Honeypots & Real Threat Intel

Kat Fitzgerald

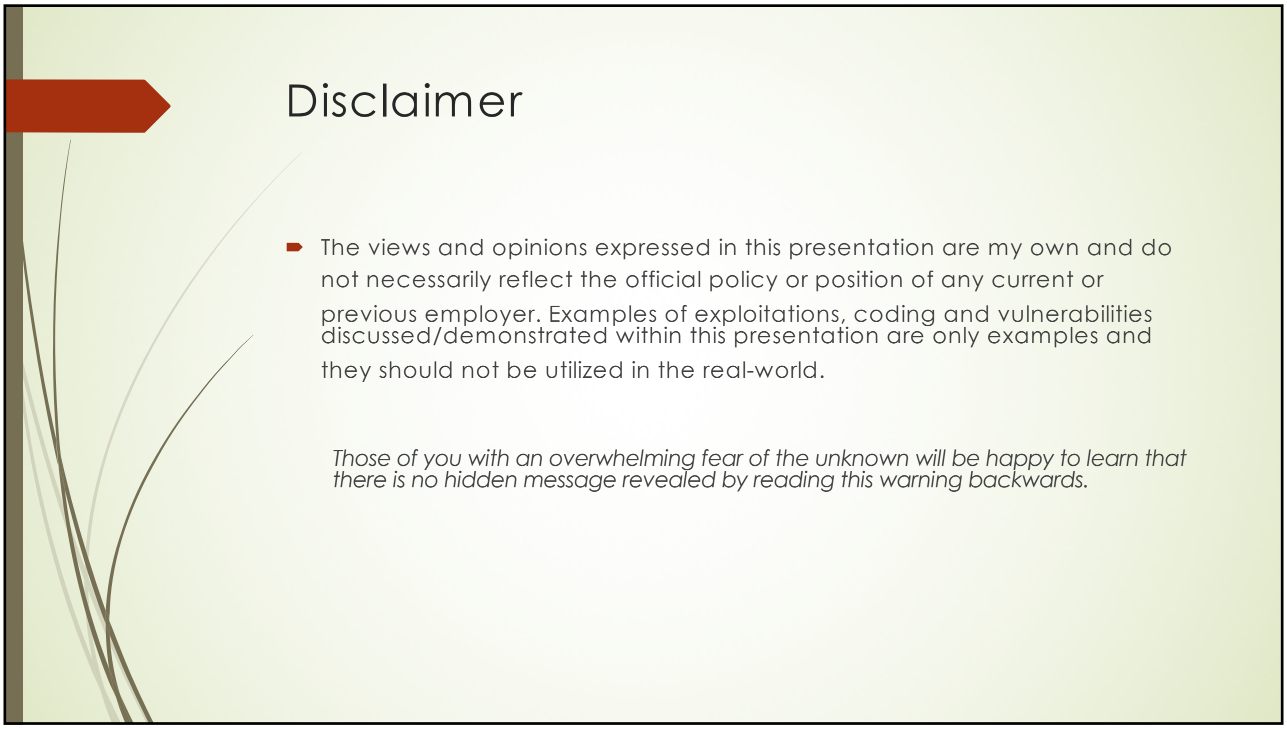
Principal Security Architect

whoami

$ whoami

Kat Fitzgerald (@rnbwkat or evilkat@rnbwmail.com)

- *First DEFCON was DC 3 (1995) with 16 speakers.*
- *Over 25(?) years in the Security field, with an emphasis on Security Operations, Incident Response and Purple Teams.*
- *Based in Chicago and a natural creature of winter, you can typically find me sipping Casa Noble Anejo whilst simultaneously defending my systems using OSS, magic spells and Dancing Flamingos against a barrage of attackers.*
- *Honeypots & Refrigerators*



Disclaimer

- The views and opinions expressed in this presentation are my own and do not necessarily reflect the official policy or position of any current or previous employer. Examples of exploitations, coding and vulnerabilities discussed/demonstrated within this presentation are only examples and they should not be utilized in the real-world.

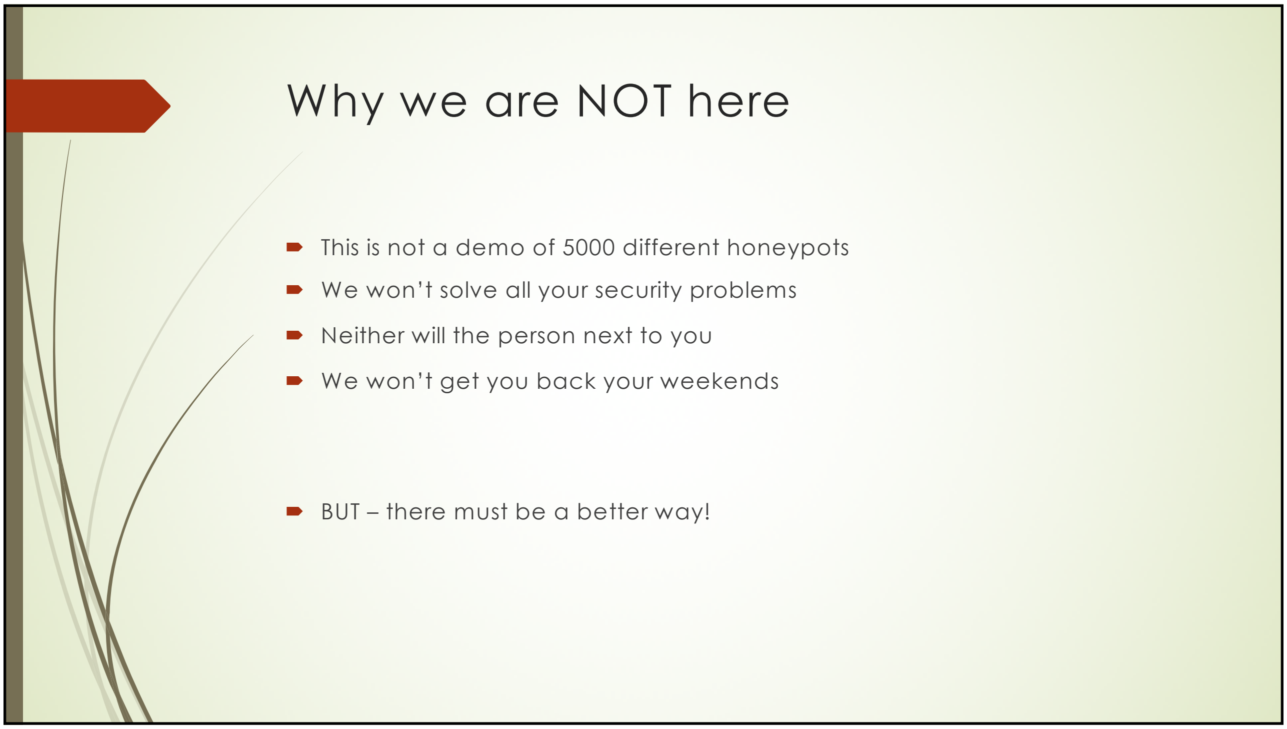
Those of you with an overwhelming fear of the unknown will be happy to learn that there is no hidden message revealed by reading this warning backwards.

Why are we here?

- $80 B! (2017)
- Attacks and breaches are common place
- Security Appliances and software are vulnerable
- Lateral Movement
- But what about –
  - Your Security Architecture is not unique
  - What is your "typical day"

Instead of Brilliance, we have standardized mediocrity.

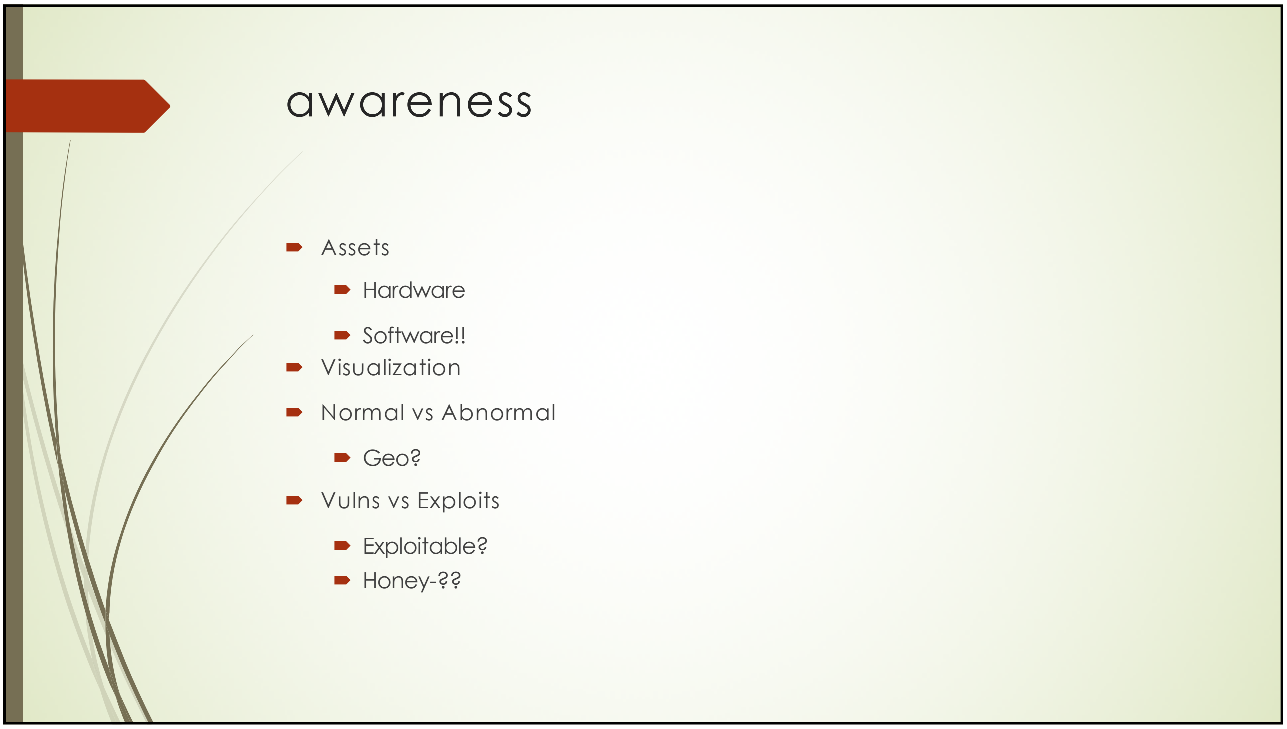
– John Strand, Offensive Countermeasures



Why we are NOT here

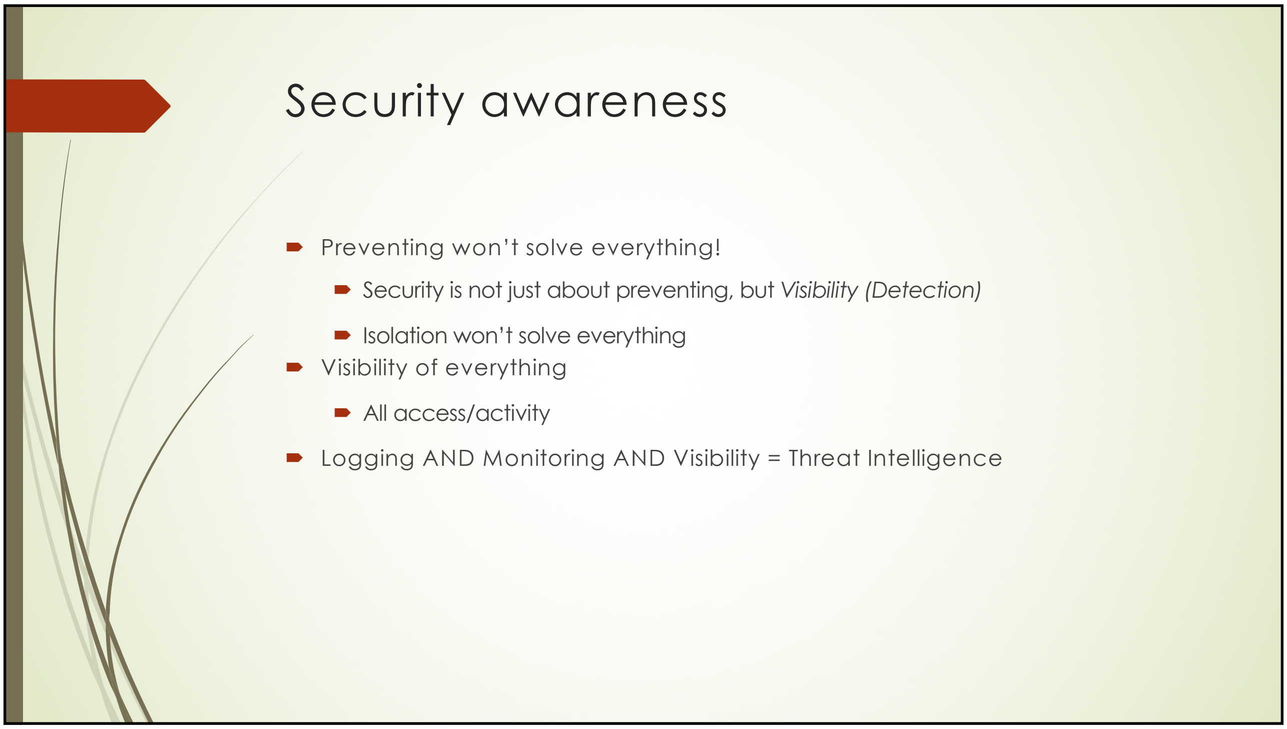
- This is not a demo of 5000 different honeypots
- We won't solve all your security problems
- Neither will the person next to you
- We won't get you back your weekends

- BUT – there must be a better way!



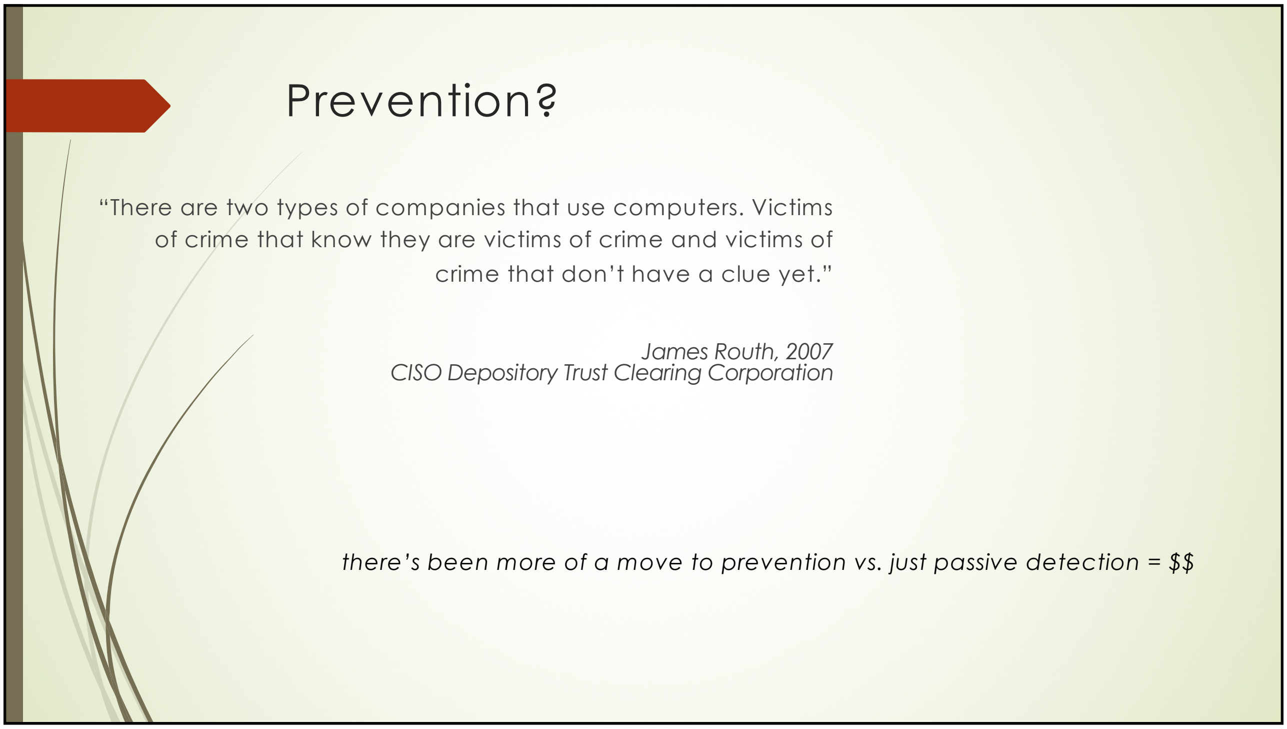
awareness

- Assets
  - Hardware
  - Software!!
- Visualization
- Normal vs Abnormal
  - Geo?
- Vulns vs Exploits
  - Exploitable?
  - Honey-??



Security awareness

- Preventing won't solve everything!
  - Security is not just about preventing, but *Visibility (Detection)*
  - Isolation won't solve everything
- Visibility of everything
  - All access/activity
- Logging AND Monitoring AND Visibility = Threat Intelligence



Prevention?

"There are two types of companies that use computers. Victims of crime that know they are victims of crime and victims of crime that don't have a clue yet."

James Routh, 2007
CISO Depository Trust Clearing Corporation

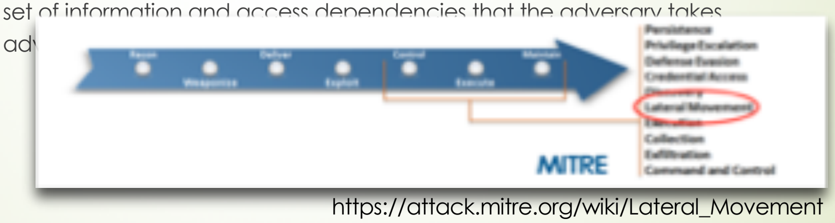
there's been more of a move to prevention vs. just passive detection = $$

HoneypotS

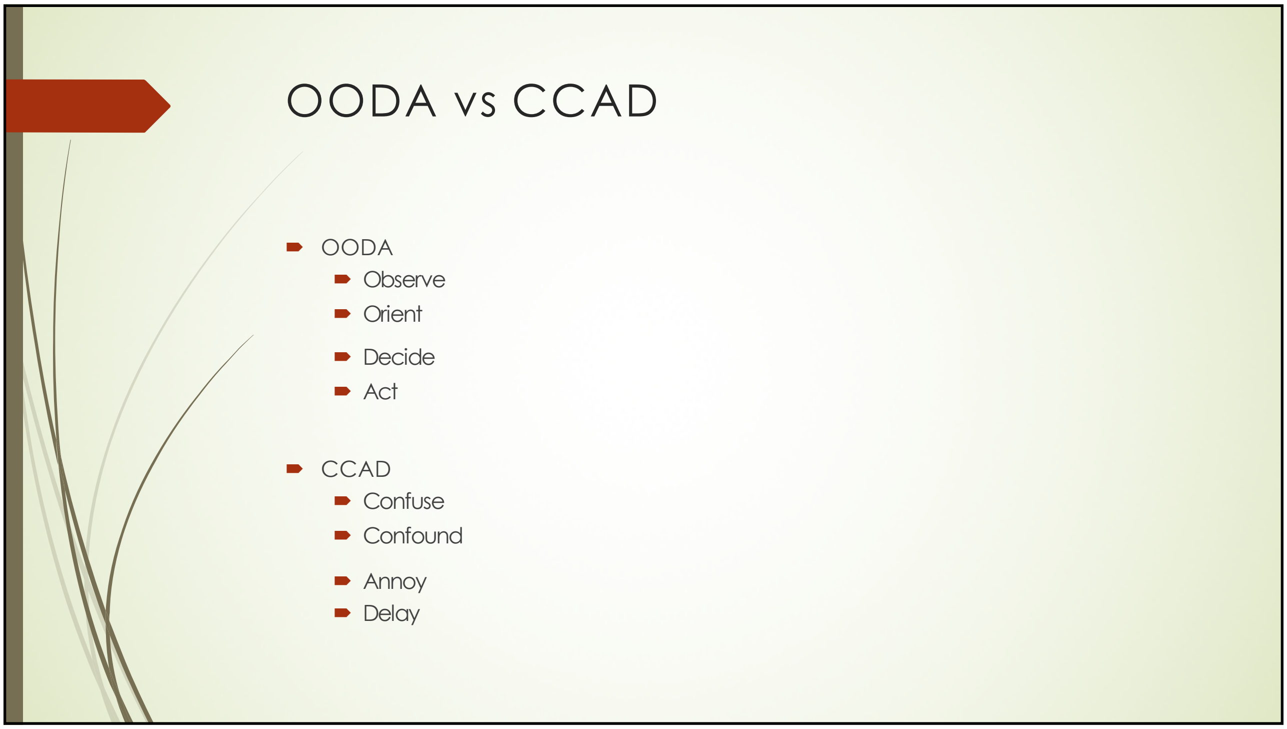
- Honeypots vs Deception
  - A resource with no value
    - Value = Use of Resource
  - -Not Hack Back
    - (Yet?)
- Important Points
  - Deployment = Architecture
  - Architecture = Deployment
  - Planning!
  - 100's of "types"

Lateral Movement

- Enables an adversary to access and control remote systems on a network.
- Could allow an adversary to gather information from a system without needing additional tools.
- Can be used for remote execution of tools, pivoting to additional systems, access to specific information or files, access to additional credentials, etc.
- Is often very important to an adversary's set of capabilities and part of a broader set of information and access dependencies that the adversary takes ad

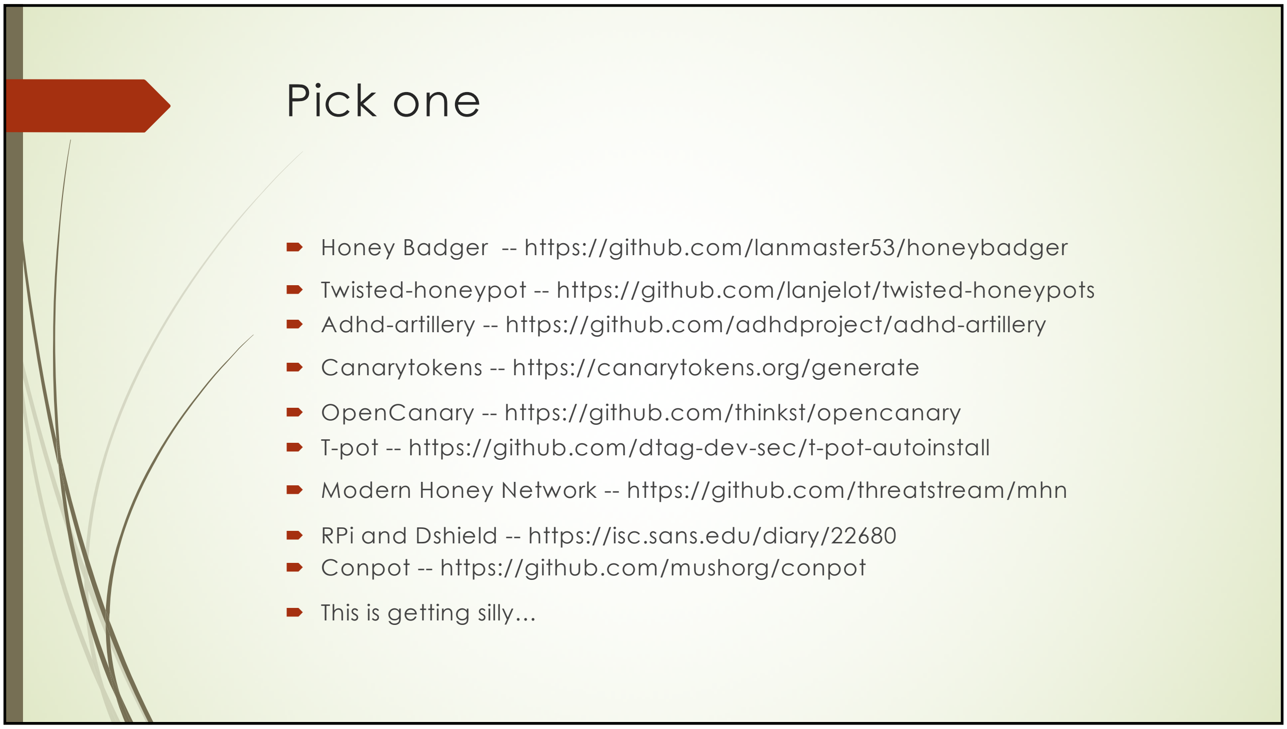


https://attack.mitre.org/wiki/Lateral_Movement



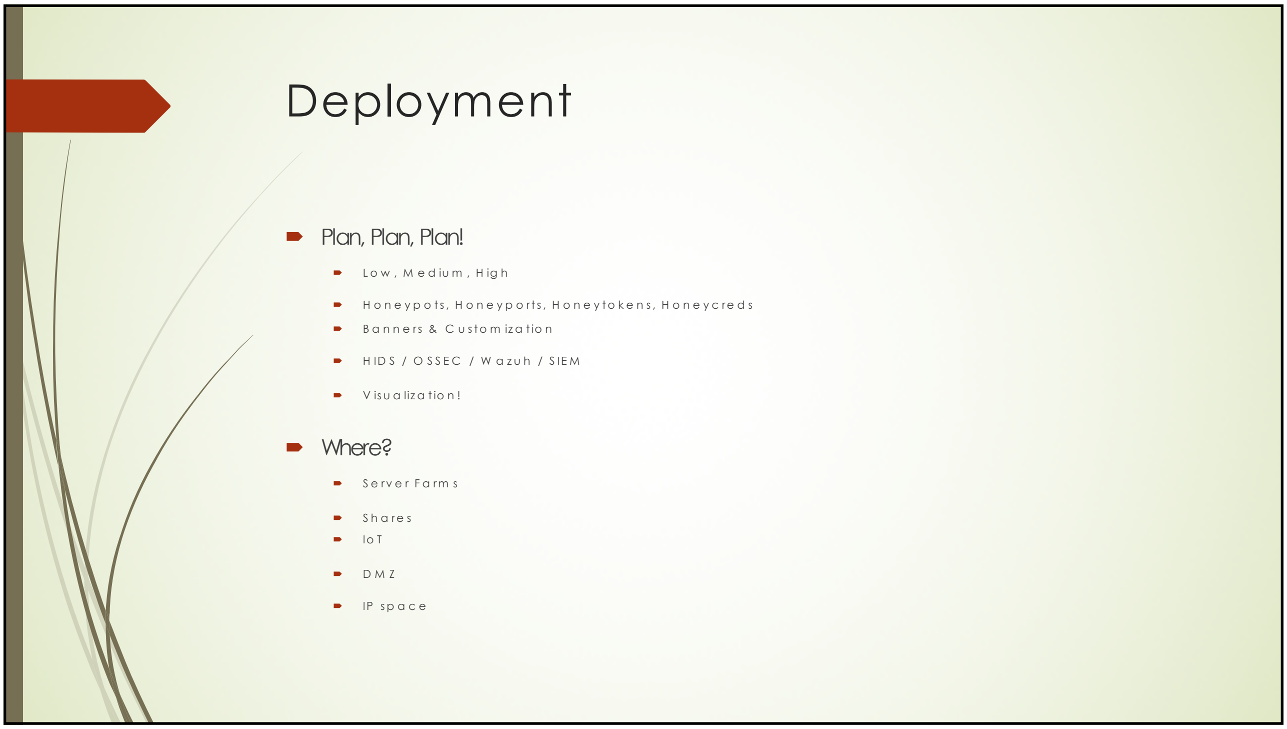
OODA vs CCAD

- OODA
  - Observe
  - Orient
  - Decide
  - Act
- CCAD
  - Confuse
  - Confound
  - Annoy
  - Delay



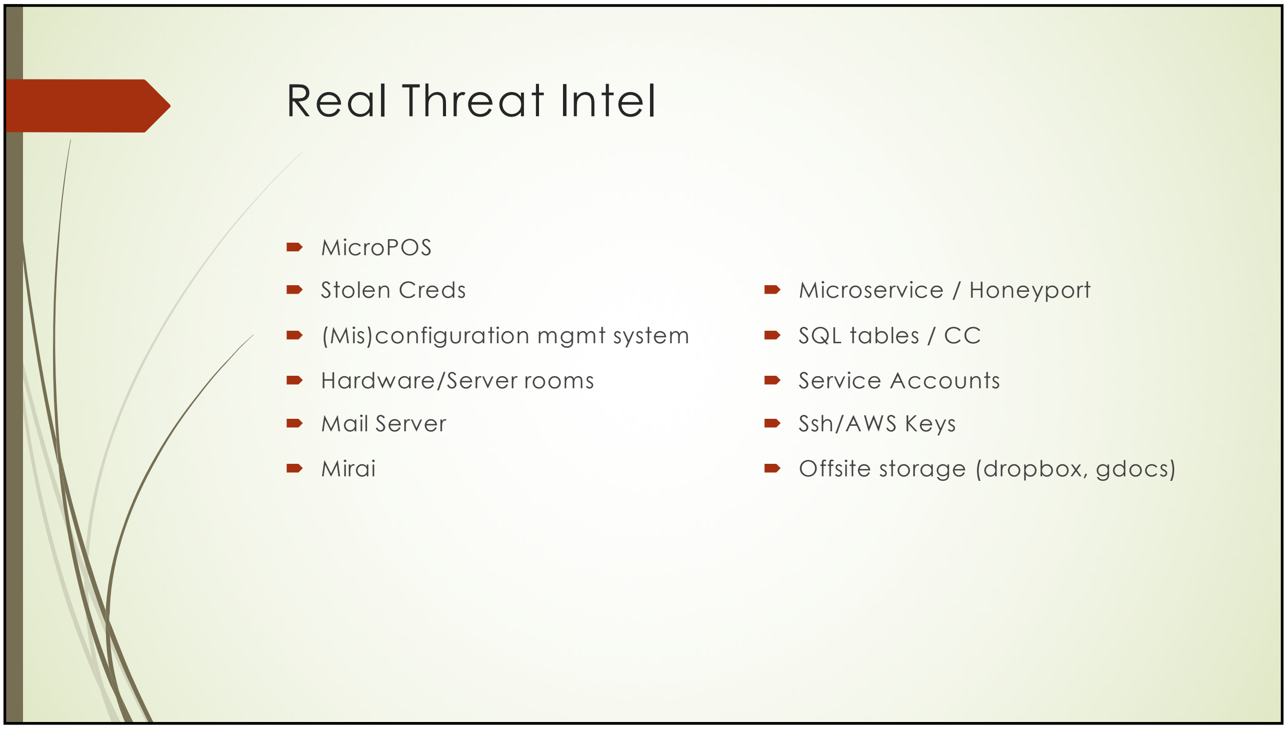
Pick one

- Honey Badger -- https://github.com/lanmaster53/honeybadger
- Twisted-honeypot -- https://github.com/lanjelot/twisted-honeypots
- Adhd-artillery -- https://github.com/adhdproject/adhd-artillery
- Canarytokens -- https://canarytokens.org/generate
- OpenCanary -- https://github.com/thinkst/opencanary
- T-pot -- https://github.com/dtag-dev-sec/t-pot-autoinstall
- Modern Honey Network -- https://github.com/threatstream/mhn
- RPi and Dshield -- https://isc.sans.edu/diary/22680
- Conpot -- https://github.com/mushorg/conpot
- This is getting silly…



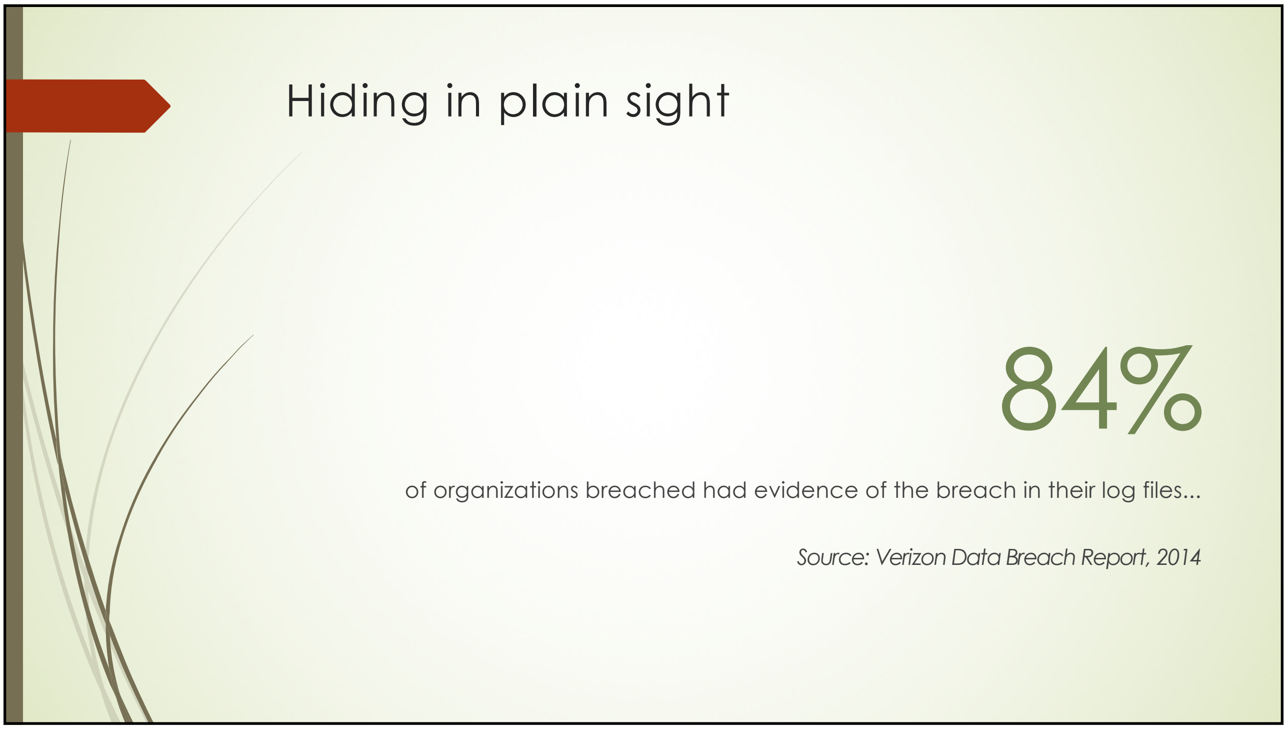
Deployment

- Plan, Plan, Plan!
  - Low, Medium, High
  - Honeypots, Honeyports, Honeytokens, Honeycreds
  - Banners & Customization
  - HIDS / OSSEC / Wazuh / SIEM
  - Visualization!
- Where?
  - Server Farms
  - Shares
  - IoT
  - DMZ
  - IP space



Real Threat Intel

- MicroPOS
- Stolen Creds
- (Mis)configuration mgmt system
- Hardware/Server rooms
- Mail Server
- Mirai
- Microservice / Honeyport
- SQL tables / CC
- Service Accounts
- Ssh/AWS Keys
- Offsite storage (dropbox, gdocs)

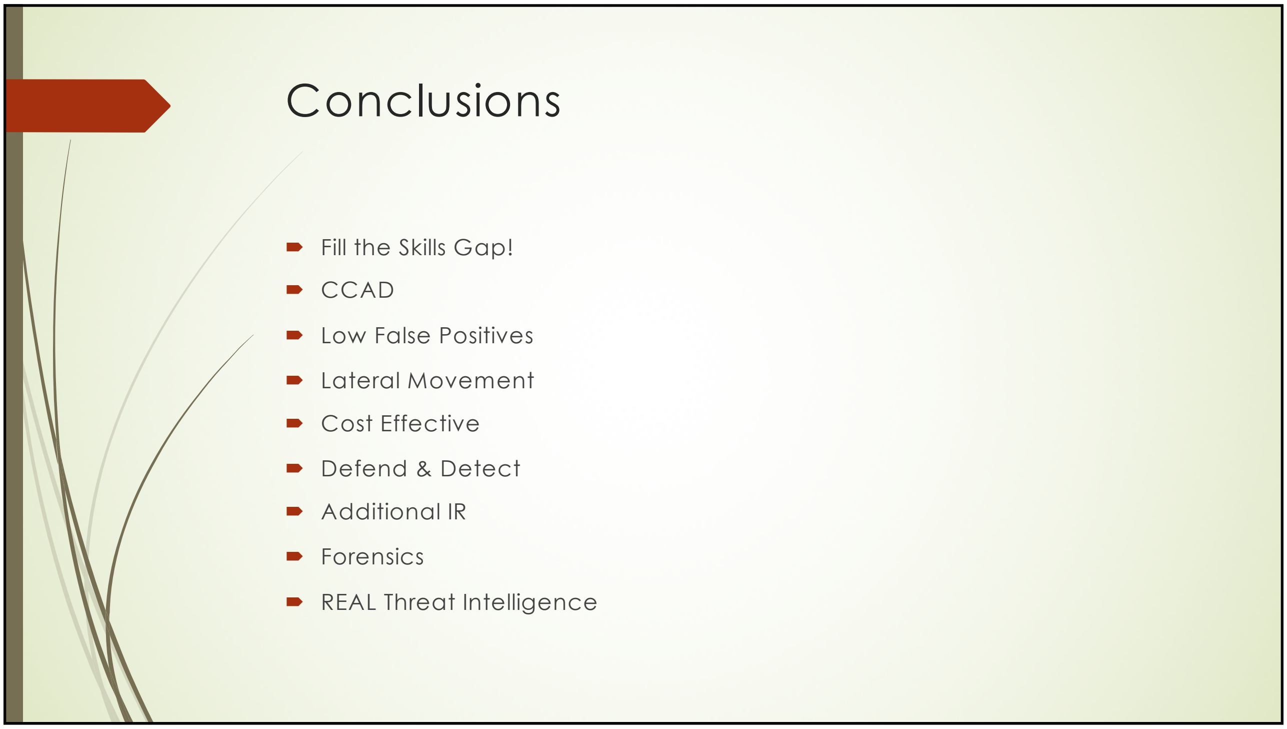


Hiding in plain sight

84%

of organizations breached had evidence of the breach in their log files…

Source: Verizon Data Breach Report, 2014



Conclusions

- Fill the Skills Gap!
- CCAD
- Low False Positives
- Lateral Movement
- Cost Effective
- Defend & Detect
- Additional IR
- Forensics
- REAL Threat Intelligence

Bottom line

You can not *protect* anything without
first *identifying* assets and risks faced by each.

You can not *respond* to events if you have
not implemented proper measures to *detect* them.

…And Finally

Thank you

Kat Fitzgerald

evilkat@rnbwmail.com

@rnbwkat