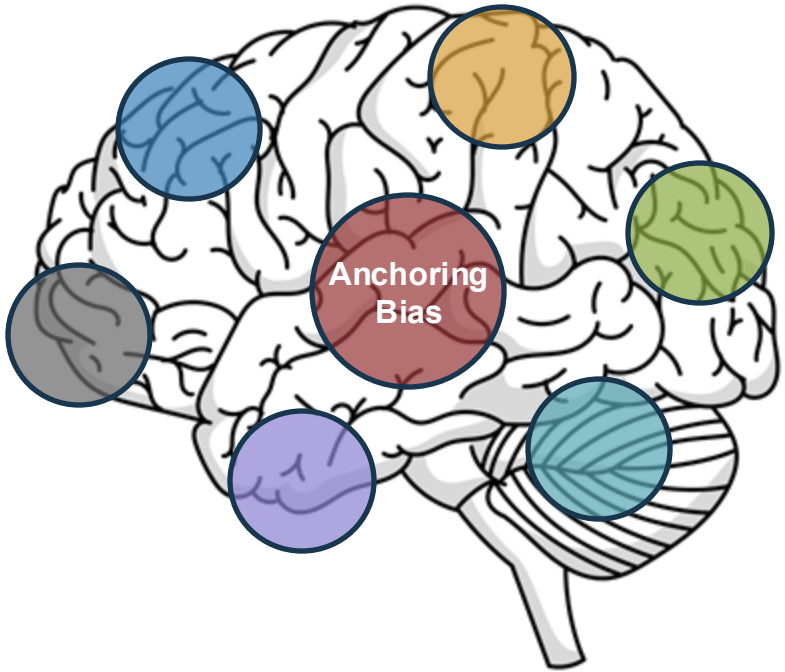
Confirmation Bias

- What is it?
  - Tendency to favor or interpret information that supports existing beliefs.
- Why it matters?
  - Poor attribution
  - Blind spots
  - Misidentification of TTPs
- Mitigation
  - Analysis of Competing Hypotheses



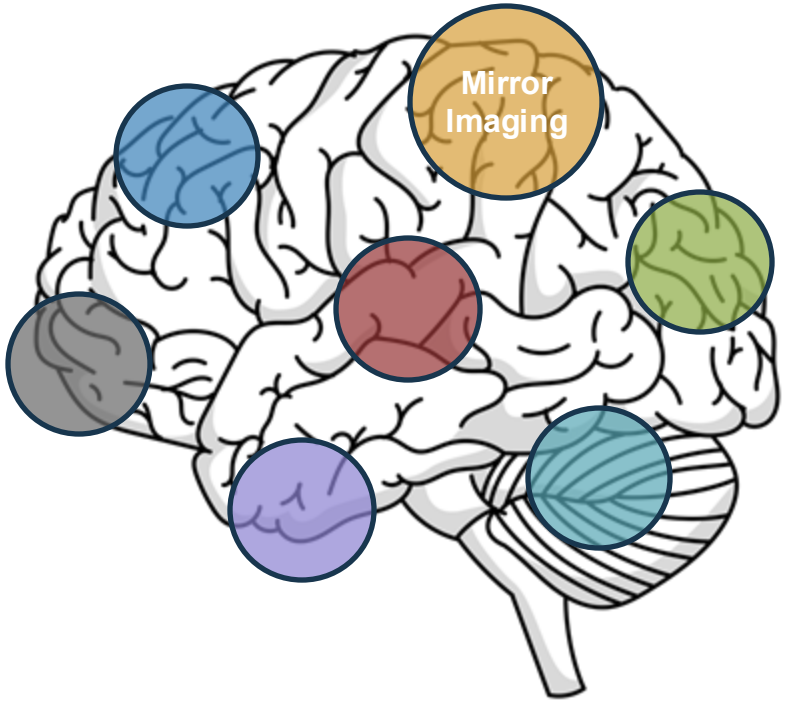
Anchoring Bias

- What is it?
  - Relying too heavily on the first piece of information received when making decisions
- Why it matters?
  - Skews analysis toward viewing further evidence
- Mitigation
  - Key Assumptions Check



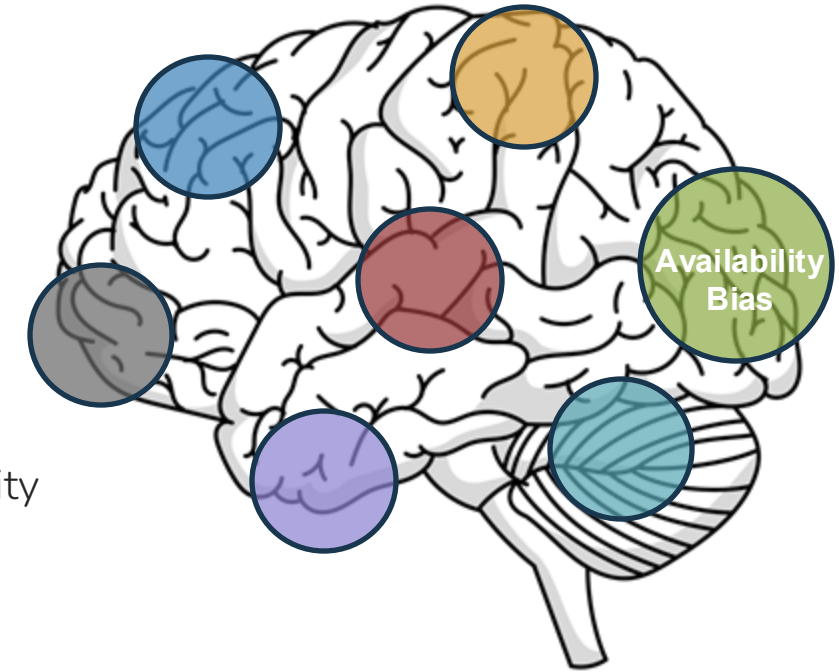
Mirror Imaging

- What is it?
  - Assuming the adversary thinks, prioritizes, or acts the way you might.
- Why it matters?
  - Flawed threat modeling
  - Misjudging adversary goals or tactics
- Mitigation
  - Red Team Analysis



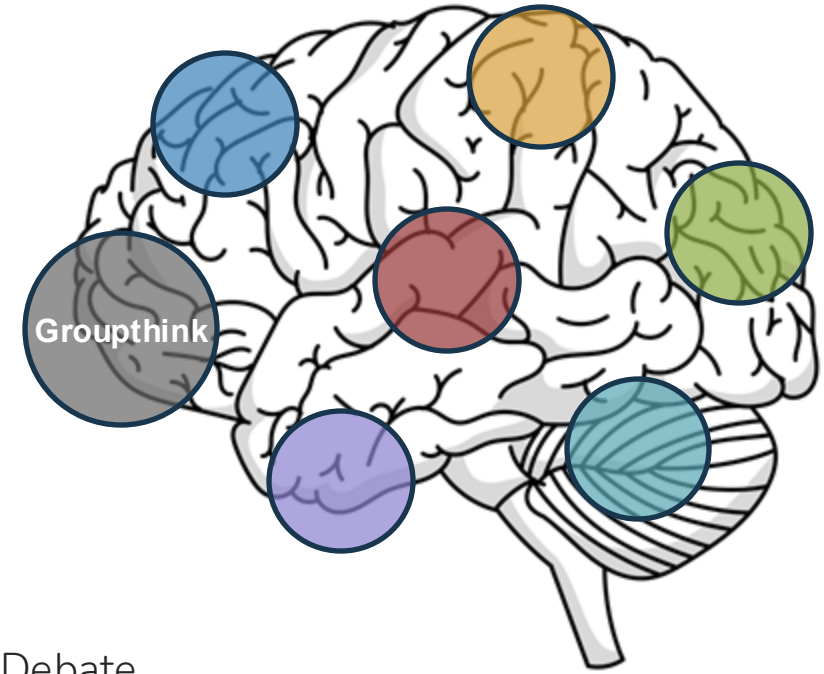
Availability Bias

- What is it?
  - Reliance on recent, vivid, or easily recalled events instead of actual probability or relevance.
- Why it matters?
  - Overweights recent attacks or high-profile campaigns
  - Ignores broader trends and low-visibility threats
- Mitigation
  - Timelines & Historical Analysis



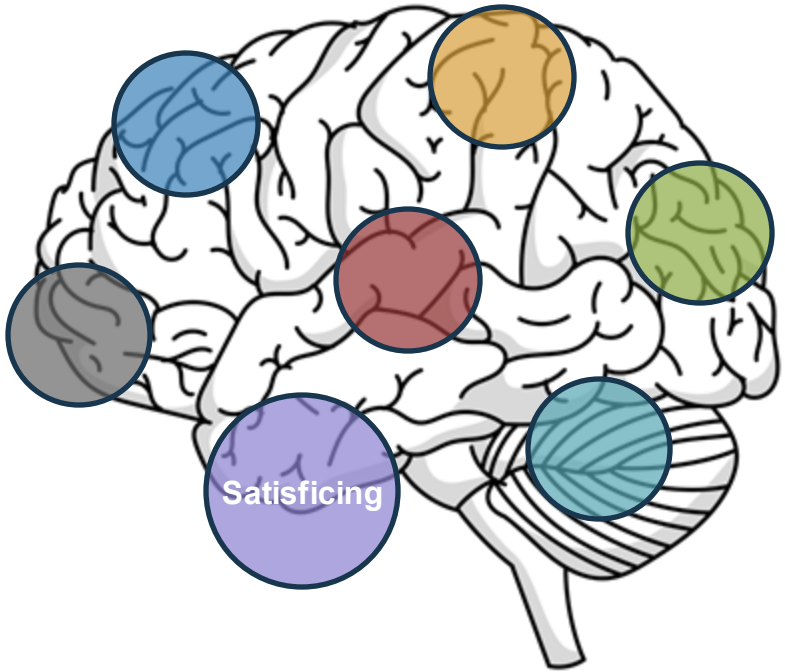
Groupthink

- What is it?
  - Pressure to conform to consensus opinions within a team, suppressing dissent or alternative ideas.
- Why it matters
  - Prevents challenging flawed assessments
  - Reduces creativity
  - Can lead to analytic failures
- Mitigation
  - Devil's Advocacy or Structured Team Debate



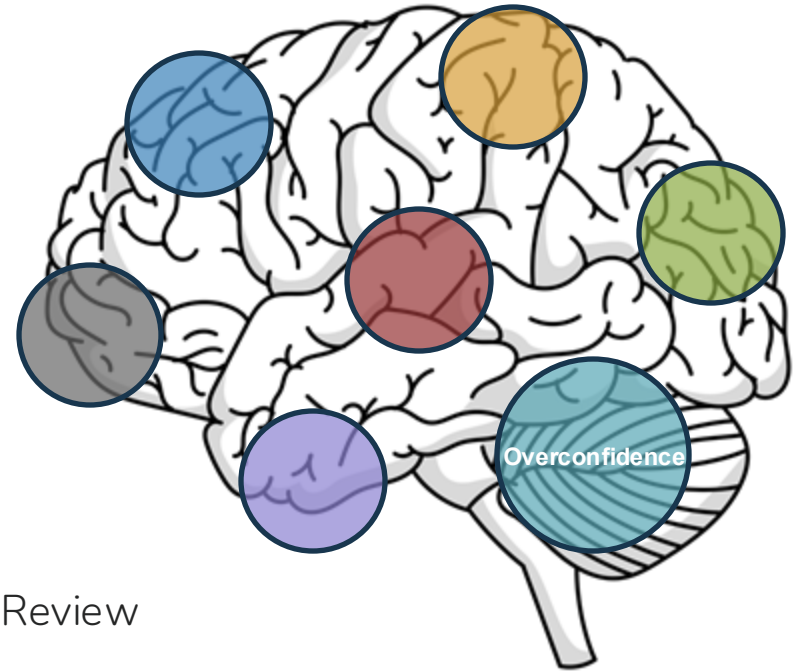
Satisficing

- What is it?
  - Stopping at the first “good enough” answer instead of continuing to explore better, more accurate explanations.
- Why it matters
  - Shallow analysis
  - Missed threats
- Mitigation
  - Indicators and Signposts of Change



Overconfidence

- What is it?
  - Overestimating the accuracy, completeness, or value of one's own analysis.
- Why it matters
  - Leads to rigid assessments
  - Poor stakeholder communication
  - Disregard for new evidence
- Mitigation
  - Confidence Rating Frameworks + Peer Review



Takeaways

- Structured Analytical Techniques = Tools for thinking critically under pressure
- Cognitive Biases = Hidden obstacles that can derail your judgement
- Combining SATs with bias awareness builds more rigorous, transparent, and actionable threat intelligence.

Sector ISACs, Government Partnerships, & Information Sharing Protocols

ISAC Origins & Governance

- Information Sharing and Analysis Centers
  - Presidential Decision Directive 63
  - Non-profit, member driven organizations
  - Critical infrastructure protection
- Major ISACs by Sector
  - Financial
  - Healthcare
  - Energy
  - IT
  - Auto
  - Multi-State Government
  - Aviation

How Do ISACs Operate?

- Threat data ingested by cleared analysts, technical platforms, and real-time feeds
- Data enrichment
- Data redistribution

Government Partnerships

- Bridging private and public sectors
- Rapid sharing of classified and unclassified cyber threat data
- Mutual coordination
- Resilience and recovery
- Federal Players
  - CISA
  - NSA Cybersecurity Directorate
  - FBI InfraGard
  - DoD/DC3
  - DOE, HHS, DOT, Treasury
  - USSS Electronic Crimes Task Force
  - USSS Cyber Fraud Task Forces

Information Sharing

- TLP labels to control distribution
- STIX packages
- Push/pull via TAXII
- Integration into tools
  - SIEMS (Elastic, Splunk)
  - TIPs (ThreatConnect, MISP, Anomali)
  - SOAR platforms

Real-World Examples

- SolarWinds (2020)
  - NSA detected lateral movement
  - Microsoft and FireEye discover supply chain compromise
  - CISA coordinated disclosure and mitigation
  - STIX package with SUNBURST IOCs were shared
- Colonial Pipeline(2021)
  - FS-ISAC shared threat indicators related to DarkSide
  - MS-ISAC disseminated guidance to SLTT agencies
  - DHS/CISA coordinated private briefings for utility sectors

Analyst Guidance & Takeaways

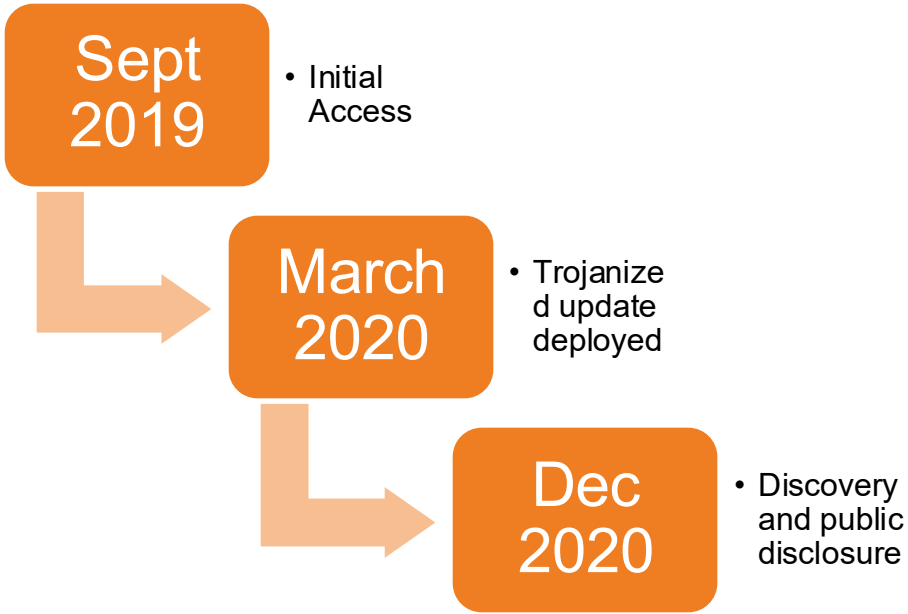
- Join an ISAC relevant to your sector
- Set up automated sharing
  - Configure TIPs with STIX/TAXII access
  - Ingest MISP feeds into SIEMs
- Build relationships
- Share Intelligence

Real-World CTI Applications

Case Study: APT29 & the SolarWinds Supply Chain Compromise

- Background
  - SolarWinds Orion platform used by thousands of orgs, including the U.S. government
  - Compromise discovered by FireEye in December 2020
  - SUNBURST backdoor was silently embedded via software update

Timeline of Events



Threat Actor Profile – APT29 (Cozy Bear)

- Russian SVR-linked group
- Previously associated with DNC hack (2016)
- Known for stealthy espionage, long dwell time, strong OPSEC

TTPs Observed

- Supply chain compromise
- SAML token forgery
- Use of native Windows tools (LOLBAS)
- C2 over HTTPS disguised as normal traffic

Intelligence Levels Applied

- Strategic: National security implications, vendor risk
- Operational: Tracking C2 infrastructure
- Tactical: Mapping TTPs to ATT&CK
- Technical: IoCs (hashes, domains, URLs, certs)

CTI Collaboration in Action

- FireEye, CISA, Microsoft, Volexity cooperation
- STIX/TAXII sharing and GitHub repos
- TLP Red > TLP Amber > TLP White

Lessons Learned

- CTI must include vendor trust models
- Detection requires telemetry beyond malware
- Attribution influences public/private response

Case Study: NotPetya and the Weaponization of Ransomware

- Context & Initial Beliefs
  - June 2017: Global attack initially thought to be ransomware
  - Targeted Ukraine via MeDoc software
  - Demanded BTC ransom, but keys non-functional

Key Characteristics of the Attack

- Wiper, not ransomware
- Exploited EternalBlue & EternalRomance
- Credential harvesting with Mimikatz
- Lateral movement via PsExec

Attribution Timeline

- Early confusion: ransomware vs nation-state
- Later attribution to Russian GRU (APT28/Sandworm)
- Target: destabilization of Ukraine, economic damage

CTI Missteps & Assumptions

+ Mistaken ransomware classification delayed proper response
+ Lack of immediate cross-sector sharing
+ Overemphasis on malware = missed strategic intent

CTI Application by Level

- Strategic: Nation-state cyberwarfare and deterrence
- Operational: Impact analysis across orgs
- Tactical: Lateral movement techniques, propagation methods
- Technical: IoCs and YARA rules

Impact on Global Companies

- Maersk, FedEx (TNT Express), Merk, Saint-Gobain
- $10B+ in total damages
- **Highlight:**
  - Maersk rebuilt its AD infrastructure from a single untouched domain controller in Ghana

Lessons Learned

- Attribution isn't just "whodunnit" – it's about intent
- CTI must continuously reassess the why of attacks
- Strategic and operational intel can't lag behind technical findings

Takeaways

- CTI is dynamic – it must evolve with adversaries
- Attribution is a lens, not a conclusion
- Intelligence must be timely, shared, and multi-level
- Real-world CTI blends strategic insight with technical details
- Collaboration is essential: no one organization sees the full picture

Intelligence in Threat Hunting - Summary

Key Concepts

+ **The Intelligence Lifecycle**

+ **Types of Threat Intelligence**

+ **Integration into Cyber Defense**

LEARNING OUTCOMES

+ Explain purpose and phases of CTI Lifecycle
+ Differentiate between types of CTI
+ Enrich and correlate IoCs
+ Integrate CTI into detection and defense workflows
+ Apply frameworks such as MITRE ATT&CK and STIX/TAXII
+ Evaluate CTI quality and assess its role in cyber defense

Next Steps

+ Continue with Threat Hunting learning path

Thank you!

Intelligence in Threat Hunting

- Keep your brain open
- Think critically
- Connect the dots
- And most of all – get ready to make threat intelligence actionable.

EXPERTS AT MAKING YOU AN EXPERT