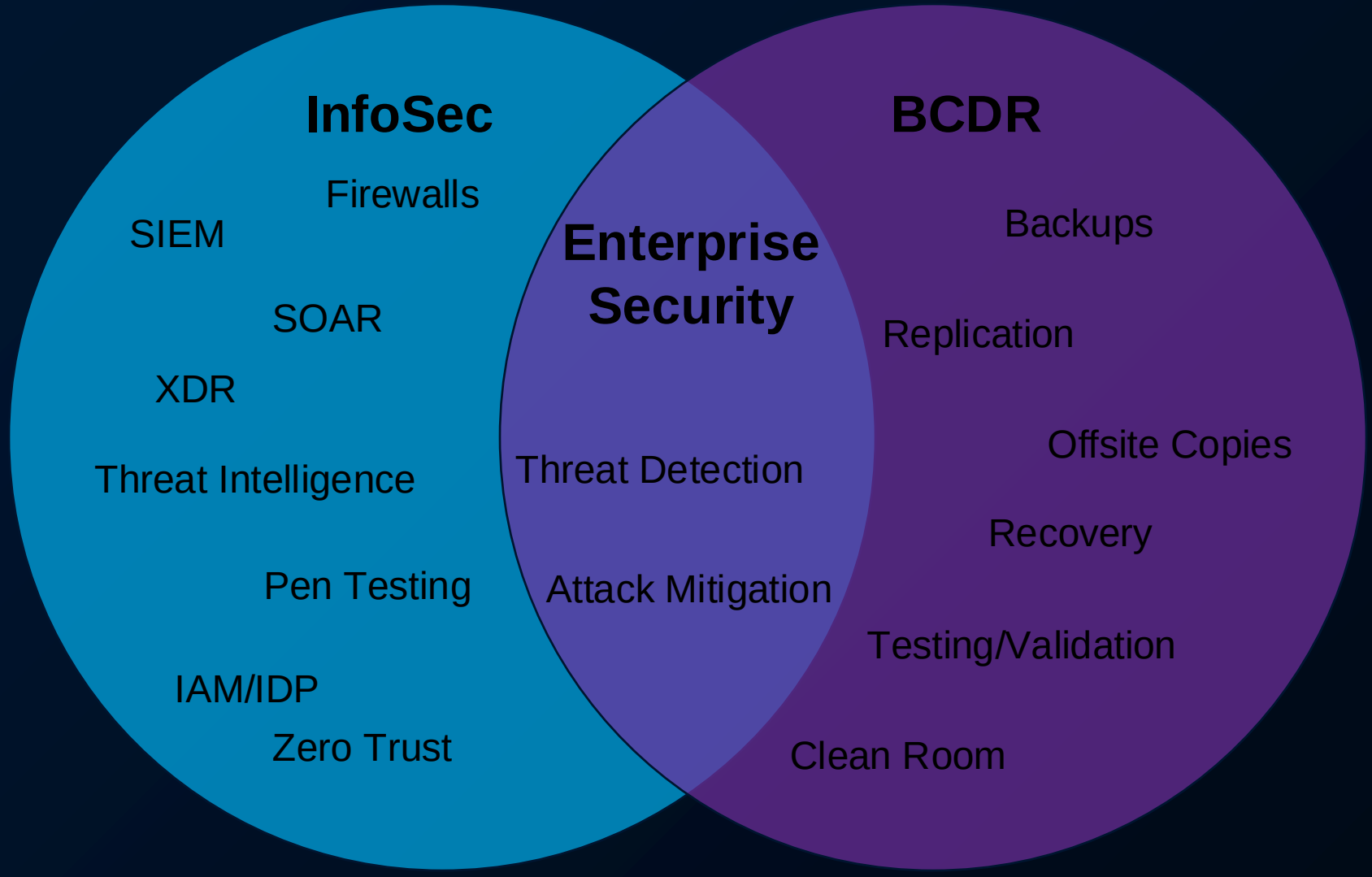
BACKUP IS SECURITY:

Designing Disaster Recovery For The Modern Era

Jim Jones
Sr. Product Infrastructure Architect
@11:11 Systems

Holistic Data Protection



VMware Hypervisor Recovery

No hypervisor found.

No hypervisor found.

RANSOMWARE SUCKS

```
    [snip]
DO NOT ATTEMPT TO RESTORE OR MOVE THE FILES YOURSELF. THIS MAY DESTROY THEM
***Also a lot of sensitive data has been downloaded from your network***
For example:
_____________________________
\\10.30.12.98\D$\[snip]
\\10.30.13.2\Y$\SQLbackup
\\10.40.10.162\D$
THIS IS A SMALL PART. WE DOWNLOADED ALL CLIENT'S SQL DATABASES
If you refuse to cooperate, all data will be published
for free download on our portal:
http://santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zig
CONTACT US BY EMAIL:
unlock@support-box.com
unlock@rsv-box.com
OR WRITE TO THE CHAT AT :->:
http://npkoxkuygikbkpuf5yxte66um727wmdo2jtpg2djhb2e224i4r25
secret=[snip]
(use TOR browser)
```

r/Veeam
u/elitegamerbros • 2d

Akira Ransomware Nuked Our Veeam Backup

Hi all, any help would be appreciated. We have Synology Nas with all our backups that was completely wiped somehow, even the Synology OS drive, after Akira Ransomware attack. Long story short, we were able to install new OS on a blank drive and plug the wiped data drives back in and recover veeam backup data using EaseUs. But when I try to extract VM from backups using veeam extractor utility, nothing is showing. Looks like some incremental backups and vbm below certain file sizes were nul'd but vbk files seem intact with data. Is there any tools we can use to restore VM from this back up files ? Or check for corruption.

8 | 19

Cyberattack Shuts Down Clinic, 21K Patients Exposed

Anosha Shariq Writer

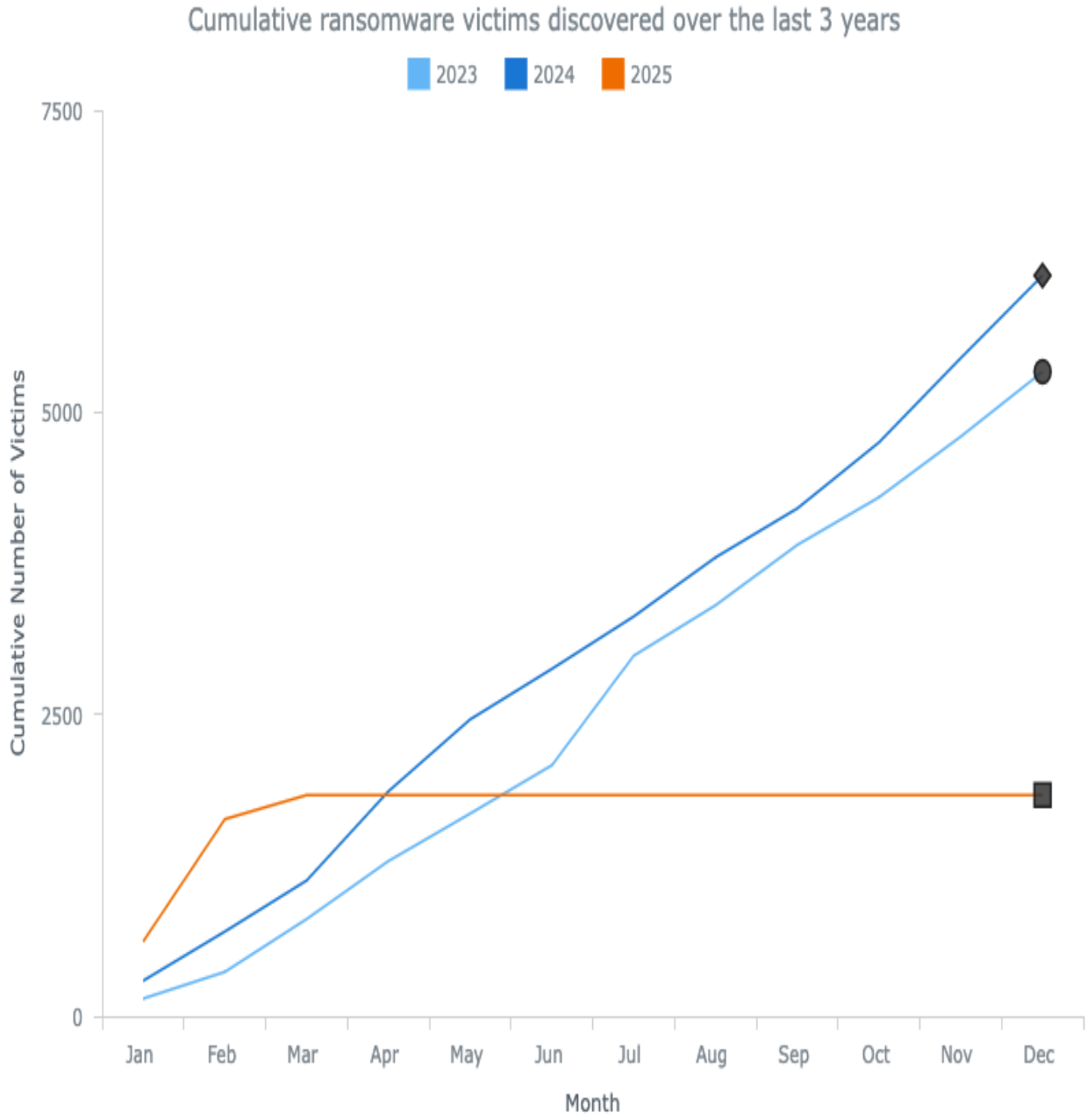
2–3 minutes

Kirkland, WA – March 20, 2025 –A ruthless cyberattack on Lake Washington Vascular has exposed 21,000 patients' medical data, shutting down operations. Victims face identity theft risks.

A devastating cyberattack has rattled Lake Washington Vascular, a leading vascular care provider, compromising the sensitive medical records of over 21,000 patients. The clinic was forced to halt operations after hackers infiltrated its network, deploying malware that encrypted its systems.

Ransomware is Pervasive

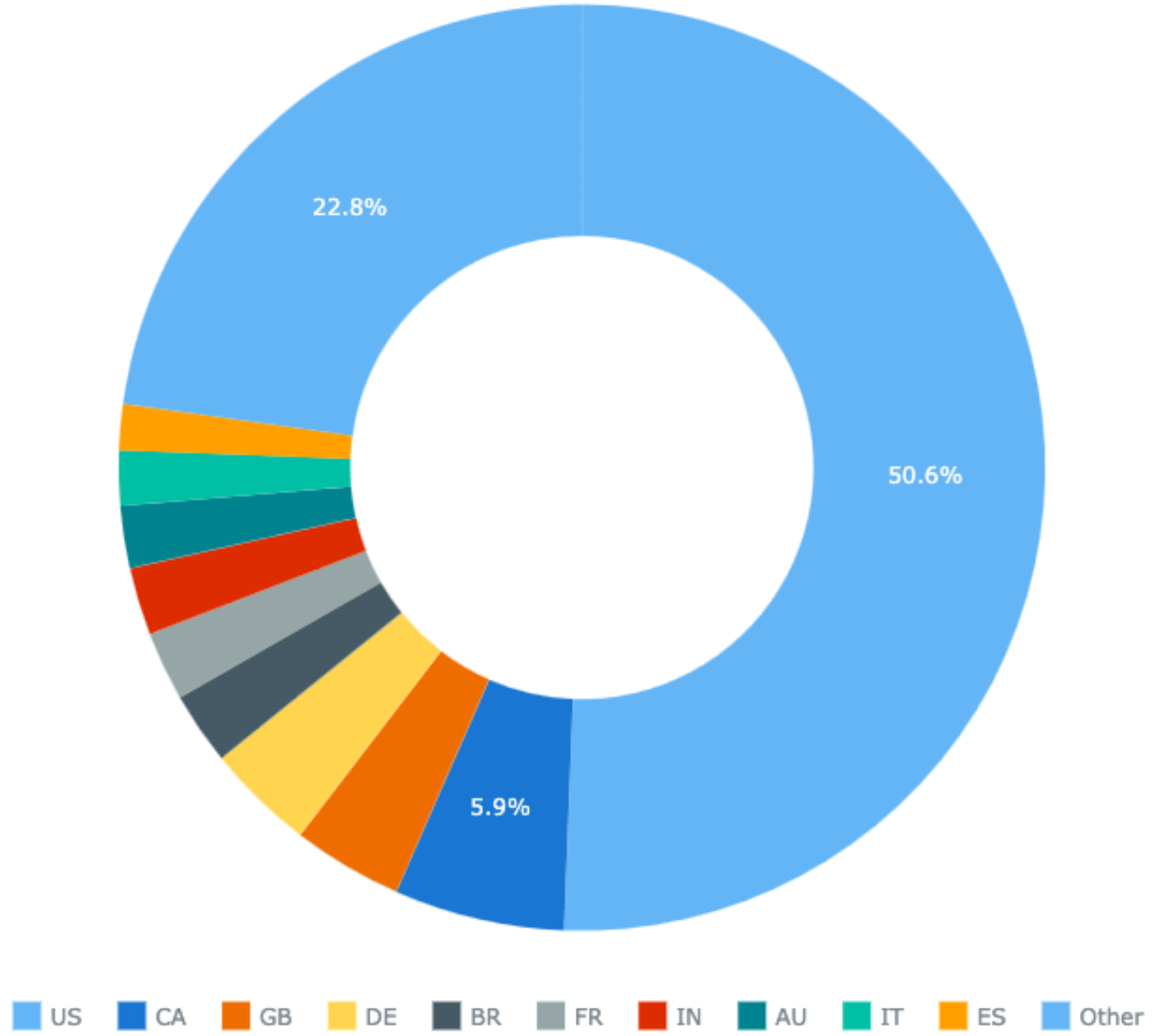
- 1,800 so far in 2025
- 6,100 attacks in 2024
- 5,300 in 2023
- Global Impact
- Across All Industries



Source: https://ransomware.live

Ransomware is Pervasive

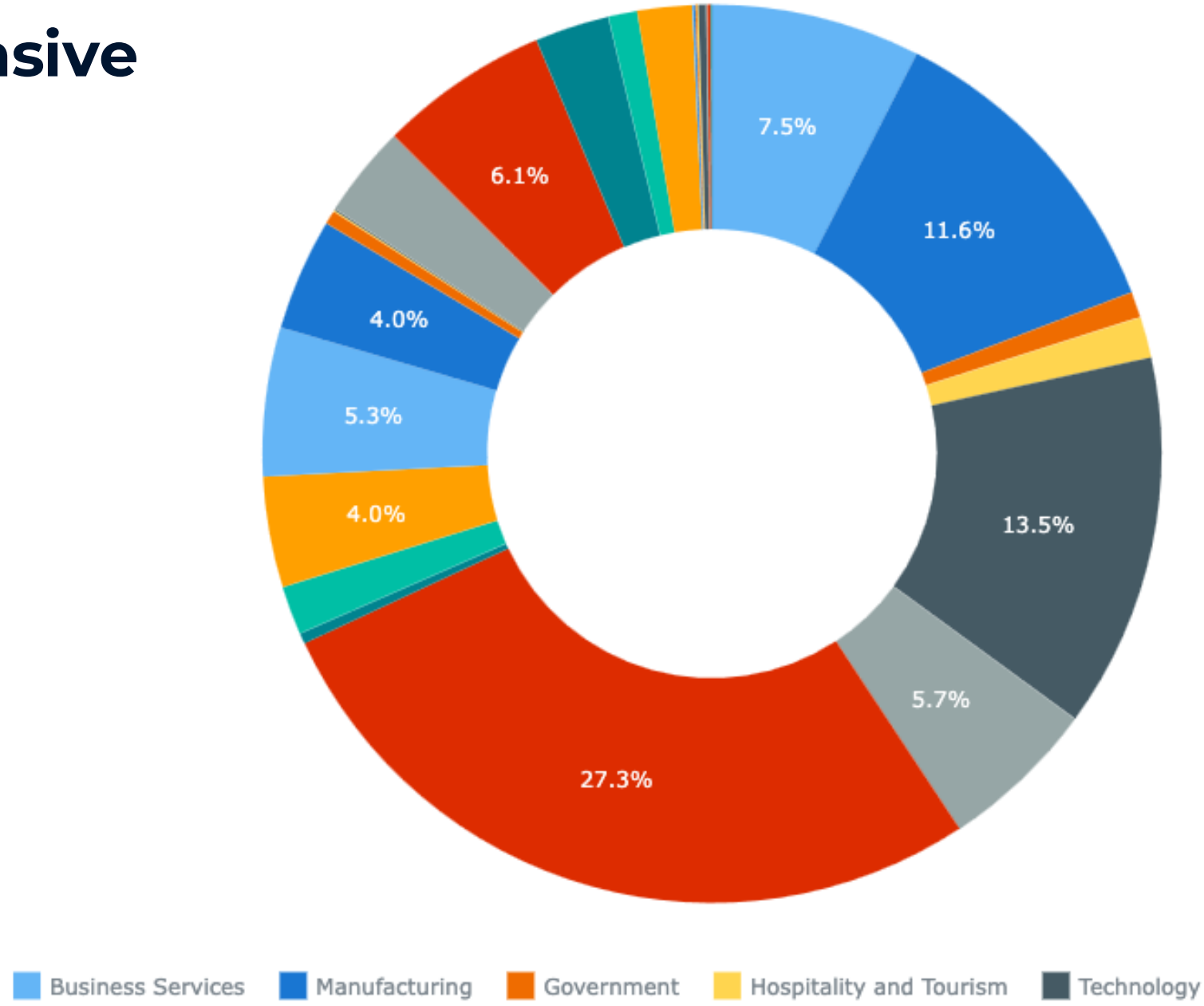
- 1,800 so far in 2025
- 6,100 attacks in 2024
- 5,300 in 2023
- Global Impact
- Across All Industries



Source: https://ransomware.live

Ransomware is Pervasive

- 1,800 so far in 2025
- 6,100 attacks in 2024
- 5,300 in 2023
- Global Impact
- Across All Industries



Source: https://ransomware.live

Multipronged Attack

1. Social Engineering (obtain credentials, identify systems)
2. Recent vulnerabilities
3. Human Error (TCP 3389)
4. Prebuilt, “Commercial” kits
5. Now with AI!

Goals

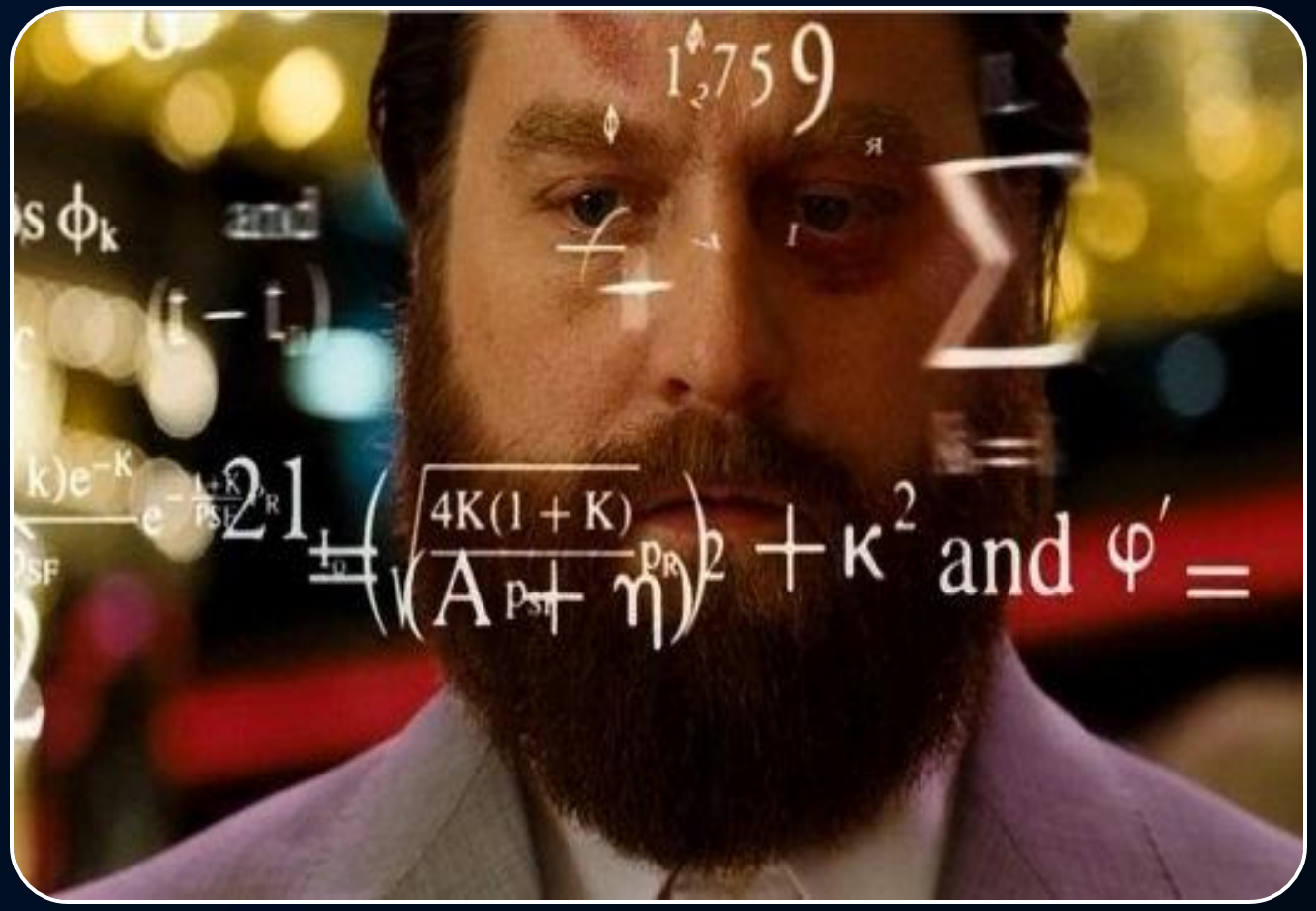
1. Credentials/Inventory
2. Exfiltrate
3. Remove Protections
4. Encrypt
5. Ransom

* MGM/Caesars: 4/5 reversed for fun and profit

MODERN DATA PROTECTION

Data Protection Prework

- Identify your core
  - Applications
  - Systems
  - Data
- Determine their RPO/RTO
- Design based on
  - Security
  - Requirements
  - Budget



Learning To Love 3-2-1

3 - 2 - 1 - 1 - 0

3	2	1	1	0
3 copies of your data	2 different media types	1 copy offsite & encrypted	1 “air-gapped” copy	0 errors in backup verification

A Layered Approach to Cyber Resilience

Backup Security Best Practices

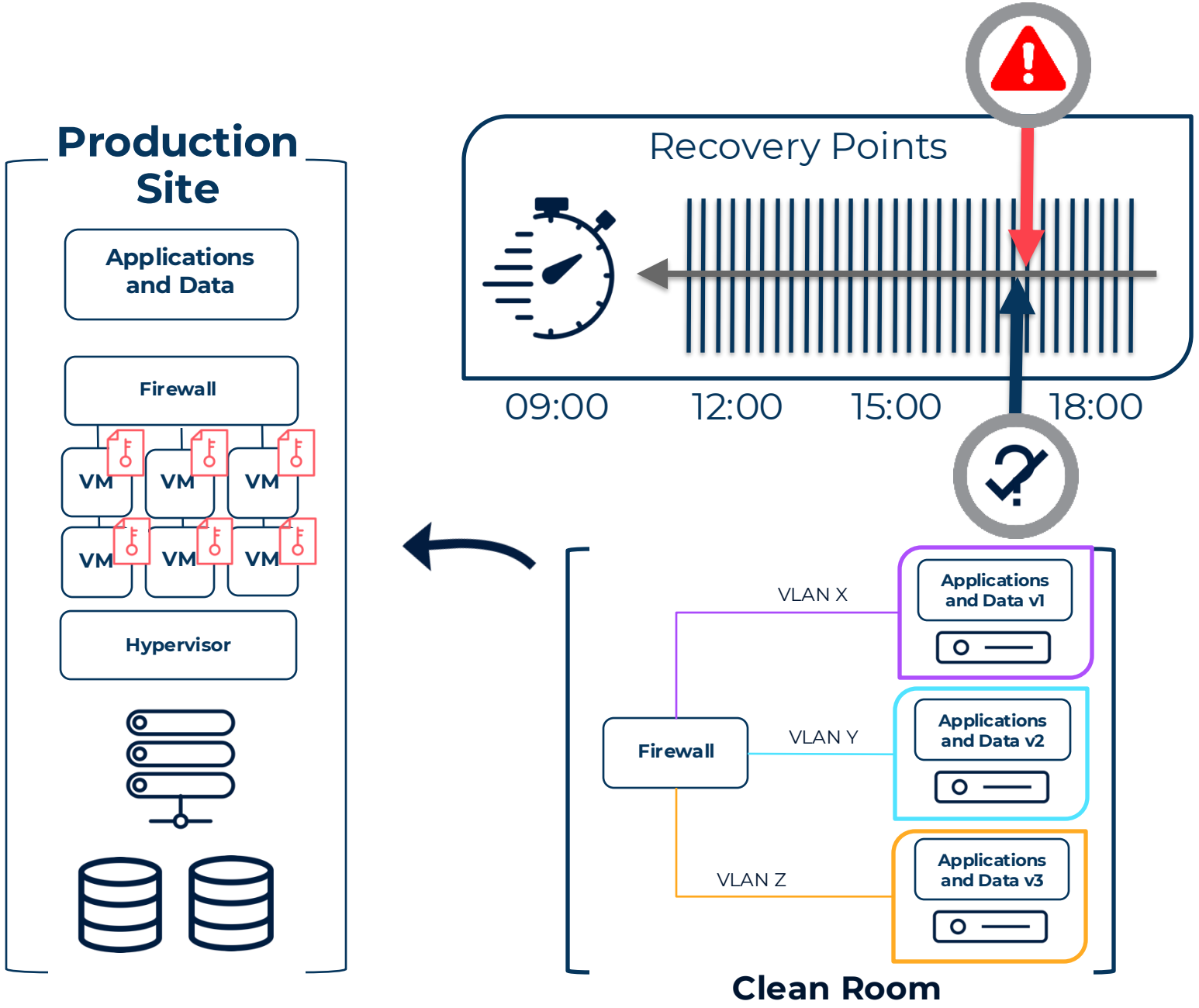
- Leverage immutability
- Encryption everywhere, with rotation
- Maintain 30-90 days standard retention
- Keep backup infrastructure isolated
- Ask stakeholders for input!!!
- Use AI but choose wisely
- Integrate backup with security tools
  - Errors, access logs to SIEM
  - XDR to vendor, vendor to XDR
  - SOAR scripting to block on events

SECURE RECOVERY

Secure Restore

- What, When, & Where
  - Know your own tiers
  - Prioritize operations
  - Know what goes where
- Create your runbook
  - Iterate through testing
  - Living document

Clean Room Recovery



Questions?

Q & A

Jim Jones

koolaid.info

@k00laidIT

THANK YOU