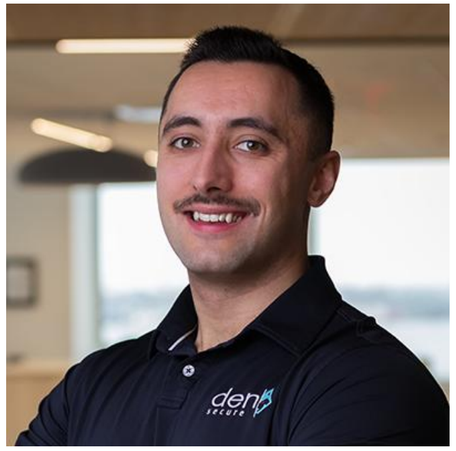
CYBER RISK EXPOSED: THE POWER OF THREAT EMULATION

CCBN Directors Roundtable • Alex Martirosyan, Lead Penetration Tester

WHOAMI

- 8+ years in offensive security
- IT Audit > Penetration Testing
- Interested in intersection of mathematics and security



Alex Martirosyan, OSEP,CRTO,OSCP

Lead Penetration Tester, DenSecure
AMartirosyan@wolfandco.com
617.261.8138
https://www.linkedin.com/in/alex-martirosyan/
https://twitter.com/almartiros
https://www.wolfandco.com/services/densecure/

Marking Hype and Reality

Anthropic's **Claude Mythos** found unknown flaws across applications, software, and operating systems. The LLM identified the vulnerability and generated the code to exploit them.

Compliance is not security

Frameworks and audits is how most of us understand cybersecurity.

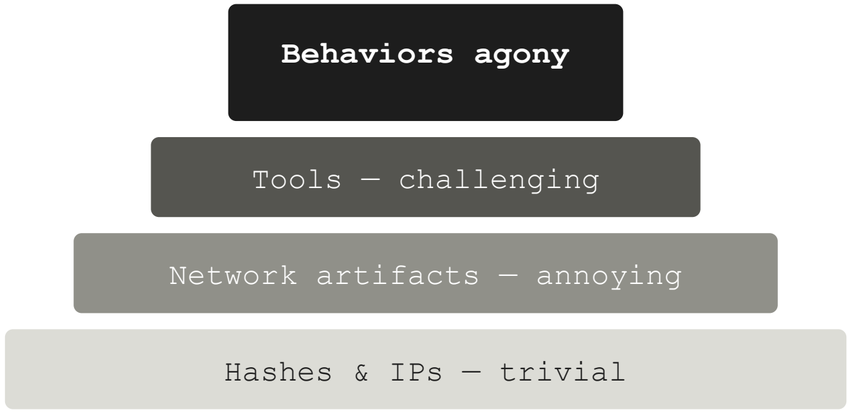
NIST CSF
NIST 800-53
CIS Top 18
PCI DSS
HIPAA
GLBA
SOC 2
SOX

Passing the audit proves you **documented** a control. It does not prove the control **works** when someone attacks it. Attackers don’t care about checklists.

Creating annoying obstacles

The goal is to make breaking in cost **more time, money, and skill** following "Pyramid of Pain."

Force attackers toward the top, and the cost lands on **them.**



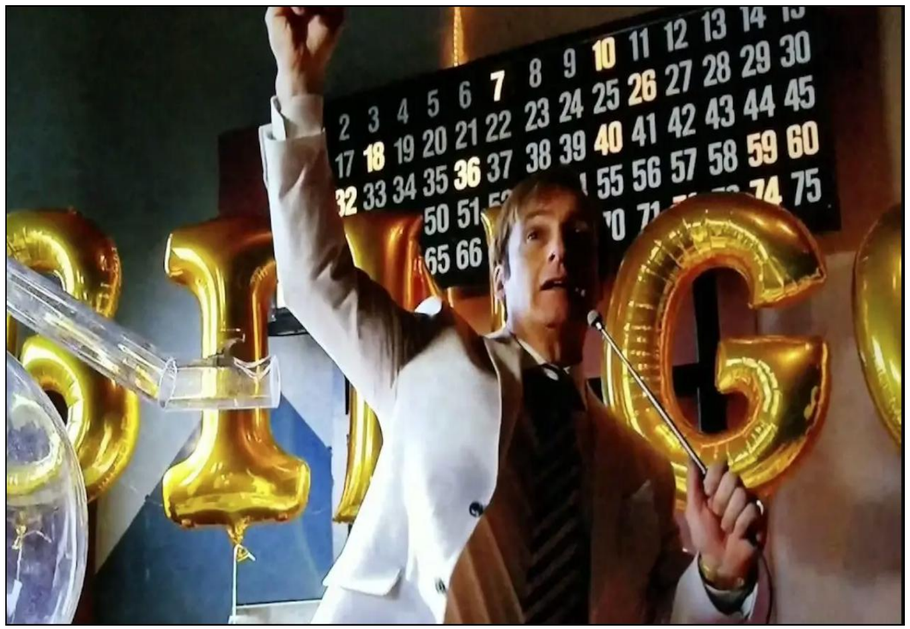
The "Pyramid of Pain" — cost to the attacker, bottom → top

Case Study: Bank Ransomware Emulation

Observability
- Did we capture a log?
- Add logging source
- Refine audit policies

Detection
- Did we generate an alert?
- Create new alert
- Refine alert thresholds

Mitigation
- Did we prevent or stop the action?
- Can we prevent within acceptable F/P rates



Atomic Testing	**Micro Emulation**	Full Emulation
Emulate single technique	**Emulate compound behaviors across 2–3 techniques**	**Emulate adversary operation**
Executable in **seconds**	Executable in **seconds**	Executable in **hours**
E.g., Atomic Red test for T1003.001 - LSASS Memory	*E.g., Fork & Run Process Injection*	*E.g., FIN6 adversary emulation plan*
Easy to automate	Easy to automate	Easy to automate
Validate atomic analytics	Validate atomic analytics	Validate atomic analytics
Validate chain analytics	Validate chain analytics	Validate chain analytics
Evaluate SOC against a specific set of TTPs	Evaluate SOC against a specific set of TTPs	Evaluate SOC against a specific set of TTPs
Evaluate SOC holistically against specific groups	Evaluate SOC holistically against specific groups	Evaluate SOC holistically against specific groups

Threat emulation

WHAT MOST DO

Buy smoke detectors

Install the tools. Confirm the lights are green. Assume that if a fire starts, they'll go off. **You've never actually lit one and rare to test.**

HOW EMULATION WORKS

Run the fire drill

Deliberately recreate a real attacker's moves, safely, and watch what your people, process and tools **actually do.** Then fix what didn't work.

Same principle as a fire drill or a stress test in banking: you don't wait for the real emergency to find out the exits are locked.

Continuous Loop

STEP 01

Model the threat

Pick the attackers who'd actually come for us, and map how they operate.

STEP 02

Test the controls

Safely run those moves against our own environment to see what triggers and what doesn't.

STEP 03

Confirm what works

Document what we caught, what we missed, and how fast we noticed.

STEP 04

Fix & track gaps

Remediate, update the controls, and report the gaps to the board. Then repeat.

The threat keeps changing so the test has to keep running. Each loop **"we checked, and here's the evidence."**

Five questions to ask your security leader

1 When did we last test our defenses against a **real attacker's playbook** — not a checklist?

2 Which attacks did we **catch**, and which walked right through?

3 How **fast** did we notice — minutes, days, or only after the fact?

4 What did we **fix** after the last test, and did we re-test it?

5 If an adversary, ransomware gang, AI-driven attack hit us tonight, where would it **get in**?

THE ONE THING TO REMEMBER

Don't wait to be tested. **Test yourself first.**

You can't buy your way to certainty. Leveraging the same offensive principals yourself before someone with an AI and a grudge does it for you.