IS YOUR PHONE SPYING ON YOU?
AN IN-DEPTH ANALYSIS OF VULNERABILITIES IN CISCO VOIP PHONES

MANTRA
INFORMATION SECURITY

Balázs Bucsay

Founder & CEO of
Mantra Information Security

https://mantrainfosec.com

BIO / BALÁZS BUCSAY

- Over two decades of offensive security experience
- 15+ years of research and consultancy
- Software Reverse Engineer
- Started learning assembly at the age of 13
- Previously worked at NCC Group and Vodafone

- Twitter: @xoreipeip
- Linkedin: https://www.linkedin.com/in/bucsayb/
- Mantra on Twitter: @mantrainfosec
- Mantra: https://mantrainfosec.com

MANTRA
INFORMATION SECURITY

BIO / BALÁZS BUCSAY

MANTRA
INFORMATION SECURITY

MANTRA INFORMATION SECURITY

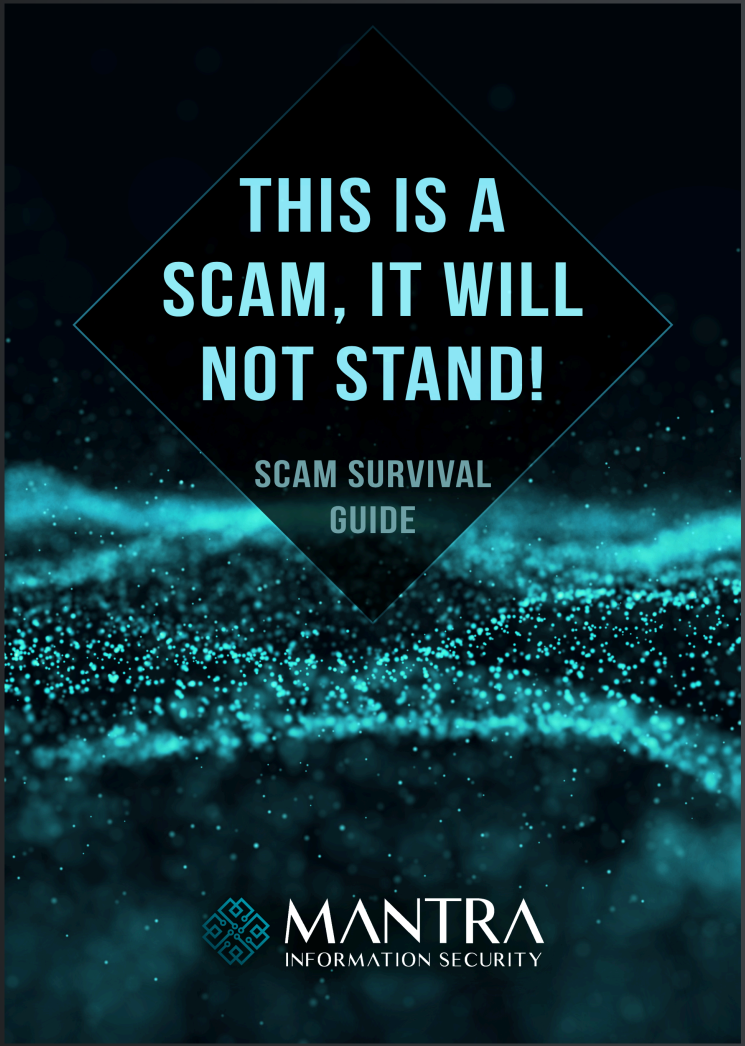
MANTRA
INFORMATION SECURITY

- Boutique consultancy
- Decades of experience and excellence
  - Specialised training delivery (Software Reverse Engineering, Ransomware Detection, ...)
  - Cloud, CI/CD, Kubernetes reviews
  - Red Teaming, EASM, Infrastructure testing
  - Web application and API assessments
  - Reverse-engineering, embedded devices and exploit development
  - ...
- Full stack consultancy: from identifying vulnerabilities to implementing fixes

https://mantrainfosec.com

BOOK: THIS IS A SCAM! IT WILL NOT STAND!

MANTRA
INFORMATION SECURITY



THIS IS A SCAM, IT WILL NOT STAND!

SCAM SURVIVAL GUIDE

MANTRA
INFORMATION SECURITY

- Empower others to protect themselves
- 11 gripping and educational real-world stories
- Download and share it freely
- Absolutely free of charge
- Perfect for a non-technical audience

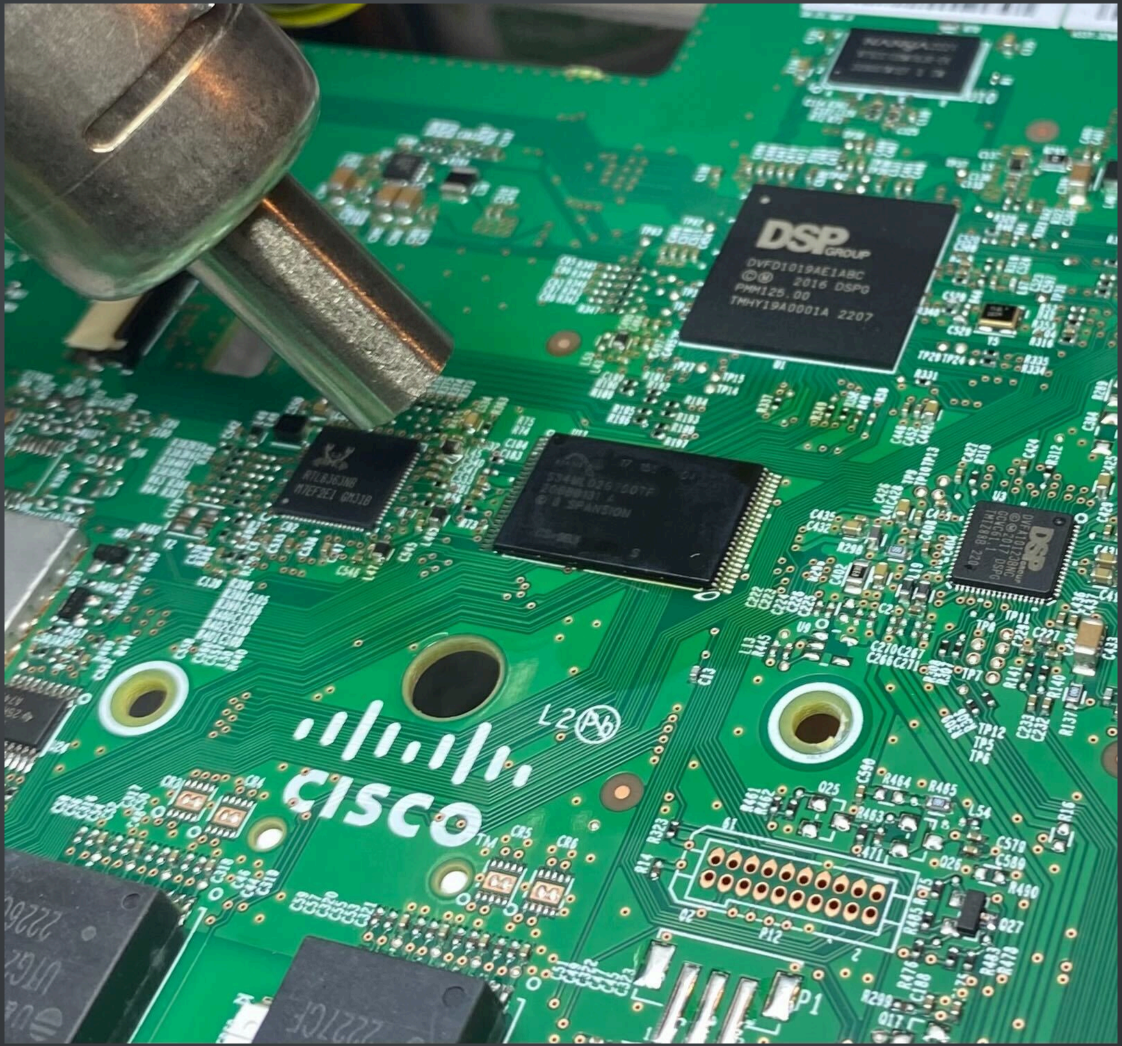
https://mantrainfosec.com/scambook

JOINT EFFORT

- Balazs Bucsay - Mantra Information Security - SRE skills
- Liviu Rombaut & Peter Lemmens - Davinsi Labs - HW skills

CHIP-OFF MASTER: LIVIU ROMBAUT

MANTRA
INFORMATION SECURITY



MANTRA
INFORMATION SECURITY

THE STARTING POINT

- **Scope:** Cisco IP Phone 6851, 7841, 8861
- Dumped the running firmware
    - Stock firmware available from Cisco's official website
- Identified that all three models use the same firmware version
- These are very well-known devices.
    - Could be found in nearly every office in the city

MANTRA
INFORMATION SECURITY

THE MINDSET

- Initial Assumptions:
  - **Cisco product:** MUST to be secure by default
  - **Widespread deployment:** MUST have undergone extensive testing
- Baseline: Won't be able to find anything

CISCO IP PHONE 8861

MANTRA
INFORMATION SECURITY

cisco
515 333 0000
Jim Nadal
Martin Bell
Jan 27 09:30 AM
Edward Molina 408 555 1234 42:03
Stacy Mathews 415 888 2345 0:45
Tom Woodrow 972 659 2004 10:28
David Shu 214 787 3435 2:07
End call
Do not disturb
Show detail

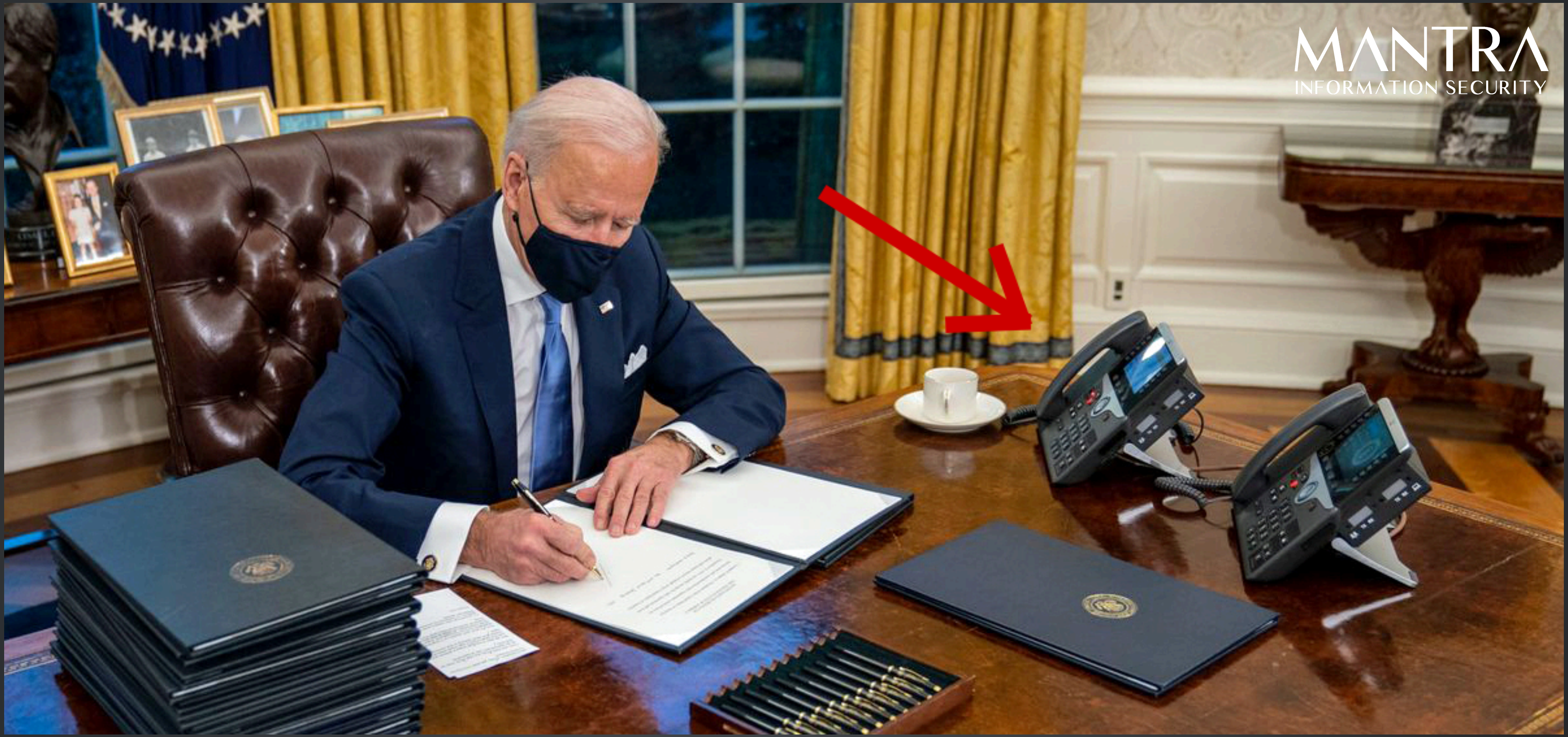
CISCO IP PHONE 7841

MANTRA
INFORMATION SECURITY

CISCO IP PHONE 6851

MANTRA
INFORMATION SECURITY

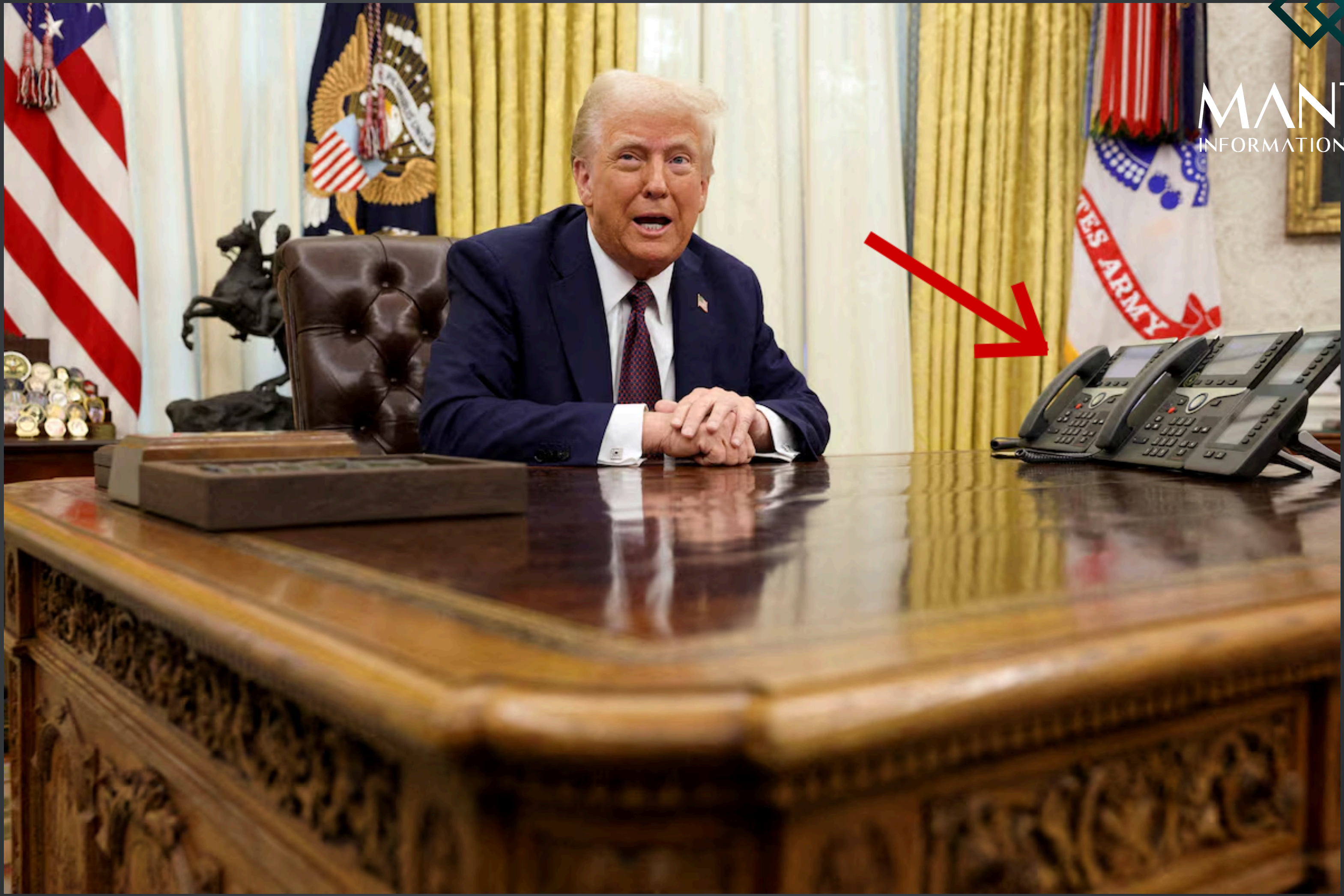
DO YOU RECOGNISE HIM? - 8851



Source: https://x.com/tnewtondunn/status/1352284365854806017
Source: https://whcacannonball.blogspot.com/2021/05/the-phones-in-president-bidens-oval.html

HOW ABOUT HIM? - 8851

MANTRA
INFORMATION SECURITY



Source: https://www.reuters.com/world/us/trump-restricts-ap-access-over-gulf-mexico-issue-2025-02-19/

MANTRA
INFORMATION SECURITY

REALITY

- I couldn't have been more wrong.
- Several CVEs were identified within just 10 days:
  - CVE-2024-20357: Cisco IP Phone Unauthorized Access Vulnerability
  - CVE-2024-20376: Cisco IP Phone DoS Vulnerability
  - CVE-2024-20378: Cisco IP Phone Information Disclosure Vulnerability

MANTRA
INFORMATION SECURITY

BUGS: INFORMATION LEAK

- **Access:** Unauthenticated
- **Type:** Exposed Logs
- **Description:**
  - /var/log/messages accessible over http://[IP]/log/messages
  - Information goldmine (crashes with verbose output)

BUGS: DENIAL OF SERVICE (CVE-2024-20357)

- **Access:** Unauthenticated
- **Type:** Buffer overflow
- **Description:**
  - The proof-of-concept successfully crashed one of the main processes
  - Repeated crashes triggered a device reboot

BUGS: .BSS BUFFER OVERFLOW (CVE-2024-20376)

- **Access:** Unauthenticated
- **Type:** Buffer overflow
- **Description:**
  - Overwrites initialized data in the .BSS section
  - Not a stack overflow, but the .BSS contains sensitive data.
  - Repeated exploitation leads to device reboots
  - Note: the XML service must be enabled for this issue to be exploitable

BUGS: INFORMATION LEAK? (CVE-2024-20378)

- **Access:** Unauthenticated - what else?
- **Type:** Packet capture
- **Description:**
    - Three endpoints that can be called:
        - Start tcpdump on all interfaces
        - Stop tcpdump
        - Download the resulting .pcap file

- Do not forget, we are talking about VoIP Phones

SNIFFING DEMO

MANTRA
INFORMATION SECURITY

THE IMPACT

- Millions of devices were — and likely still are — vulnerable worldwide
- No OTA or automatic firmware upgrade mechanism
- Patched firmware was released on May 1, 2024

- These vulnerabilities are likely just the tip of the iceberg

A FEW QUESTIONS REMAIN

- Do we really believe these vulnerabilities hadn't been discovered before?
- Would the NSA truly allow the POTUS to use this firmware if they weren't aware of its risks?
    - Ignorance? Incompetence? Something else?
- What does this say about the current state of embedded device security?

MANTRA
INFORMATION SECURITY

THE RESEARCHER MINDSET

"If you're not uncomfortable, you're not learning."

- Let’s talk a bit about the researcher mindset!
- It starts with curiosity, a drive to understand how things work
- It is **more about mentality** than knowledge
- That means you don’t need to "know everything" to begin
- **Most importantly:** Research doesn’t have to be groundbreaking to be valuable

THE BOTTLENECKS

"Research begins where curiosity outweighs fear."

- Success rate is low: think 95% failure, 5% success (ballparked)
- There are no guaranteed results — price of the emotional highs
  - Tried bug bounty? You’ve probably felt the grind
- Impostor syndrome? You're not the only one. Don’t assume others don’t feel it too
- Burnout is real — a bad streak can make you want to quit

THE EMOTIONAL ROLLERCOASTER

MANTRA
INFORMATION SECURITY

- Continuous failures can lead to constant lows, which may contribute to burnout
- On the flip side, occasional successes offer a drive and create significant emotional highs
- A few examples:
  - Application crash found — Exciting!
    But wait... not exploitable? A letdown.
  - Critical risk identified — Great!
    But wait... already published as a duplicate? Disheartening.

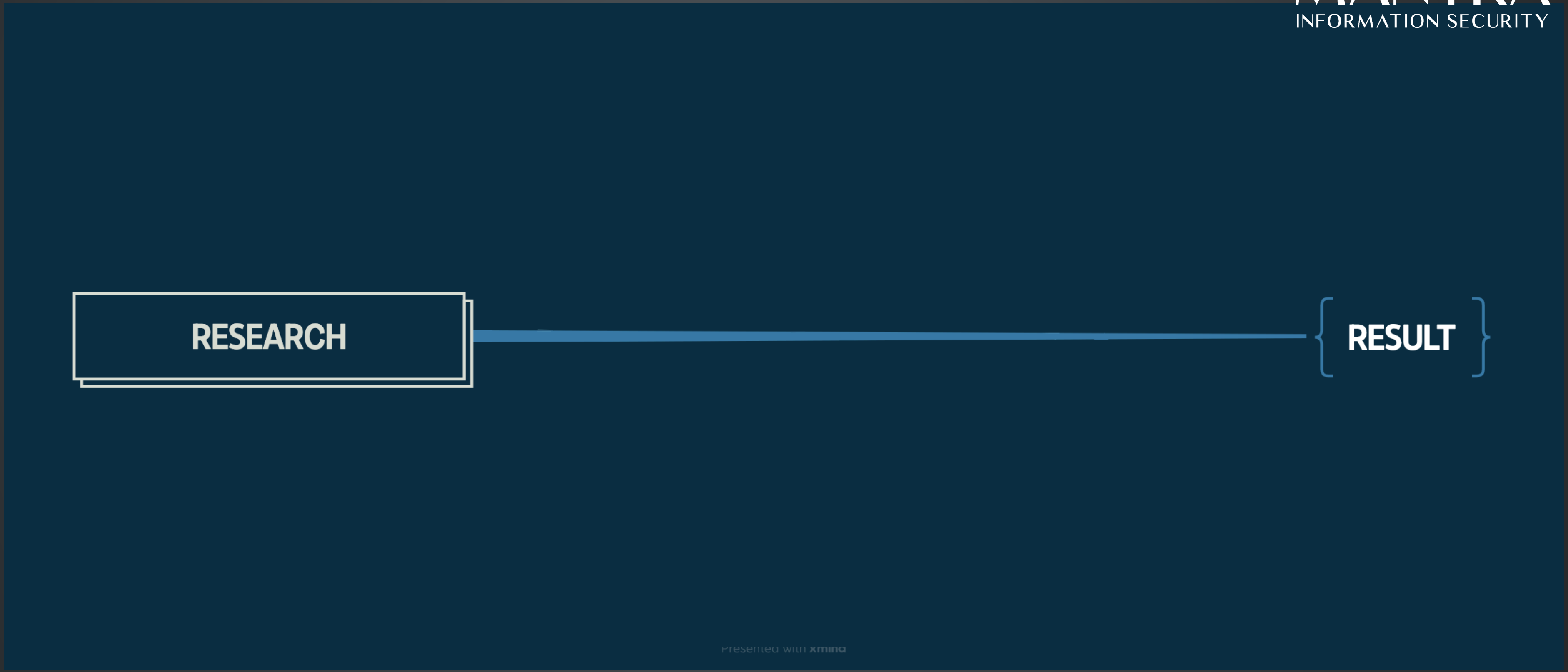
THE ASSUMPTIONS

"Never mistake reputation for security."

- "It’s been tested a thousand times" - do I need to give you an example?
- "They must have tested this" - Ignore this thought, get used to failure
- "Trusted product/service" — by whom, and why?
- Big brand ≠ secure. Popular doesn't mean bulletproof

LINEAR MINDSET

MANTRA
INFORMATION SECURITY



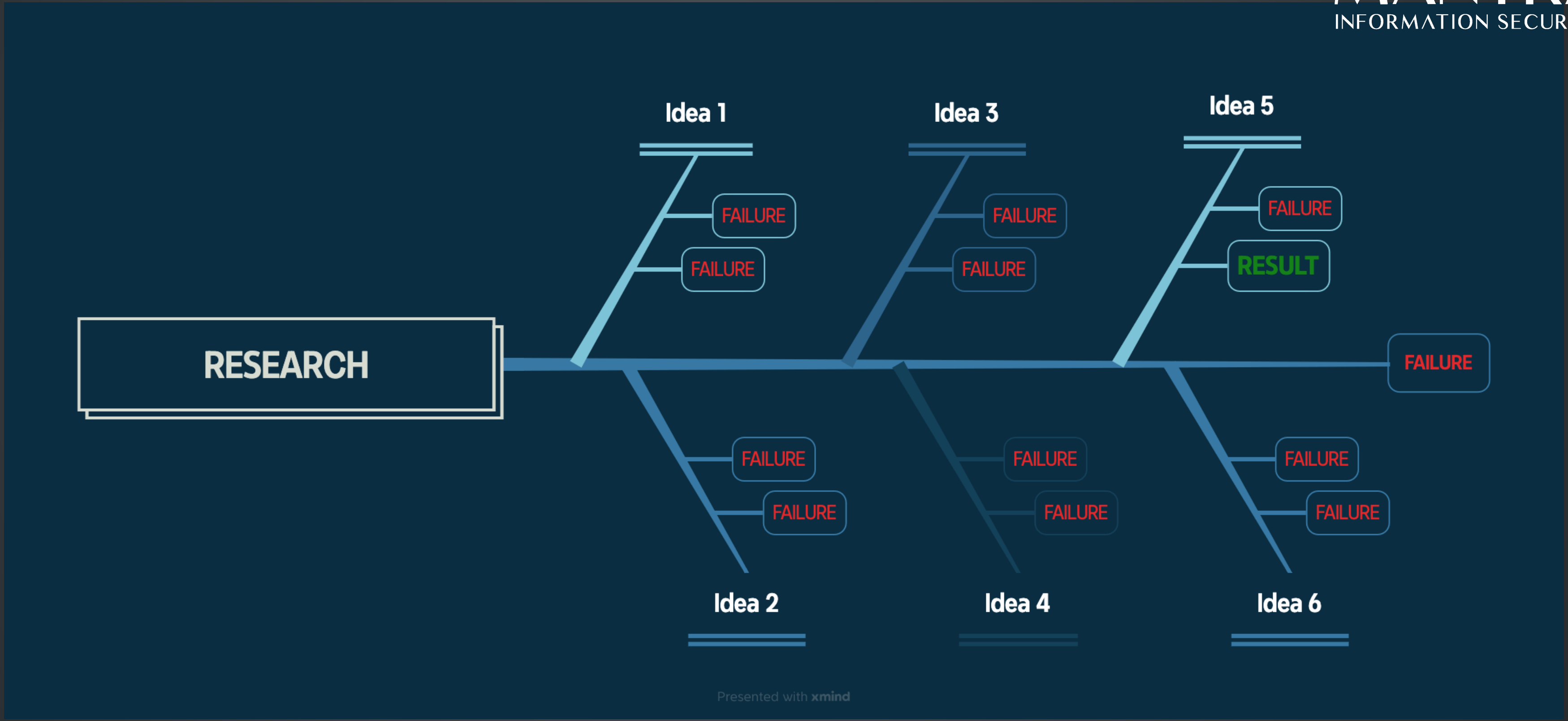
RESEARCH

RESULT

Presented with xmind

RESEARCH MINDSET

MANTRA
INFORMATION SECURITY



THE SUPPORT

"Trivial doesn't mean easy."

- Just because something looks simple doesn't mean the research was
- Being jealous won't move you forward - learning will
- If you appreciate someone’s research, say something!
  - Positive or constructive feedback helps more than silence

MANTRA
INFORMATION SECURITY

THE RESPONSIBILITY

"Discovery is knowledge; resolution is value."

- Ethics in research is vital — but who are we ultimately responsible to?
  - Vendors (often large corporations)? Are we demanding responsibility — or just making sure no one loses money?
  - Clients (to the vendors)?
  - End-users (everyday people who bear the risk)?

THE RESPONSIBILITY

- Types of Disclosure:
  - Responsible Disclosure: Most effective when the vendor is cooperative and acts in good faith
  - Full Disclosure: Seen by some as irresponsible — work well for negligent or unresponsive vendors
  - Non-Disclosure: Choosing silence. May happen when you're disillusioned or burned out
  - Commercial Disclosure: Selling to bug bounty platforms or third parties (e.g., 0day brokers)

MANTRA
INFORMATION SECURITY

CLOSING NOTES

"Comparison is the thief of joy."

- Never doubt yourself — there's no value in that
- Don't build imaginary boundaries — they'll only stop you from trying
- Stop reaching up to others — comparison is a game you can't win
- Make time. "Waste" it on research and learning. That's how growth happens

MANTRA

INFORMATION SECURITY

Q&A

https://mantrainfosec.com