> INITIALIZING TALK ... [ACCESS GRANTED]

SOLVING FOR Y

The “Secret” formula to opening doors, triggering curiosity and to tackle the challenges you find in Cybersecurity.

[HRTBRKRNR]

Cybersecurity Analyst // CTF Runner // Cyberpunk Enthusiast

BSides Delaware // [2026]

ABOUT

[HRTBRKRNR] Amber Kirylak



bio.txt

```
role      : "Information Security Analyst"
focus     : "Blue Team // Threat Hunting –> Detection Engineering"

[2011] // BFA, Univ. of the Arts. Over a decade in photography & post-production.
[2020] // lockdown hits. Harvard drops CS50x for free. Curiosity: rebooted.
[2020–2022] // found the right mentors, broke in. First role: GRC.
[2025.01] // WiCyS Scholarship (2024–25) — SANS GFACT/GSEC/GCIH/GCCC cleared.
[2025.08] // pivoted to Security Operations. Currently running defense ops.

next_target : Security Engineer // Threat Hunter // Detection Engineering
```

// CERTIFICATIONS & CREDENTIALS



00

AGENDA

agenda.sh

01	[THE PROBLEM]	*Problems are like puzzles — a thousand pieces, no box art to guide you.*
02	[THE FORMULA]	*Same shape, every domain: Z = X + Y.*
03	[THE GAP]	*90% of solving it is approach. 10% is what you already know.*
04	[THE APPROACH]	*Night City wasn't built in a day — neither is your understanding.*
05	[EXAMPLE]	*Solving for Y, start to finish — one real alert, walked all the way through.*

reality_check.log

“ CYBER SECURITY IS NOT AN ENTRY-LEVEL CAREER. ”

— walked in with a Fine Arts degree. No tutorial level, no roadmap.
You do not have to begin as an expert. It is about how you invest your time in navigating, and retaining information over time.

> DOMAIN 01 // INITIALIZING

01

[THE PROBLEM]

Problems are like puzzles — a thousand pieces, one picture, no box art to guide you.

01

[FACING THE CHALLENGE]

What do you do when you're handed a challenge you do not understand? (Imagine 1000 jigsaw pieces)

- Do you sort the pieces by shape, color, or signature?
- Do you start with the corners, then edges, or do you go by patterns and colors?
- Are you doing this by yourself or do you have a team?
- Are you committed to completing it all in one day or do you know when to take a step back to see the “bigger picture”?
- Do you know when to ask for help?



01

[WHEN YOU DON'T KNOW YET]

How are you approaching the challenge?

- How good are you at journaling your journey?
- Are you asking AI for the end-all-be-all answer, or are you earning it yourself?
- Do you give up when you hit a wall, or are you persistent and push through?
- Do you read directions first or jump right into troubleshooting?
- Do you push forward to do it all at once, or do you know when it is time to take a break?



01

Some challenges can appear to be a big scary monster



01

Really, all the big scary monster needs is a hug.



> DOMAIN 02 // INITIALIZING

02

[THE FORMULA]

Same shape, every domain: Z = X + Y. Today we run it through Security Operations.

> THE FORMULA

Z = X + Y

The alert / ticket that gets generated.

All your data — logs, telemetry, packets, files, commands, processes, event codes.

What we're solving for. More on this next.

// Framed here through Security Operations — swap the nouns and the same formula runs on any domain.

2a

[OTHER EXAMPLES]

Same formula, three more lenses — swap the nouns, run it again.

1

GRC

Z = The Audit Requirement **X** = All the data you're collecting **Y** = The purpose behind collecting it

2

THREAT HUNTING

Z = The MITRE ATT&CK TTP **X** = All the data you're collecting **Y** = The patterns you're observing

3

TROUBLESHOOTING 101

Z = The Problem **X** = All the data you're collecting **Y** = The behaviors you're observing

> WHAT IS Y?

Z - X = Y

The alert / ticket that gets generated.

All your data — logs, telemetry, files, and more.

The logic that turns X into Z.

Short answer: Y is the event of interest we are identifying.

> Why is the logic we are detecting important?
> Is the alert logic being built significant enough to investigate?
> Why are we building for Y in the first place? Threat Hunting? Suspicious Activity? Policy Violation?

> DOMAIN 03 // INITIALIZING

03

[THE GAP]

90% of solving it is approach. 10% is what you already know.

03

[MIND THE GAP]

01

90 / 10 SPLIT

You already know the 10%. Finding the 90% is all about approach.

02

NOT OMNISCIENT

Not a SME? No problem. Can you learn a new skill outside your comfort zone?

03

OK NOT TO KNOW

Are you asking the right questions or did you do the research to ask the right questions?

04

AI ISN'T THE “SOLE” ANSWER

Remember AI is a tool! Do you know how to use it? Do you understand the data it is trained on? Do you understand how to prompt?

> KEY WORD

CRITICAL THINKING

How do you find the Y?

> What do you do when there's no AI to guide you?
> What resources do you have to find the answers to the questions you are asking?
> Pieces of the puzzle are your data, can you fit them together and is it meaningful?
> Do you know someone who understands it better? Is there someone out there?

> AI CONSIDERATION

Remember: AI isn't the "SOLE" answer.

When leveraging AI to solve problems, consider the following:

1. **What model will you be using?**
2. **Do you know how to prompt?**
3. **Have you considered training related to the models you are using (e.g. ChatGPT, Claude)?**

Don't just ask AI for the answer and treat it as a source of truth: that's a search engine. Take the time to interrogate the model and ask where it got its sources. Hallucinations happen, so **call them out.**

AI is a tool — learning to use the tools to fit your goals is part of the journey to help you be successful using them.

This goes for non-AI tools and skills, too.

> DOMAIN 04 // INITIALIZING

04

[THE APPROACH]

Night City wasn't built in a day — neither is your understanding.

//

[KEY TRAITS OF PROBLEM SOLVING]

[THE MINDSET]

- Curiosity — always ask why.
- Patience — the answer isn't instant.
- Being hungry — chase the next unknown.
- Staying humble — you don't know it all.

[THE METHOD]

- Know your resources — the internet, tools (e.g. Platforms and AI), people.
- Be creative — thinking outside the box is half the battle.
- Question everything — assumptions included.
- Document everything — for future-you, and everyone after.

“ The Internet is the World’s Library, use it wisely. ”

— Lucie G. Kirylak

04

[HOW TO APPROACH IT]

Three habits before you touch the puzzle.

1

PATIENCE

Night City wasn't built in a day. Reading, writing, learning, and building all take time.

2

HUMILITY

Not knowing is part of the process. Imposter syndrome is loud!!! No one is born knowing it all.

3

BYTE-SIZE IT

Foundations are key. Take one piece of the puzzle at a time, then build outward from there.

> DOMAIN 05 // INITIALIZING

05

[EXAMPLE]

Solving for Y, start to finish — one real alert, walked all the way through.

> THE SCENARIO

Arasaka SOC flags an impossible travel alert on Anders Hellman, Director of Special Projects. Consistent logins from Arasaka Tower, Night City — then, minutes later, a login from Shenyang, China. No known travel plans. No VPN change.

[Z] azuread_signin_logs.csv

ARASAKA SOC · ALERT TRIAGE

Impossible Travel: Soulkiller Access from Shenyang

```
$ index=azure sourcetype=azure:aad:signin userPrincipalName="a.hellman@arasaka.com" | sort _time
```

#	TIME	APP	IP ADDRESS	LOCATION	RISK
1	2026-10-12T05:07:44Z	Arasaka365 Exchange Online	198.51.100.24	Santa Monica, California, US	none
2	2026-10-12T05:26:31Z	Arasaka365 Exchange Online	198.51.100.24	Santa Monica, California, US	none
3	2026-10-12T05:48:02Z	Arasaka365 Exchange Online	198.51.100.24	Santa Monica, California, US	none
4	2026-10-12T06:31:17Z	**Soulkiller**	203.0.113.88	Shenyang, Liaoning, CN	HIGH
5	2026-10-12T06:58:40Z	Arasaka365 Exchange Online	198.51.100.24	Santa Monica, California, US	none

ROUTE	TIME BETWEEN SIGN-INS	DISTANCE	REQUIRED SPEED
Santa Monica → Shenyang	43 min	~9,500 km	~13,200 km/h

Fictional scenario for BSides Delaware. All data is simulated; IPs are from RFC 5737 documentation ranges.

$$Z = X + Y$$

> THE DATA

This is X — the raw signal behind the alert, pulled straight from Azure AD Identity Protection. Same account, same timestamp, same incident — just one layer deeper.

[X] risk_detection_8841.json


```
{
  "riskEventType": "impossibleTravel",
  "riskState": "atRisk",
  "riskLevel": "high",
  "detectedDateTime": "2026-10-12T09:14:02Z",
  "ipAddress": "203.0.113.88",
  "userPrincipalName": "a.hellman@arasaka.com",
  "location": { "city": "Shenyang", "countryOrRegion": "CN" },
  "previousLocation": { "city": "Santa Monica", "countryOrRegion": "US" }
}
```


$$Z = X + Y$$

> THE LOGIC

This is Y — the detection logic that turns raw telemetry into a HIGH risk verdict. Two sign-ins, one impossible speed between them — that's the whole rule.

[Y] detect_impossible_travel.spl

```
index=azure_ad sourcetype=signinLogs earliest=-15m
| streamstats last(city) as prev_city, last(_time) as prev_t by user
| eval km=geodist(prev_city, city), mins=(_time-prev_t)/60
| eval max_kmh=km/(mins/60)
| where max_kmh > 900 AND mins < 120
| eval riskEventType="impossibleTravel", riskLevel="high"
| table user, prev_city, city, max_kmh, riskLevel
```

Adapted from a real Sigma HQ detection rule, converted to SPL.

github.com/SigmaHQ/sigma — rules/cloud/azure/identity_protection/azure_identity_protection_impossible_travel.yml

$$Z = X + Y$$

> WHY SOLVE FOR Y?

Z − X = Y

Z = THE ALERT · **X** = THE DATA · **Y** = THE LOGIC + WHY IT MATTERS

Why does impossible travel matter?

01 Physically impossible, full stop. Even the Concorde took longer to cross that distance than this logic takes to catch it.

02 A valid account is a foothold. Compromised credentials enable initial access, persistence, privilege escalation, and defense evasion. *(MITRE ATT&CK T1078)*

03 Login is available on the public web. Anybody can access it!!!

04 Credentials get compromised easier than we'd like to admit. Weak policies, leaks, reuse, phishing... or just being human.

05 ~3 devices per person, on average. That's a lot of endpoints and identities to keep track of.

06 VPN or no VPN — that is the question. Legitimate remote access can look just as “impossible” — until you check.

> BONUS FINDING

Arasaka SOC has identified an additional alert related to data exfiltration from the user's account. Traffic from IP address 203.0.113.88 moved out to a ChromeDrop cloud service for exfiltration.

[+] microsoft365_data_exfiltration_to_unsanctioned_app.yml

ARASAKA SOC · BONUS: EXFILTRATION

Data Exfiltration: Project Soul Killer → ChromeDrop

Sigma rule **Data Exfiltration to Unsanctioned Apps** (T1537) converted to Splunk SPL

```
index=o365 sourcetype="o365:management:activity"                    ← SIGMA RULE (CONVERTED)
  eventSource="SecurityComplianceCenter" eventName="Data exfiltration to unsanctioned apps" status="success"
| eval data_gb = round(bytes_out / 1024 / 1024 / 1024, 1)
| table _time user src_ip dest_app file_path file_count data_gb
| rename user AS "User", src_ip AS "Source IP", dest_app AS "Destination App",
        file_path AS "Source Folder", file_count AS "Files", data_gb AS "Data (GB)"
| sort - _time
```

TIME	USER	SOURCE IP	DEST APP	SOURCE FOLDER	FILES	DATA (GB)
2026-10-12 08:02:51	a.hellman@arasaka.com	203.0.113.88	ChromeDrop	/sites/RnD/Project Soul Killer/	1,847	56.4

DATA EXFILTRATED	FILES	UPLOAD WINDOW	DESTINATION
56.4 GB	1,847	49 min · 07:14–08:02	ChromeDrop unsanctioned

Fictional scenario for BSides Delaware. All data is simulated; ChromeDrop is a fictional service. Only the highlighted search comes from the Sigma rule; other fields are illustrative.

> SCENARIO ANSWER

After additional investigation using several tools and platforms, the Arasaka SOC collected additional information and concluded:

Arasaka SOC traced it to Kang Tao's HQ in Shenyang. A rival corp! Valid MFA push. Connection to Kang Tao's ISP. This wasn't impossible travel; it was a real session, from the wrong side.

Manager Yorinobu Arasaka confirmed it: Hellman was MIA. No expected travel plans! Not answering the call! Access revoked, sessions killed, workstation isolated within minutes of approval.

The alert fired. The control didn’t. DLP flagged the restricted-data upload correctly, but detection isn’t prevention. A missed or misconfigured block action means the data still walks out the door.

Conclusion: Classification: Critical Insider Threat. Privileged R&D, Soulkiller research, engram technology. Arasaka Security is now hunting for exfiltration.

> LESSONS LEARNED

01 There's a reason every alert exists; however is the alert valuable. It's not just “because” there's purpose behind it. Is the alert valuable to your organization or is it just noise?

02 You're collecting all this data, but why? Is it just because audit told you to? Data is what builds the alerts so what data do you actually have?

03 The logic isn't there because someone thought it mattered. The real question is why it matters. Ask yourself:

- → Does it map to something like MITRE ATT&CK?
- → Do you have real-world examples?
- → Is the logic creating value or noise?

> KEY TAKEAWAY

TLDR: Not every event is a threat, and not every event deserves an alert. Detection logic helps us identify what matters. The key is understanding why it matters.

THANK YOU

> LET'S CONNECT

[WEBSITE]



https://www.HRTBRKRNR.com

[LINKEDIN]



[STAY CURIOUS // STAY SHARP // END TRANSMISSION]