<hunter_strategy>

Less Resources, More Impact: Doing More With Less In Cybersecurity

Jake Williams, VP R&D
Jake.Williams@hunterstrategy.net

cat /home/jake/bio.txt

VP of R&D, risk manager, breaker of code, responder of incidents

IANS Faculty Member, former SANS Senior Instructor and Course Author

Frequent eye bleach user thanks to the Biden laptop…

Two-time winner of the annual DC3 digital forensics challenge

Former NSA hacker, Master CNE operator, recipient of the DoD Exception Civilian Service Medal

Cyber skills formally endorsed by Russian intelligence

Agenda

You have less.

The mission hasn't changed.

Actually, it has. Now you have more to do.

And no more resources to do it with...

The "Situation"

Budgeting? Good luck with that...

<hunter_strategy>

Budgets are flat

Few are seeing increases in their cybersecurity budgets.

Costs Are Up

Nobody can seemingly put finger on why, but costs are up… 🤷 🤷 🤷

Photo: licensed Adobe Stock

Even Flat Budgets Lose Ground to Inflation

Real talk: If your budget isn't growing, **it's shrinking.**

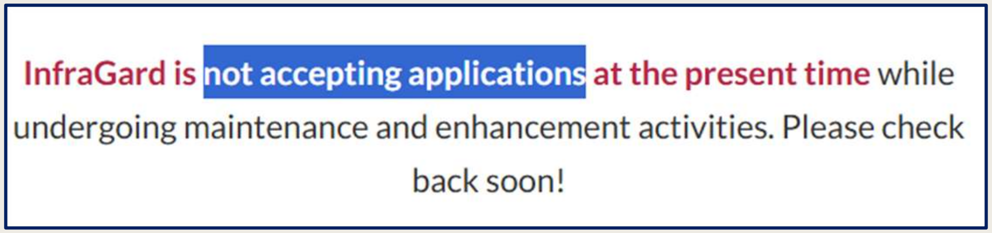
Degraded/Absent Free Services

NVD is all but dead.

InfraGard: where are you?

ISACs impacted by membership cuts.

Decreased reporting from CISA (and lower trust in what we're still getting).



InfraGard is not accepting applications at the present time while undergoing maintenance and enhancement activities. Please check back soon!

Photo: licensed Adobe Stock

The Answer is AI!

Who *doesn't* want to add a bullsh*t artist to their business-critical workflows?

AI - Whether You Want It Or Not...

A primary enterprise use case today for AI seemingly is diverting investment dollars from proven technologies while creating new attack surfaces for security teams (with no new budget for allocated for its defense).

Doing More With Less

All joking aside, what should we be doing?

Budget Security Goals: Data > Prevention

- If you lack resources to stop the majority of attacks, focus on having the data for detection and investigation.
- That data will help prioritize future security efforts when you have budget and time.

No SIEM Budget? At Least Keep Local Event Logs!

Increase the size of your event logs with GPO

- There's no reason for 20MB default sizes before event logs roll over

Whether or not you use a SIEM, increasing local storage for event logs is critical

- But as long as the logs haven't rolled over, they're available for investigations

Start With a Zero-Base Review

Inventory everything in your security program - it you dedicate capital to it (money or human), quantify the cost and outcomes it enables.

Precision doesn't matter as much as understanding relative cost and value.

Get rid of sunk cost bias.

"Pet projects" don't get a pass.

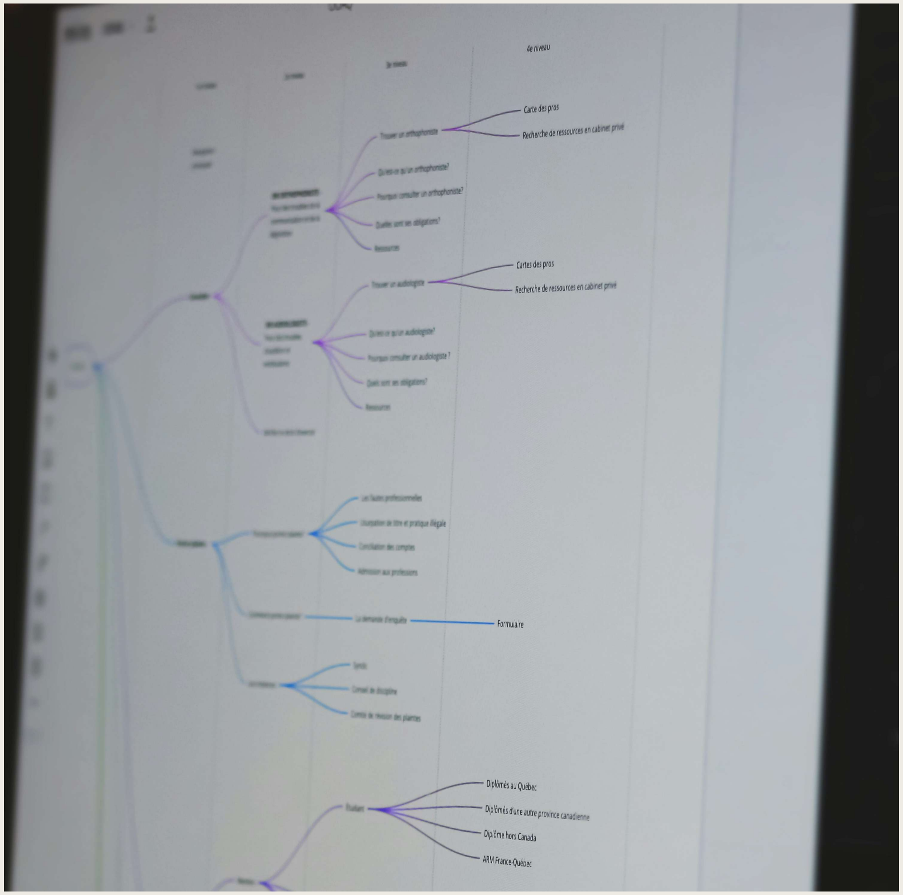

4e niveau
Carte des pros
Recherche de ressources en cabinet privé
Cartes des pros
Recherche de ressources en cabinet privé
Formulaire
Diplômés au Québec
Diplômés d'une autre province canadienne
Diplôme hors Canada
ARM France-Québec

Photo by Sigmund on Unsplash

Write a Security Program Charter

You know your resources. Honestly evaluate what you can't do.

Write a charter documenting that and get an executive sponsor to approve.

Key insight: You're better off having adult discussions about what you aren't doing than stretching so thin you're doing security poorly.

Pro Tip: Don't write a charter that consumes all of your resourced hours. This is security. 💩 💩 💩 happens.

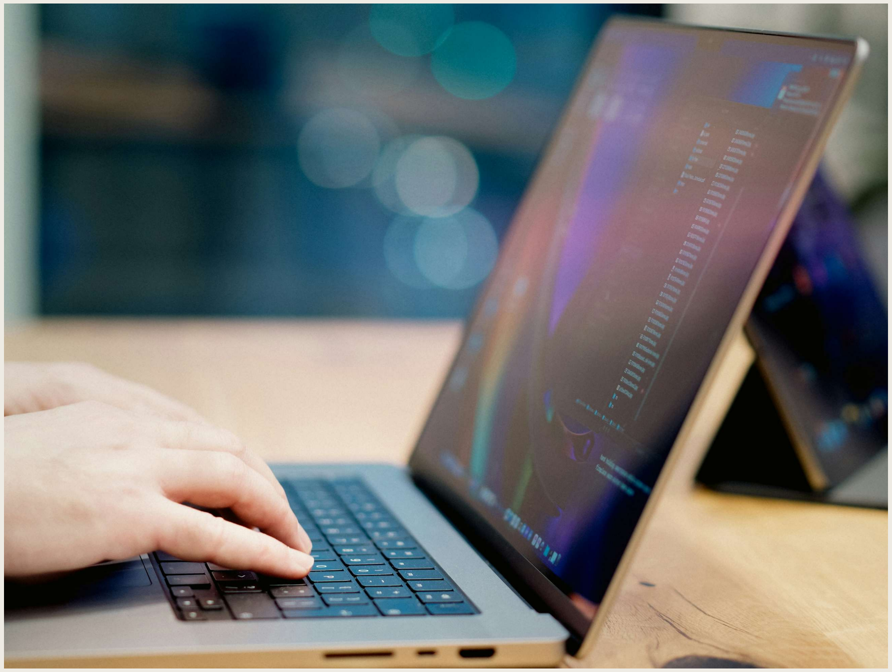


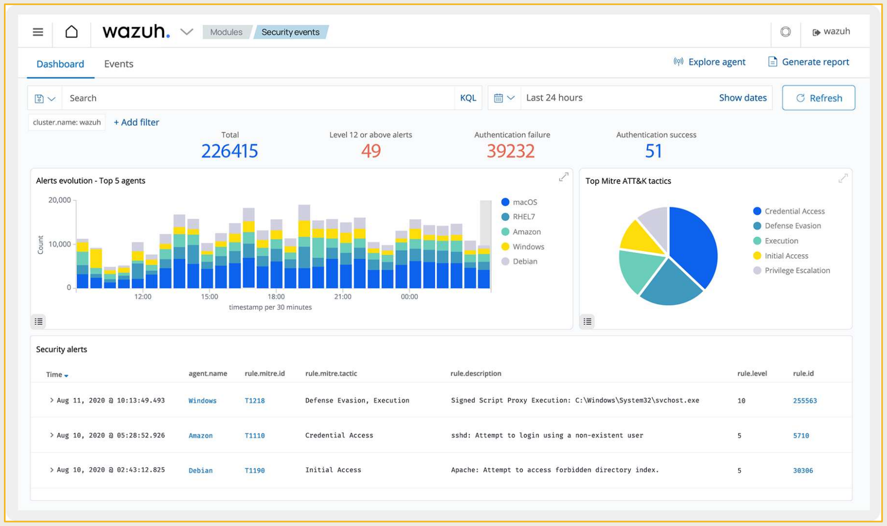
Photo by Jakub Żerdzicki on Unsplash

Deploy Security Onion for NSM

- Most firewall logs are not sufficient for incident investigations
  - Don't wait for an incident to find this out
- Security Onion is **trivial** to deploy
- It runs just fine on legacy (lifecycle replacement) server hardware for almost any SMB/SME sized network
  - Full disclosure: Security Onion isn't necessarily something I'd use in some very large security deployments, but that's probably not what we're talking about here...
  - You don't need to do any configuration, just let it run

SIEM Licensing Got Cut?

- Security Onion (NSM mentioned earlier) runs an ELK stack that can be configured to ingest data from other sources.
- If you can deploy a dedicated SIEM in addition to NSM, consider Wazuh as an open-source solution.
- Side benefit: Wazuh also has endpoint agents that can serve as EDR if you can't afford a commercial agent.



Total	Level 12 or above alerts	Authentication failure	Authentication success
226415	49	39232	51

Security alerts

Time	agent.name	rule.mitre.id	rule.mitre.tactic	rule.description	rule.level	rule.id
Aug 11, 2020 @ 10:13:49.493	Windows	T1218	Defense Evasion, Execution	Signed Script Proxy Execution: C:\Windows\System32\svchost.exe	10	255563
Aug 10, 2020 @ 05:28:52.926	Amazon	T1110	Credential Access	sshd: Attempt to login using a non-existent user	5	5710
Aug 10, 2020 @ 02:43:12.825	Debian	T1190	Initial Access	Apache: Attempt to access forbidden directory index.	5	30306

Deploy Sysmon for Endpoint Telemetry

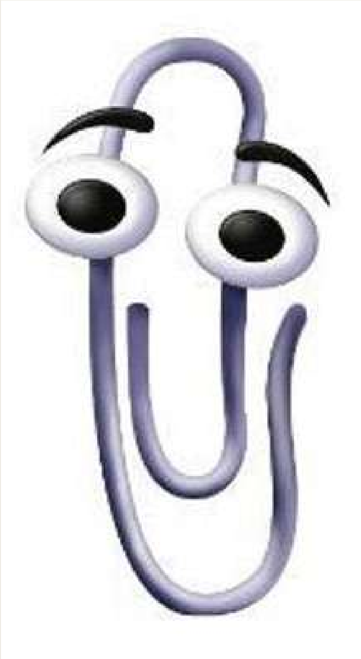
Sysmon is the Clippy of Windows Event Logs.

If your EDR budget is cut, consider deploying Sysmon so you at least are getting decent telemetry.

Forward the data to an ELK server using Windows Event Forwarding.

Pro Tip: Check out Olaf Hartong's modular Sysmon configuration repo:

- https://github.com/olafhartong/sysmon-modular



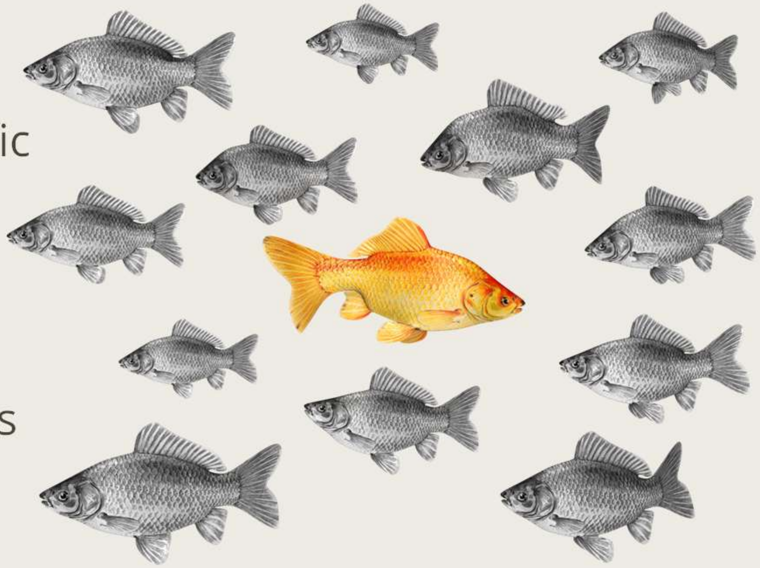
Look for Non-Standard Tooling Options

Look at native tooling options where you can to find close capability gaps created by budget consolidation.

- Sysmon can be configured monitor all changes to specific files: change control
- Azure ARM Templates: configuration management

During budget consolidation, look to pay-as-you-go services

Pro Tip: Use platform-native tools for security in cloud deployments. With the right maneuvering, the cost can get absorbed into ops budgets.



Use Your Logo Power

Every year at the RSA Conference, we see tons of new product vendors in the Innovation Sandbox. Black Hat does something similar and attracts other vendors too.

These vendors are new to the space and hungry for customer success stories.

In many cases, you can replace an existing vendor with one of these hungry startups for a tiny fraction of the cost of an established player.

For the right customers with the right logo, I've even seen the low cost of free.

Interns: Assemble!

If you don't have FTE budget, consider interns.

Pay them (obviously).

Be realistic about whether or not you can eventually hire them.

This is mutually beneficial - they clear "grunt work" while getting experience that differentiates them and gives them a leg up in hiring.

Image credit: Disney, fair use

Automations: Focus on Easy

Automations require process and some time investment, but are a ***great*** way to do more with less.

- "But Jake, I'm drowning. I can't take the time to build an automation."

Focus on **small**, **easy to develop** automations that offer **incremental** time savings on **frequently** executed tasks.

Fail Fast: estimate the time to build the automation. If the time consumed exceeds double your estimate, bail.

Pro Tip: Block a few hours on the calendar periodically with the intent to focus on automation. Defend that time. It's an investment in "future you."

Automations: "Perfect" vs "Better"

When building automations, don't strive for full automation.

Focus on semi-automation by tackling small components of the overall task.

Key Insight: EVERY automation I've designed has followed the 80/20 rule (or worse)

Build "Phone a Friend" Relationships

A quick "sanity check" with a trusted partner can be priceless.

In the days of budget excess, the org can pay for consultants.

You can get quick "phone a friend" help by building a network of trusted advisors you can get quick feedback from.

- "Are you impacted by the OCI incident? What are you looking for in the logs?"
- "We're seeing a ton of latency after the last $app update."

Pro Tip: Remember these are informal relationships: you can't expect immediate responses. Be ready to reciprocate.

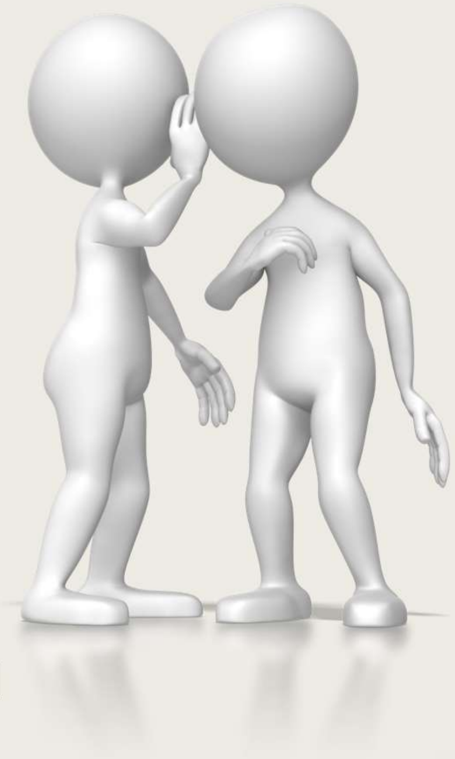
Informal CTI Sharing Groups

We're seeing cuts in quantity and quality to CTI from the federal government.

Many programs are cutting funding for their commercial CTI feeds.

It costs zero dollars to set up a Discord Server with a small group of trusted friends that you put indicators from your phishing incidents into for everyone to benefit.

Same for sharing malware samples.



Pro Tip: Don't unilaterally decide to do this unless you're in security leadership at your org. "Informal CTI sharing" rhymes with "Unauthorized sensitive data disclosure."

Wrapping Up

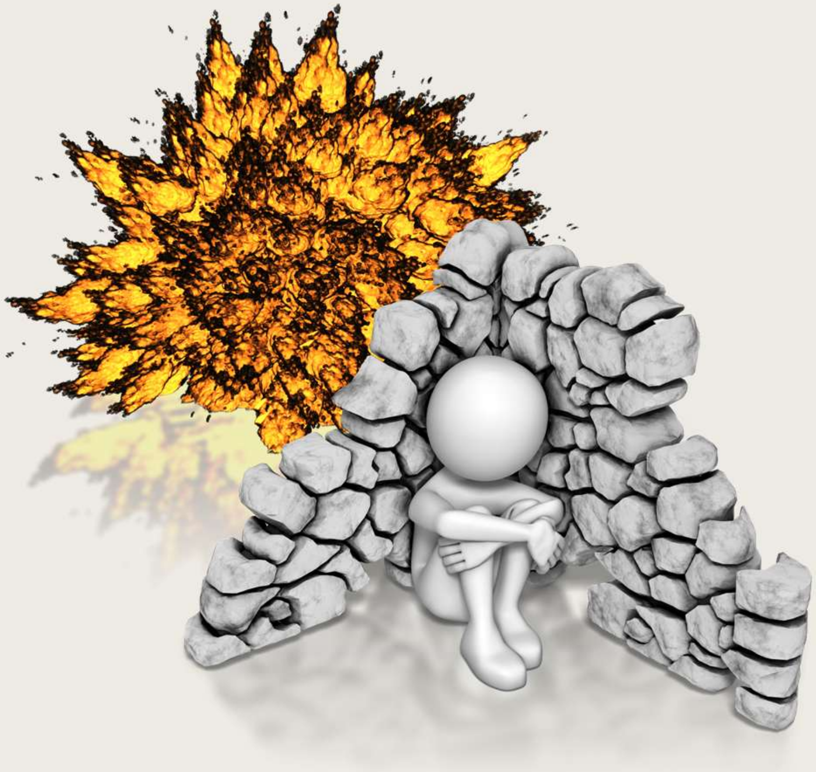
<hunter_strategy>

Many of the Best Came Through Lean Times

Budgets are cyclical and move with the economy.

Some of the best people you know in industry came through really lean times.

You can curl up in a ball and hide or you can rise to the challenge.



Don't Burn Out

If you're Blue Team, your job is critically important.

YOU are more important.

YOUR health (and **mental health**) is more important.

Building a support network is important.

Advocate for yourself and don't be afraid to say NO.

Any organization that expects you to work ludicrous hours to compensate for their lack of resourcing **is abusing you.**

Image: Mental Health Hackers

Conclusions - Wrapping Up

- Automate smartly - perfect is the enemy of ***better***.
- You probably don't need an agent...
- When budget items didn't make the cut, the services they supported usually can't either.
- Be realistic about what you can **and can't** do with the new state of play.

Jake Williams

@MalwareJake

Jake.Williams@hunterstrategy.net

You've Got This

We've had industry downturns before.

We made it through to the other side.

Take a deep breath - **you've got this.**