REBUILDING SECURITY STRATEGY FROM BREACH LESSONS

A DEFENDERS INITIATIVE PRESENTATION

Attackers are FOCUSED

FOCUS VS DISTRACTION

Defenders are DISTRACTED

- Mythos or NPM Attacks?
- YellowKey or CopyFail?
- Public Wi-Fi or Personal GitHub repos?
- Identity Governance or PQC?
- Sonicwall vulns or Flipper Zero?

WHAT IS THIS?

show n' tell time...

distraction or foreshadowing?

IMAGINATION VS EVIDENCE

Mythos, Quantum, Zero Days

INSIGHTS FROM INSURANCE COMPANIES

Akira & Sonicwall

- 1400+ companies attacked
- $244M taken
- 40% of all At-Bay ransomware claims
- 25% of all Coalition ransomware claims
- 86% of cases involved Sonicwall exploits
- *The most reliable way of getting ransomed in 2025*

Data from At-Bay and Coalition's 2026 claims reports

INSIGHTS FROM INSURANCE COMPANIES

Orgs with more risk

- Manufacturing 2.2x more likely to get ransomed
- VPN and RDP: 87% of all ransomware claims
- Orgs with exposed RDP: breach 3x-8x more likely
- SSH services are attacked more than any other service on the Internet
- Orgs with on-prem OWA (Exchange) are 4x more likely to get breached

Data from At-Bay and Coalition's 2026 claims reports

INSIGHTS FROM INSURANCE COMPANIES

The most common claims

- Financial Fraud. I know, boring.
- For At-Bay, it's largest with 45% of claims
- For Coalition, it is 58% of claims
- Ransomware doesn't even come close
- This category includes BEC (business email compromise)

Data from At-Bay and Coalition's 2026 claims reports

BREACHES YOU'VE PROBABLY HEARD OF

TARGET

BREACHES YOU'VE PROBABLY HEARD OF

TARGET TRIVIA

We actually don't know how the intrusion happened

Fazio didn't have network access

Only access to Ariba for billing

Payment data-stealing malware

how do you deploy malware to every POS at every target store in a few hours?

They detected the attack... THREE TIMES

This was Target's FIFTH data breach

BREACHES YOU'VE PROBABLY HEARD OF

BRITISH LIBRARY

Terminal Services, hastily set up during the pandemic

No MFA

The REAL story is about tech debt, however

BREACHES YOU'VE PROBABLY HEARD OF

EQUIFAX

Why did they get breached?

How do you remember it from the headlines?

BREACHES YOU'VE PROBABLY HEARD OF

Equifax Control Failures

1. No asset inventory
2. No software inventory
3. No file integrity monitoring
4. No network segmentation
5. **Neglected SSL Inspection (SSLV) Appliance**
6. Neglected SSLV failed open
7. SSLV lacked certs for key systems
8. **SAST failed to find Struts due to user error**
9. No anomaly detection on web servers
10. **Custom snort rule didn't work**
11. **Custom snort rule wasn't tested**
12. Vulnerability scanner didn't find Struts
13. Failed to detect webshells
14. Failed to detect interactive activity
15. **Admins stored cleartext creds in open shares**
16. **Least privilege principles not followed for database access**
17. Adhoc database
18. No database ano
19. No field-level enc
20. No data exfiltratio
21. DAST scanning fai
22. Ineffective IR plan
23. **No owners assigne**
24. Comms issues due
25. Lack of accounta
26. **No followup on pa**
27. Old audit findings
28. Insecure NFS conf
29. Logs retained for l
30. Nonexistent or ine

THE DH / SHOSTACK + ASSOCIATES

BREACHES YOU MIGHT NOT HAVE HEARD OF

DRIZLY

Alcohol delivery startup acquired by Uber in 2021

Anyone familiar with this one?

The story is an identity governance thriller

BREACHES YOU MIGHT NOT HAVE HEARD OF

DRIZLY TRIVIA

The FTC singled out the CEO and sanctioned him *personally*

Company was sanctioned for the next 20 years

CEO sanctioned for 10

Uber shut it down in 2024, 3 years after acquiring it for $1.1B

BREACHES YOU MIGHT NOT HAVE HEARD OF

POWERSCHOOL

A contractor with no MFA had credentials stolen

This contractor had access to every customer

Attacker downloaded all teacher & student data

BREACHES YOU MIGHT NOT HAVE HEARD OF

POWERSCHOOL TRIVIA

- One of the worst-handled breaches ever
- No information or support from Powerschool
- Customers created their own support group, around a widely circulated Google Doc
- Powerschool paid a ransom and told customers the attacker deleted data
- The attacker did not, and started ransoming each school district
- Canadian privacy administrators put partial blame on school districts for not doing due diligence before handing over data to a third party

BREACHES YOU MIGHT NOT HAVE HEARD OF

OLDSMAR, FLORIDA

KEY FINDINGS FROM BREACH ANALYSIS

- **Exploitation of Security Tools**
  Attackers frequently leverage IT and security tools against organizations.
- **Ignored Known Risks**
  Documented risks from reviews and tests are often overlooked.
- **Human Alert Fatigue**
  Alerts are frequently missed or disregarded by personnel due to high volume.
- **Product Misuse/Misconfiguration**
  Purchased security products are not utilized effectively or are improperly set up.
- **Insufficient Monitoring**
  A lack of adequate monitoring impedes understanding of breach root causes.
- **Inconsistent MFA Implementation**
  Multi-Factor Authentication is not uniformly applied across all resources and accounts.
- **Misaligned Detection Strategies**
  Security detection mechanisms do not accurately reflect actual attacker behaviors.
- **Lack of Segmentation**
  Absence of network segmentation concentrates risk.
- **Widespread Clear Text Credentials**
  Sensitive credentials are often stored or transmitted in plain text.
- **Governance Failures**
  Deficiencies in governance regarding the lifecycle management of accounts, data, and systems.
- **Insecure Development Environments**
  Development environments are inadequately protected, often serving as an entry point.

RECOMMENDATIONS

What to do next

1 **Improve identity governance**

Stale accounts, stolen passwords

2 **Implement FIDO2, Passkeys**

All day. MFA shows up more than anything else.

3 **Remove legacy services and protocols**

The asbestos of the Internet - get rid of VPNs, FTP, self-hosted Exchange, and never expose administrative consoles/interfaces to the Internet

4 **Train your SOC**

Would they know a real attack if they saw one? How can you be absolutely sure?

5 **The basics go a long way**

- Reduce attack surface
- segmentation and isolation
- removing plaintext credentials
- understanding dataflows,
- hardening systems
- active and passive mitigations

The old plan is the new plan: harden systems, get rid of tech debt, governance. Good luck, it's not easy!

ADRIAN, YOUR RECOMMENDATIONS SUCK

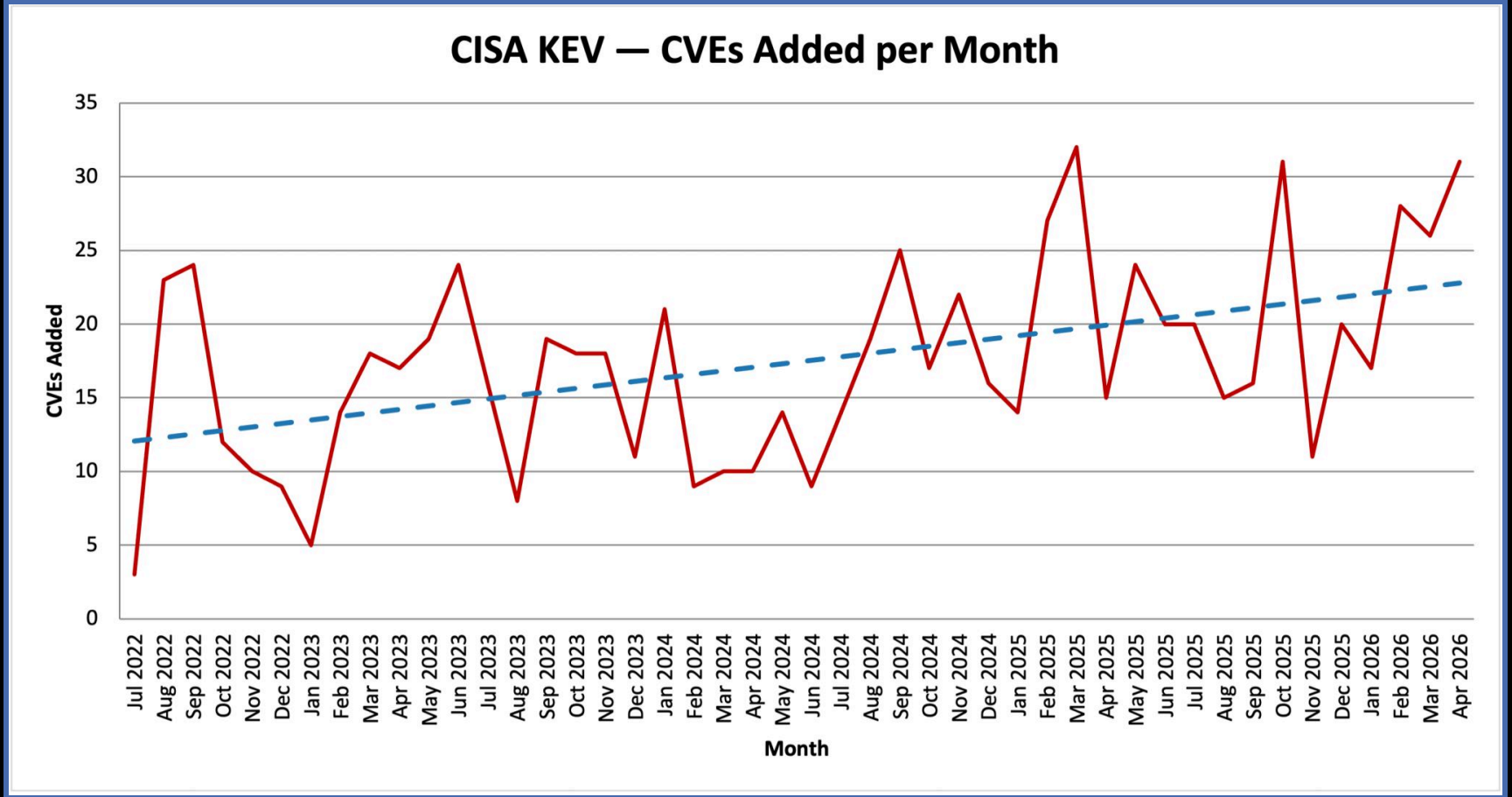
"the basics" are impossible

IT won't get rid of tech debt

IT doesn't really listen to us in general

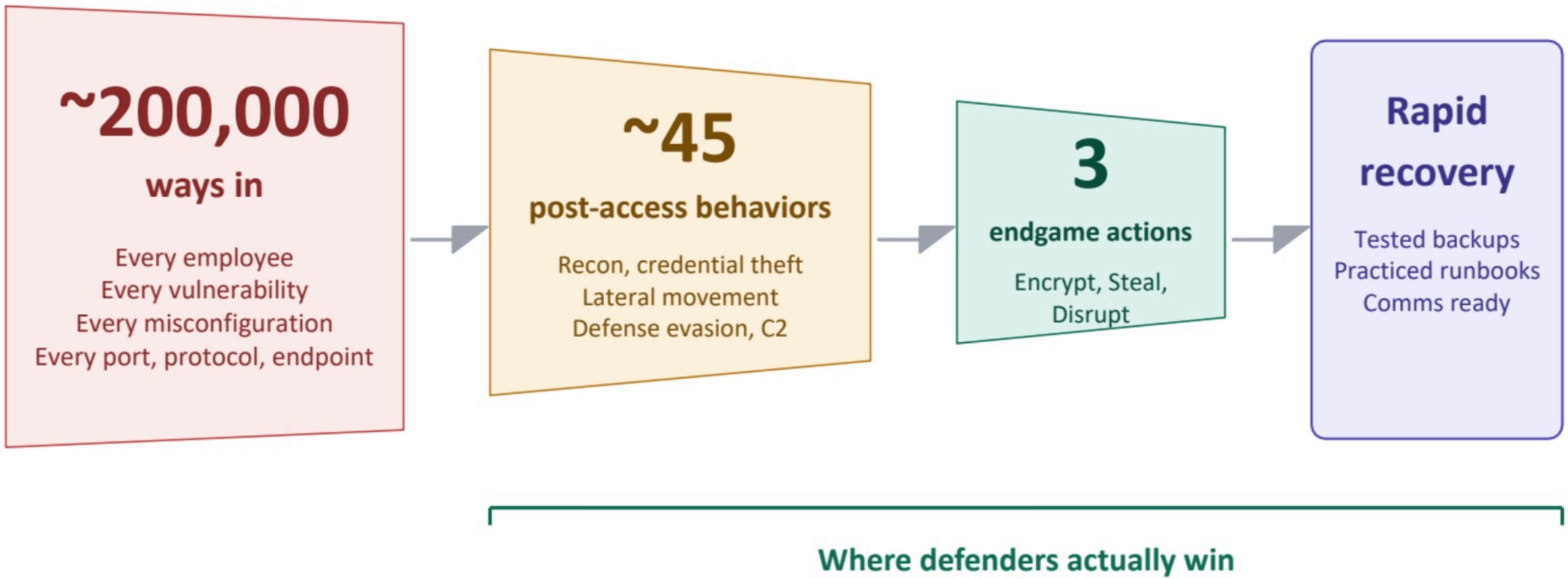
THIS ISN'T SUSTAINABLE

"Only 26% of critical vulnerabilities—defined as being in the Cybersecurity Infrastructure and Security Agency Known Exploited Vulnerabilities (CISA KEV) catalog—were fully remediated by organizations in 2025, a drop from the previous year's 38%."



The defender's funnel

Attacker actions narrow sharply once they're inside — recovery decides the outcome



Pre-compromise: impossible to fully secure

Post-compromise: tractable, finite, decisive

“GET BETTER AT GETTING BREACHED. YOU’RE NOT JUDGED FOR HAVING ONE, YOU’RE JUDGED ON HOW YOU HANDLE IT.”

-- Adrian, exhausted and out of ideas

WHERE CAN WE FIND EVIDENCE?

Threat Actor & DFIR Reports

Solid reports on attacker behavior drop monthly.

Verizon DBIR

M-Trends

TheDFIRReport.com

Federal Investigations

Federal government ordered

FTC Complaints

Canadian Privacy Commissioners

Eurepoc.eu

Insurance Companies

Reports on the *failures that led to claims*

At-Bay

Coalition

Cowbell Cyber

Transparent Companies

Sometimes companies share the breach details of their own volition!

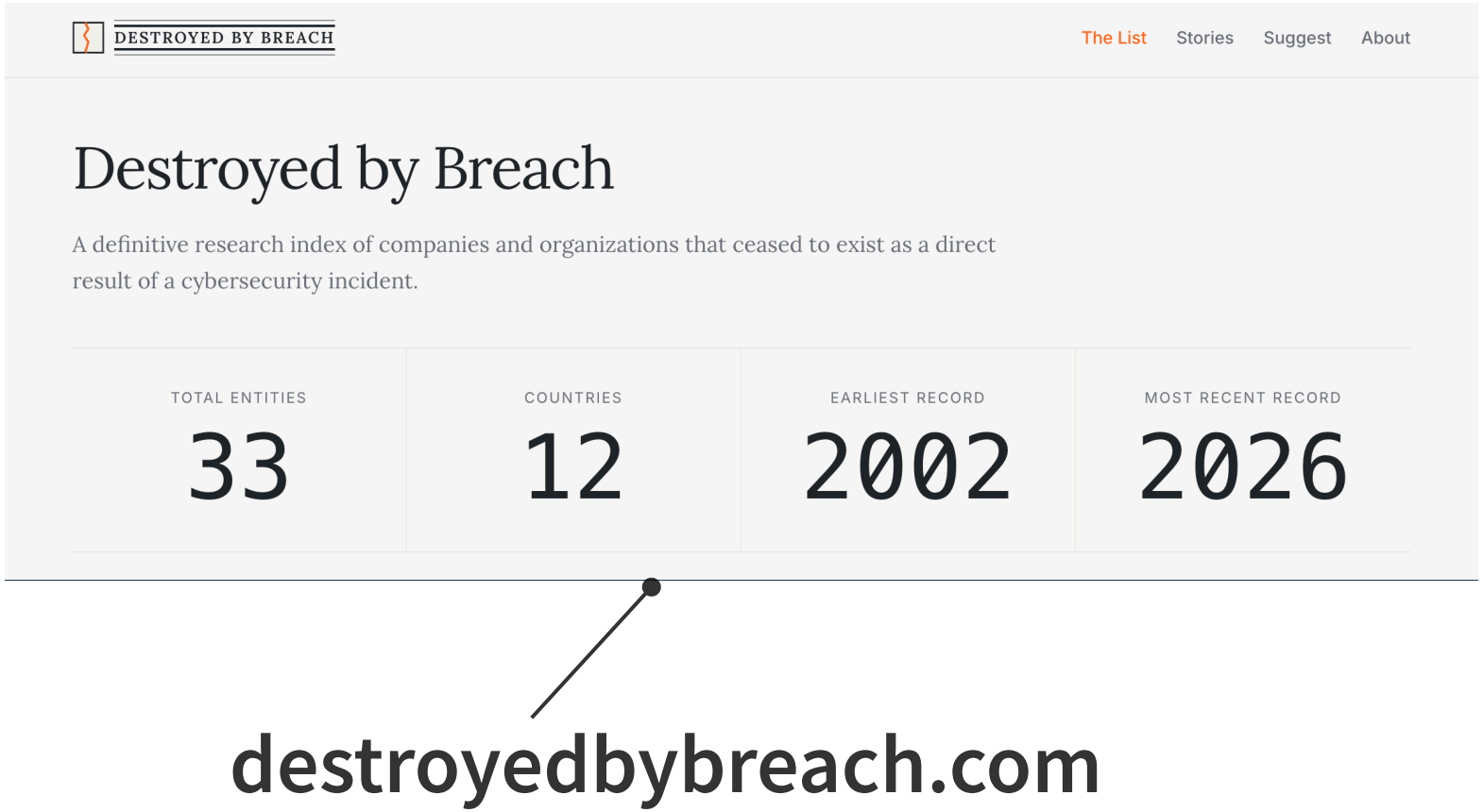
Code Spaces

The British Library

Most breached security vendors

LEARN MORE

Ever wondered how many companies have gone out of business due to a breach?

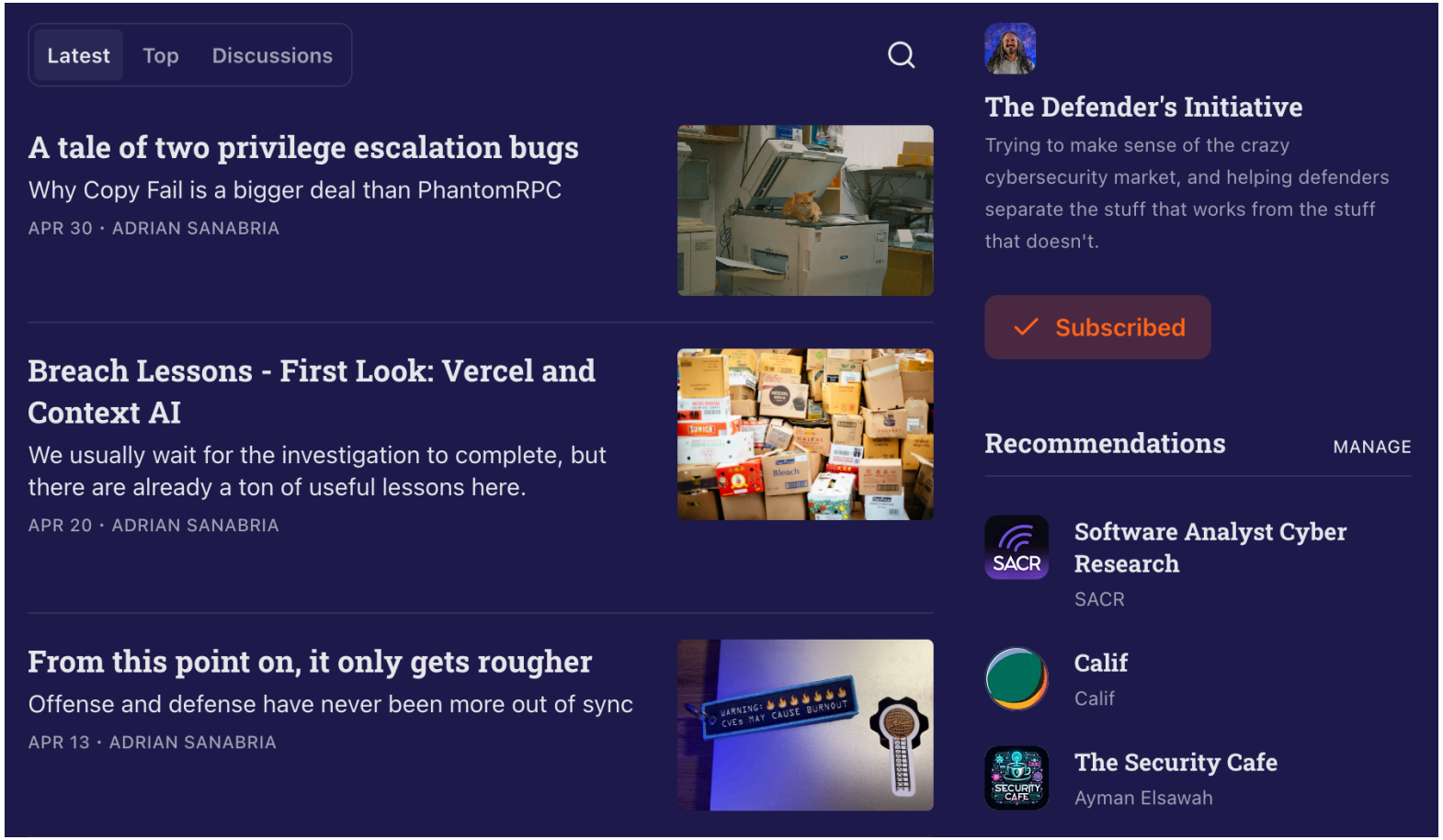


destroyedbybreach.com

LEARN MORE

Want to learn more about breaches and vulnerability management?

Want to help fund breach research?



defendersinitiative.com

GIVE ME A SHOUT.

@ adrian@defendersinitiative.com