websense®

# USAGE PRACTICES AND USER REQUIREMENTS

Carl Leonard
Principal Security Analyst

BRAVE THE NEW WORLD.

# BRAVE THE NEW WORLD.

WE ENABLE ORGANIZATIONS TO **PREVENT DATA THEFT** WHILE **INNOVATING** AND **GROWING** IN THIS AGE OF **DISRUPTIVE CHANGE**.

websense®

# ENISA 2014 – Top 15 Threats

1. Malicious code: Worms/Trojans ↑

2. Web-based attacks ↑

[redacted]

4. Botnets ↓

[redacted]

6. Spam ↓

7. Phishing ↑

8. Exploit kits ↓

9. Data breaches ↑

[redacted]

11. Insider threat →

12. Information leakage ↑

13. Identity theft/fraud ↑

14. Cyber espionage ↑

15. Ransomware/ Rogueware/ Scareware ↓

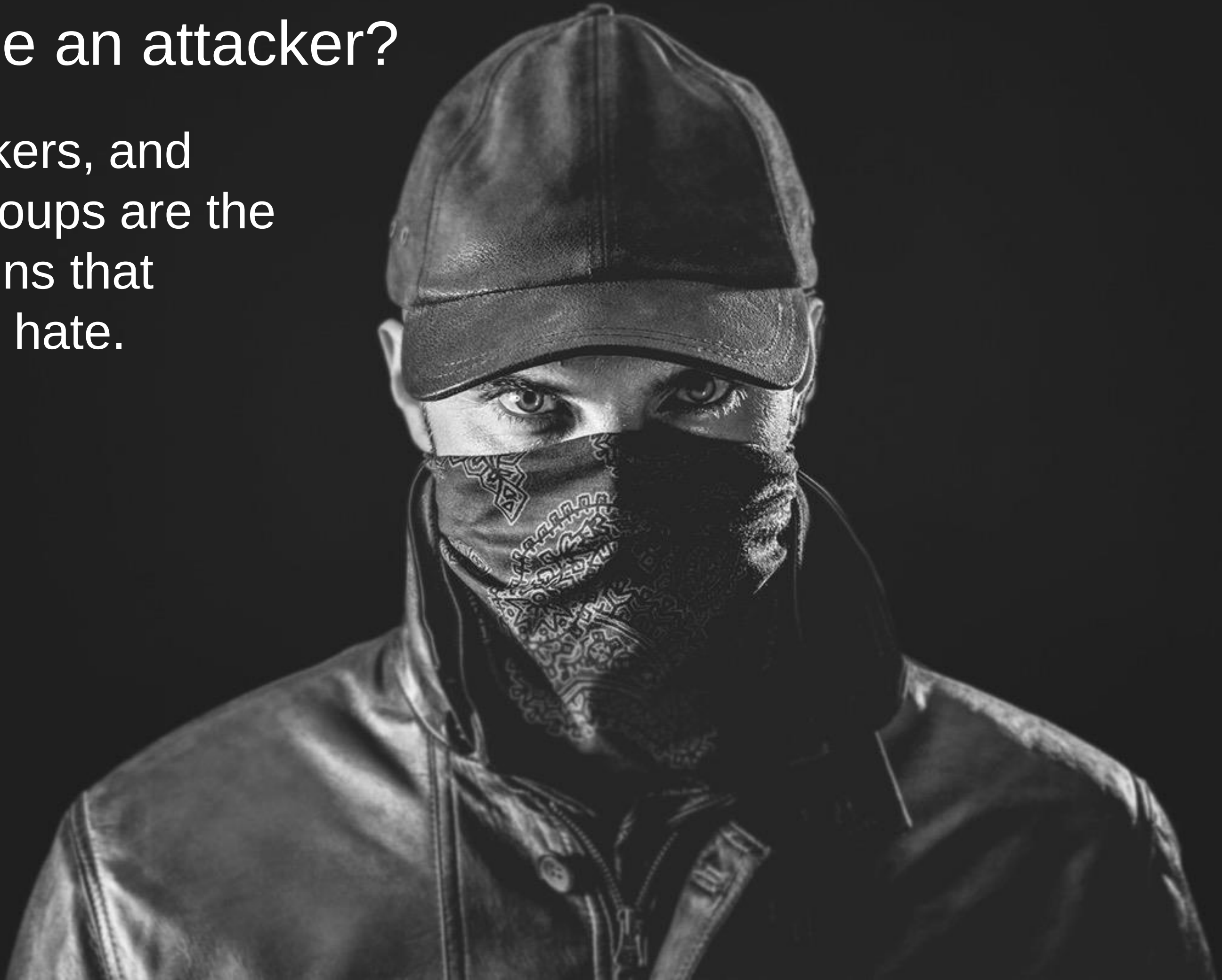
# Profiling an Attacker

BRAVE THE NEW WORLD.

# Can you recognise an attacker?

- Nation-states, hackers, and organized crime groups are the cyber security villains that everybody loves to hate.

- BUT…



* PwC - The Global State of Information Security® Survey 2014 & 2015

# Can you recognise an attacker?

- EMPLOYEES ARE THE MOST-CITED CULPRITS OF INCIDENTS*

- 32% of respondents said insider crimes are more costly or damaging than incidents perpetrated by outsiders.

* PwC - The Global State of Information Security® Survey 2014 & 2015

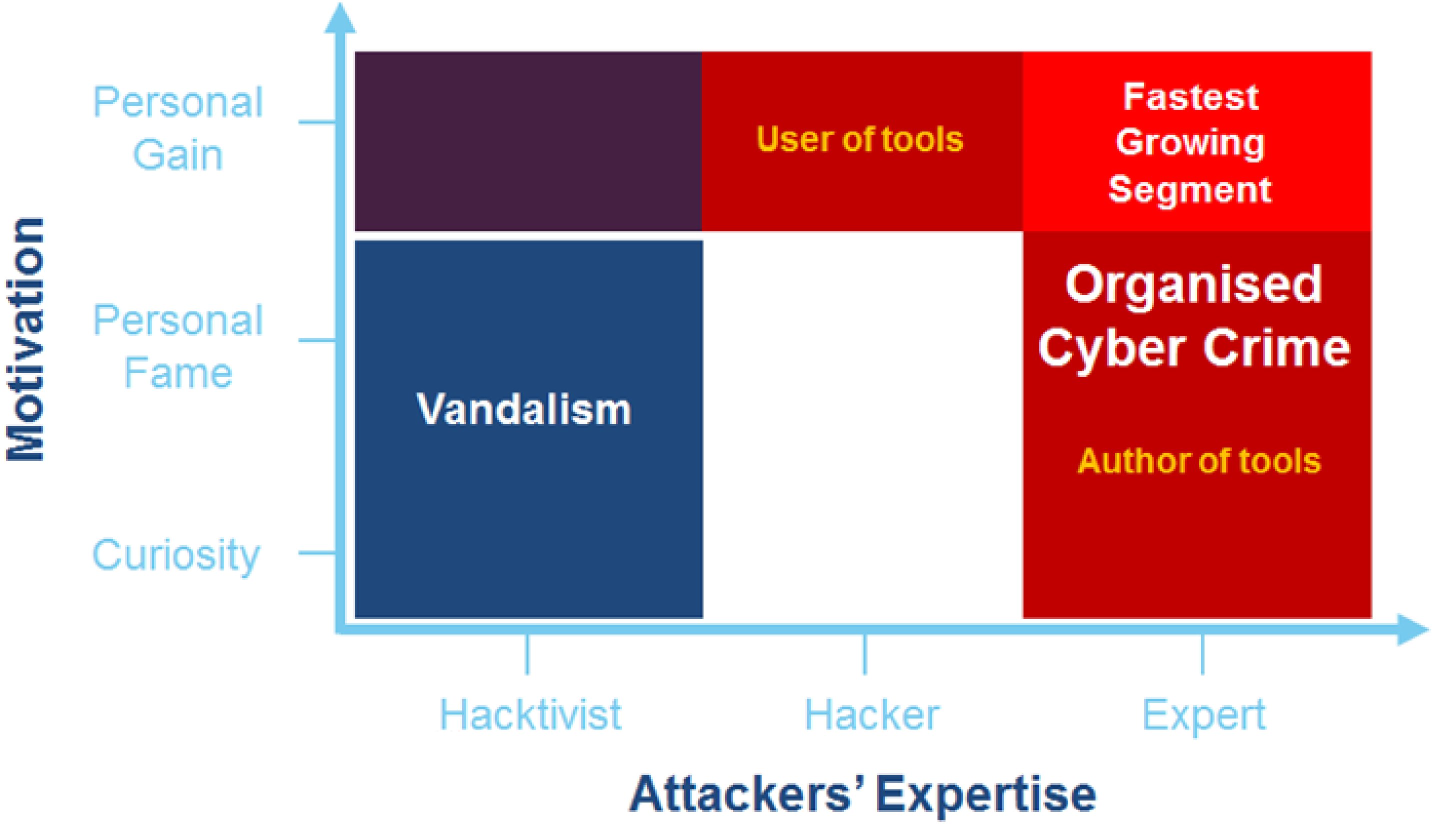
# Attackers Have Evolved

| | |
|---|---|
| Goals: | Profit and disruption |
| Skill Level: | Professional |
| Success Level: | High |

- Advanced is the new normal

- Evasion techniques are common:
  - Sophisticated social engineering to defeat end-users
  - Evasion tactics within the malicious payload to defeat sandboxes
  - Custom Encryption to C&C to defeat analysis
  - Polymorphism to defeat signatures

# Skill vs. Motivation



websense®

# Profiling a Defender

BRAVE THE NEW WORLD.

# Defenders Must Evolve

| | |
|---|---|
| Goals: | To protect their data |
| Skill Level: | Low-Medium |
| Success Level: | Low |

- Business challenges must be overcome
- Attack techniques are increasingly advanced
- Defenders seek to be pro-active but don’t have the tools or the skill set

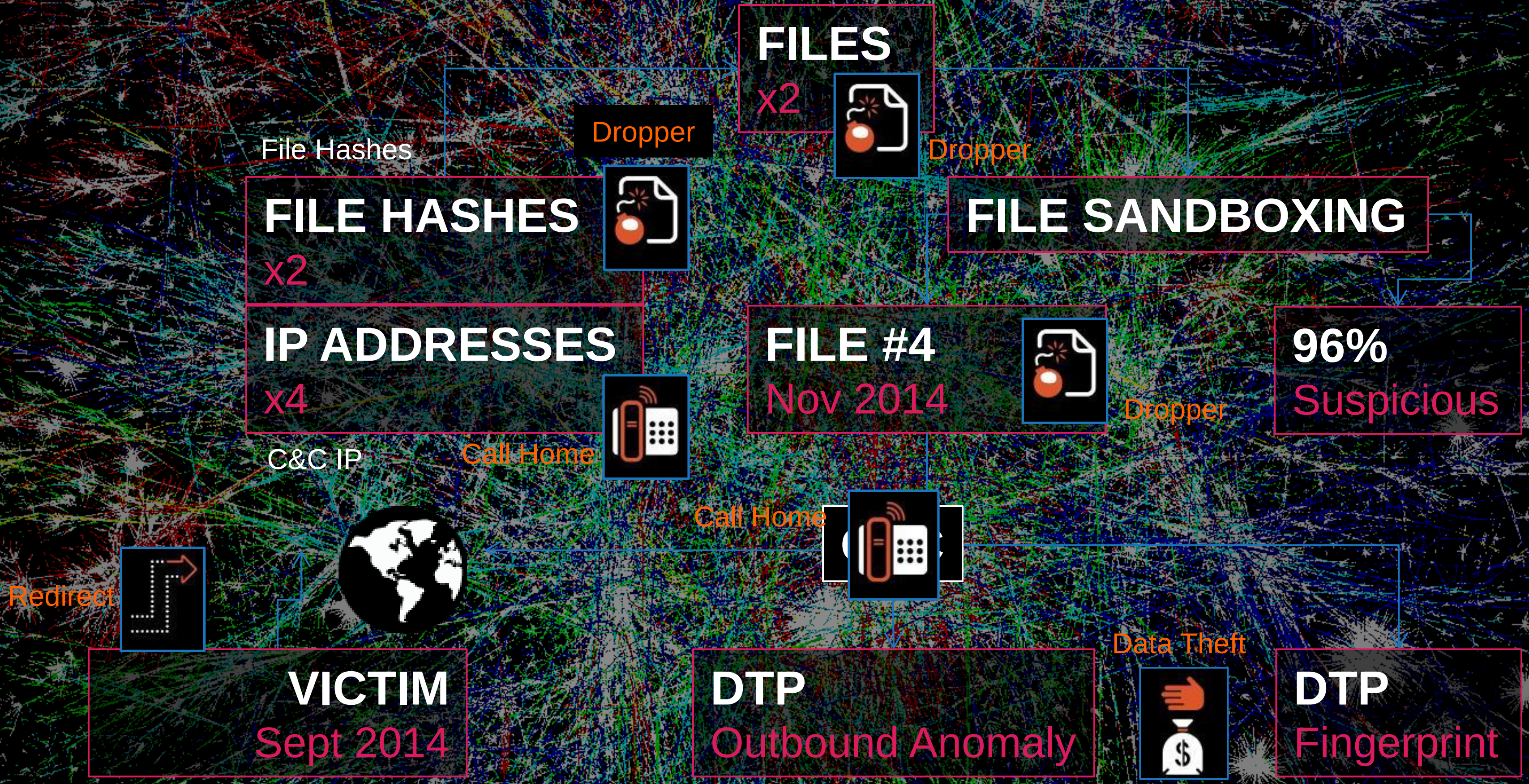
websense®

# Challenges

BRAVE THE NEW WORLD.

# Business-level Challenges

- Budget Squeeze
- Skills Shortage
- Increased Risk of Attack
- Regulation, Regulation, Regulation
- New Platforms…Internet Of Things, Cloud
- Old Platforms…Bring Your Own Device, Cloud



FILES
x2

Dropper

File Hashes

Dropper

FILE HASHES
x2

FILE SANDBOXING

IP ADDRESSES
x4

FILE #4
Nov 2014

Dropper

96%
Suspicious

C&C IP

Call Home

Call Home

Redirect

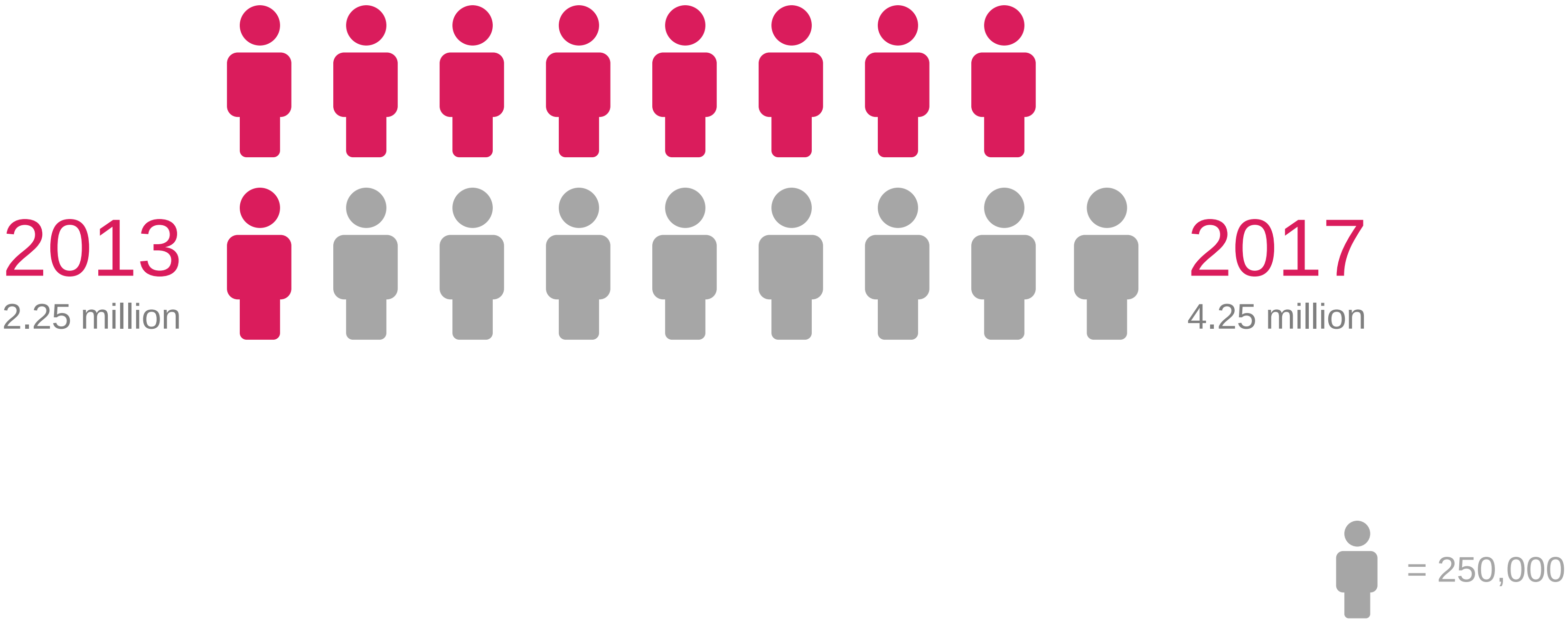
VICTIM
Sept 2014

DTP
Outbound Anomaly

Data Theft

DTP
Fingerprint

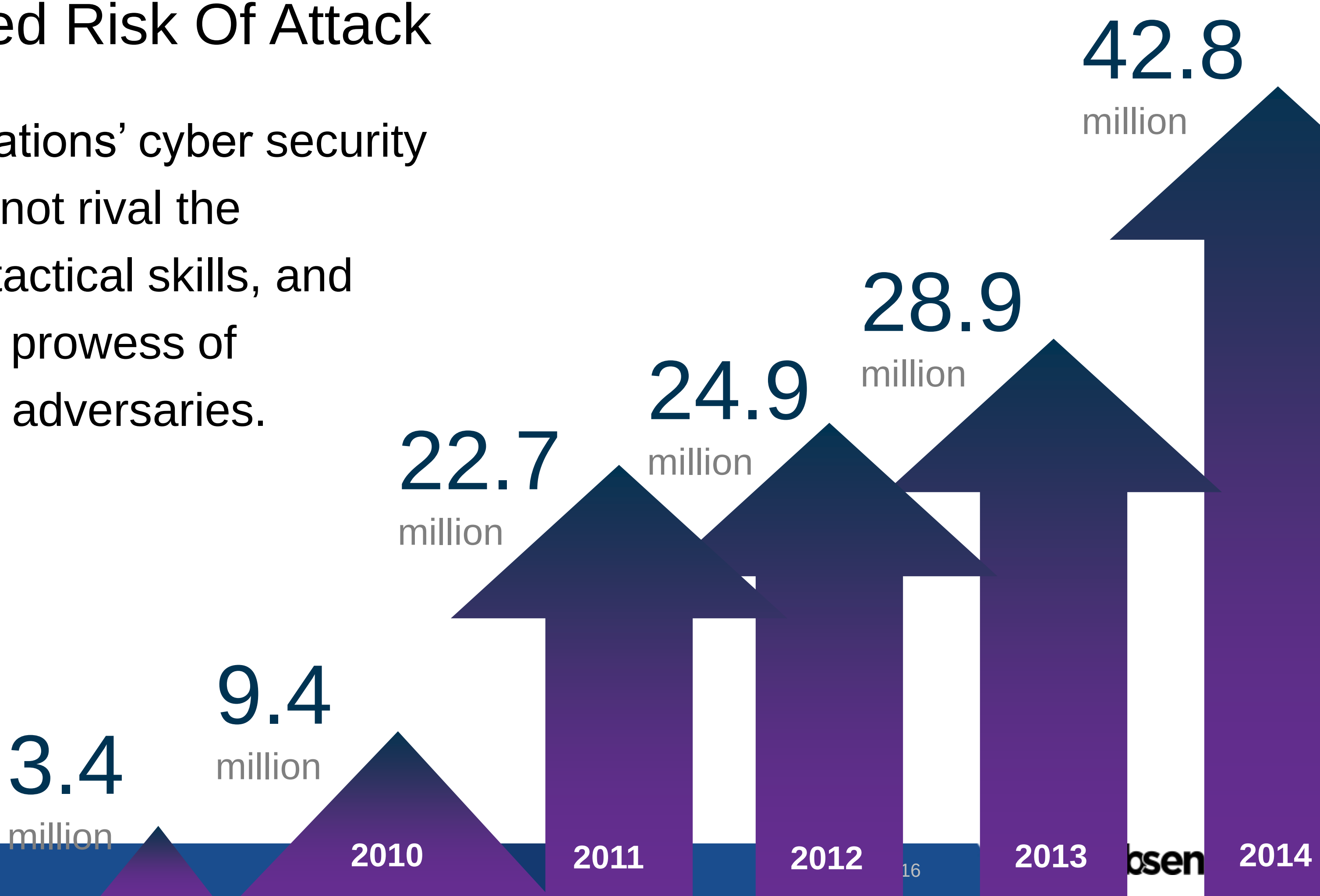
# #2 Skills Shortage



2013 (ISC)2 Global Information Workforce Study

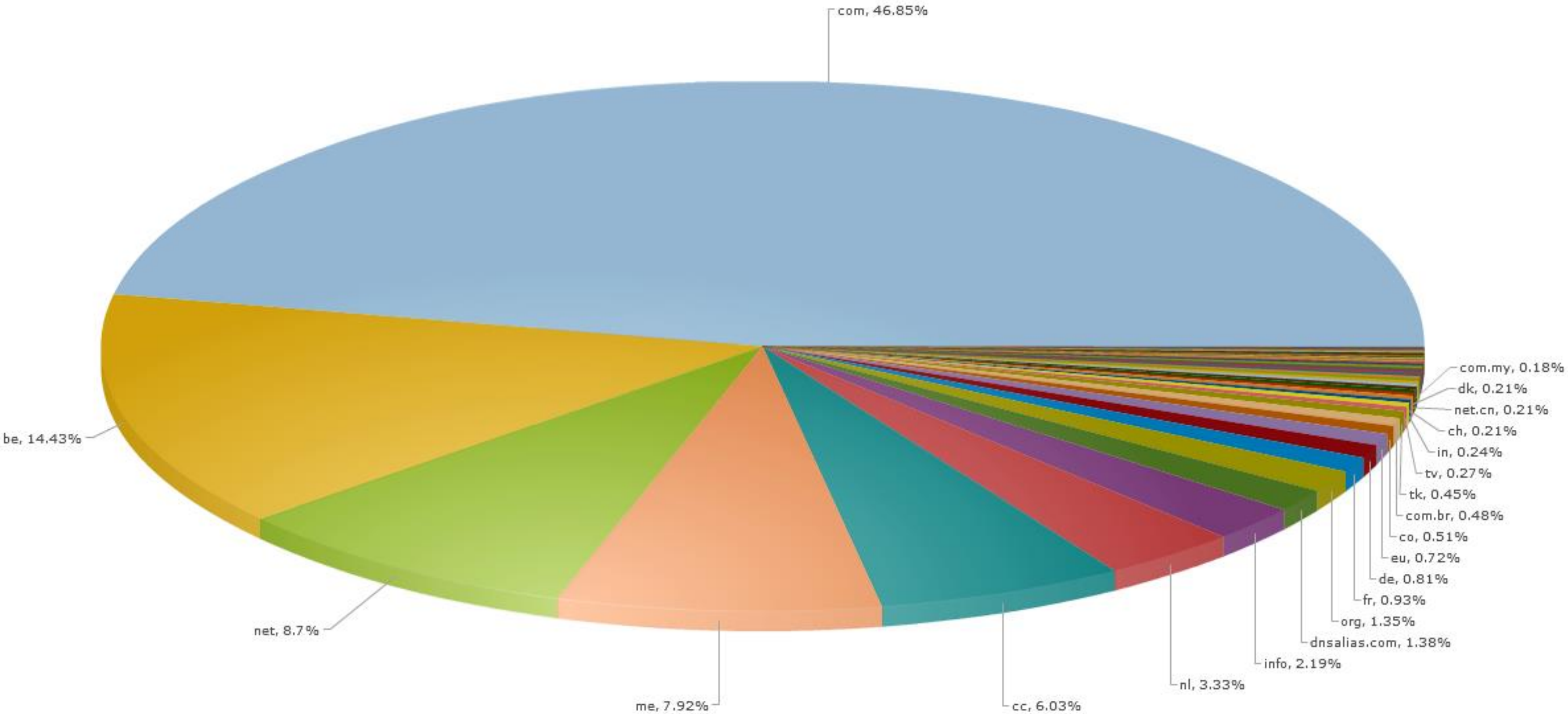
# #3 Increased Risk Of Attack

Most organizations' cyber security programs do not rival the persistence, tactical skills, and technological prowess of today's cyber adversaries.

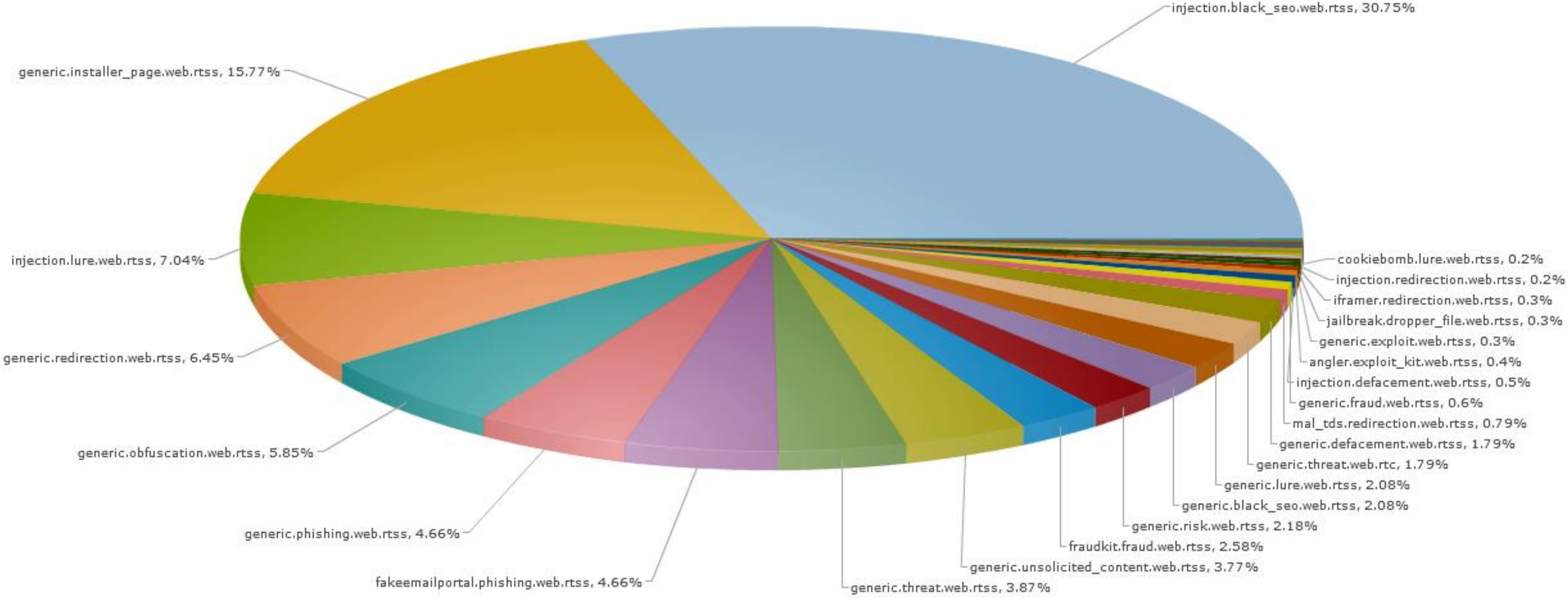


PwC - The Global State of Information Security® Survey 2014 & 2015

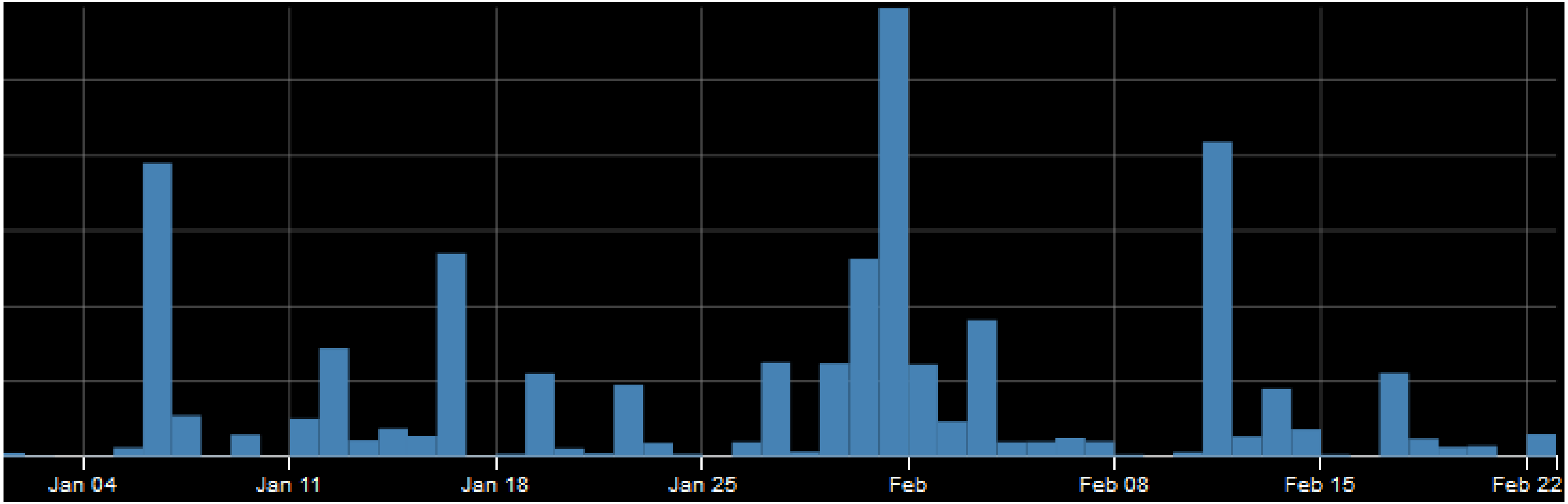
# Security Profile: Belgium: TLD



# Security Profile: Belgium: Threat Type

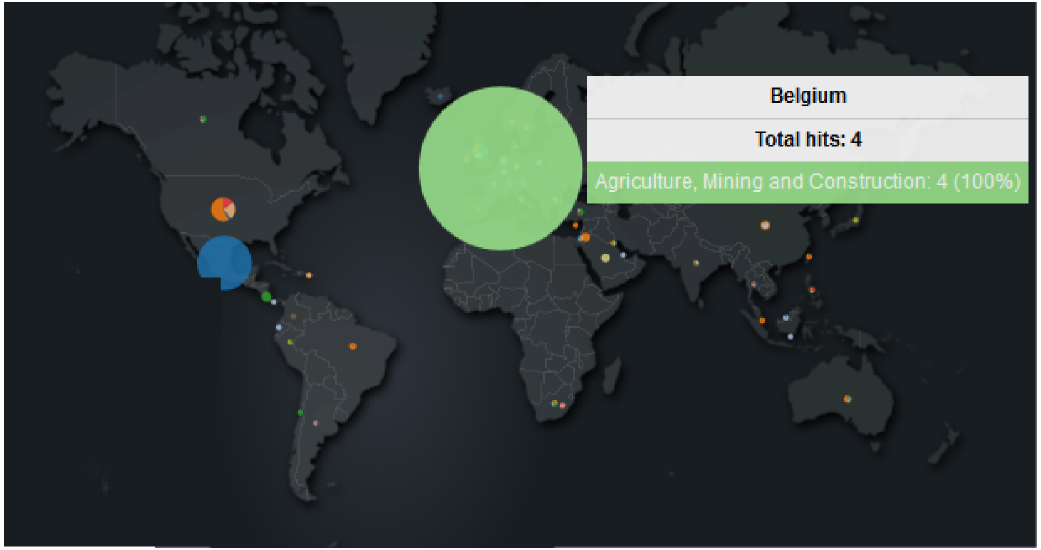


# Security Profile: Belgium: Industry

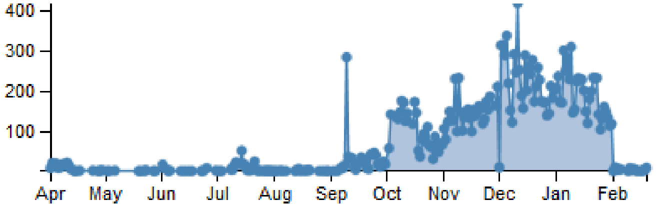


# Security Profile: Belgium: Lateral Movement

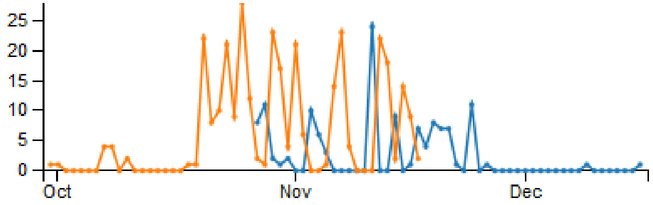
## Detections by Location and Industry



## Timeline



## Attachment and URL Detections



# Attack-level Challenges

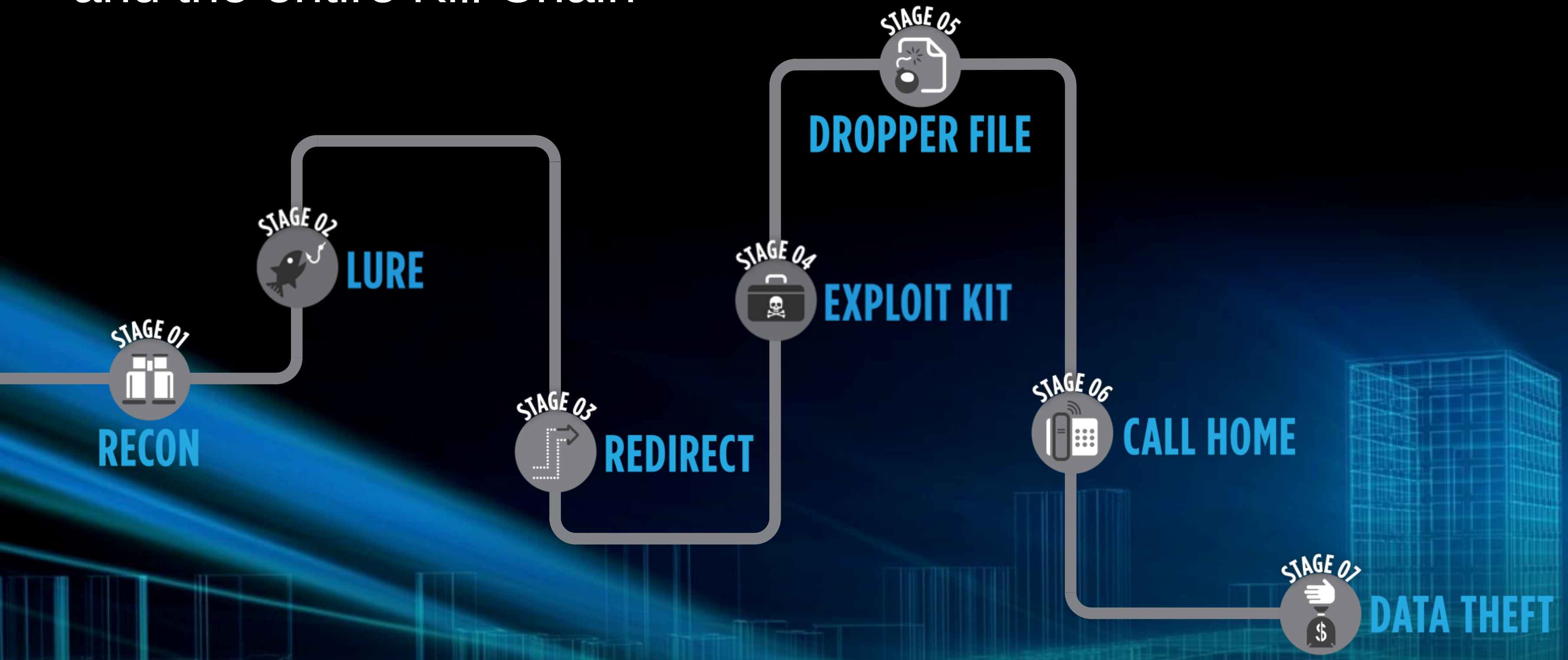
- Protection is not guaranteed

- Unable to handle threats at all stages along the kill chain (aka threat lifecycle)

- Too much data and too much noise

- The data we seek to protect is now unstructured; was structured

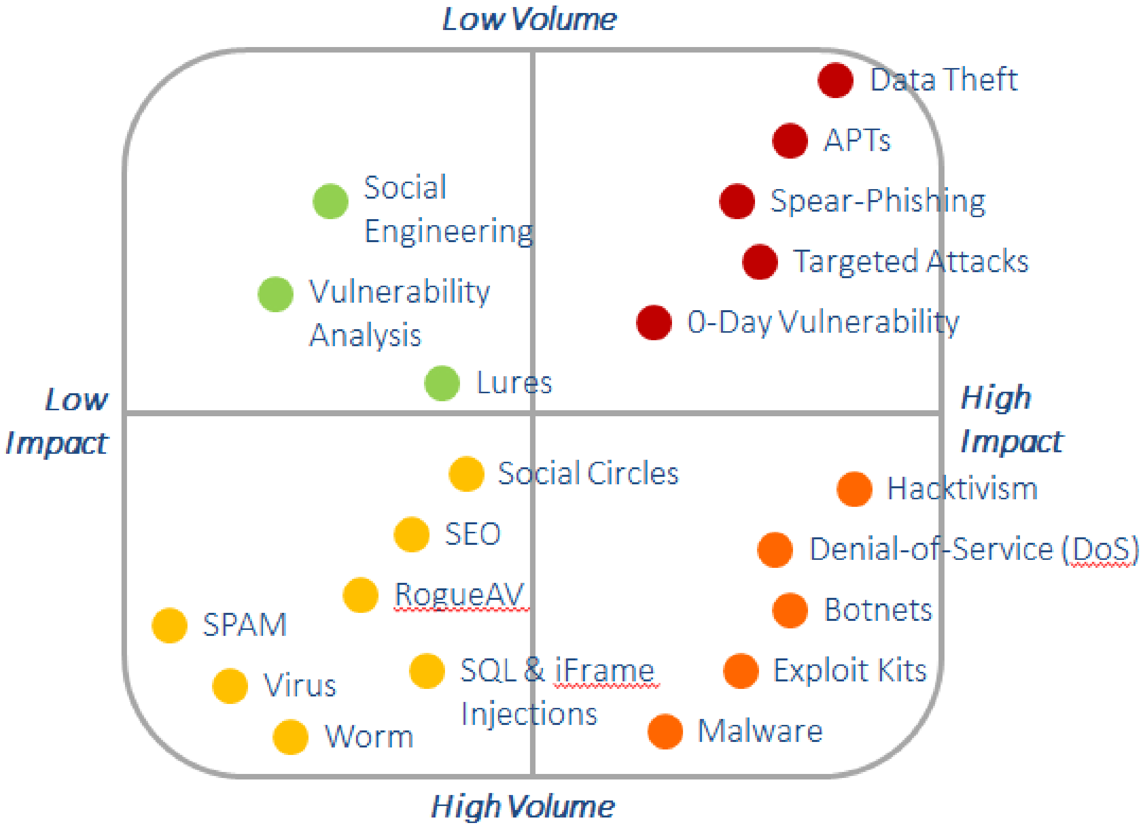
# Protect everyone, everywhere, across all channels and the entire Kill Chain



# Threat Risk Modelling

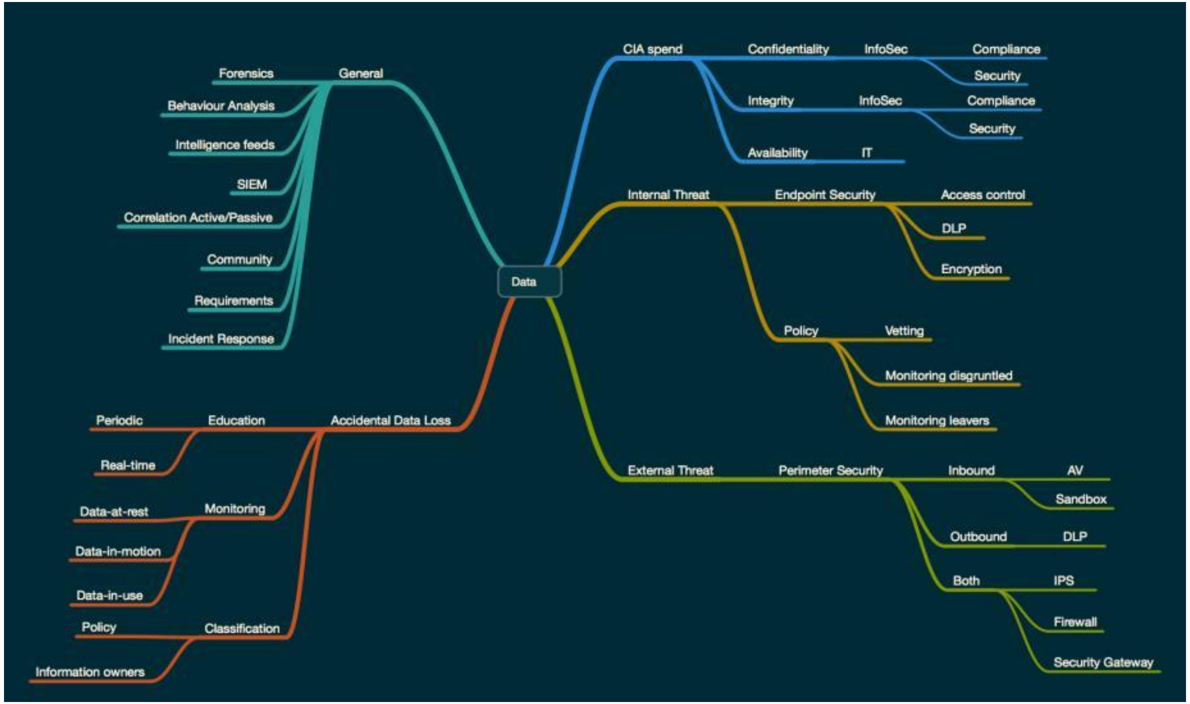
**PRESENT**
Low volume
Persistent
Targeted/focus
Data theft
Profit

**PAST**
High volume
Short lifespan
Visible/news
Infection/deface
Limelight

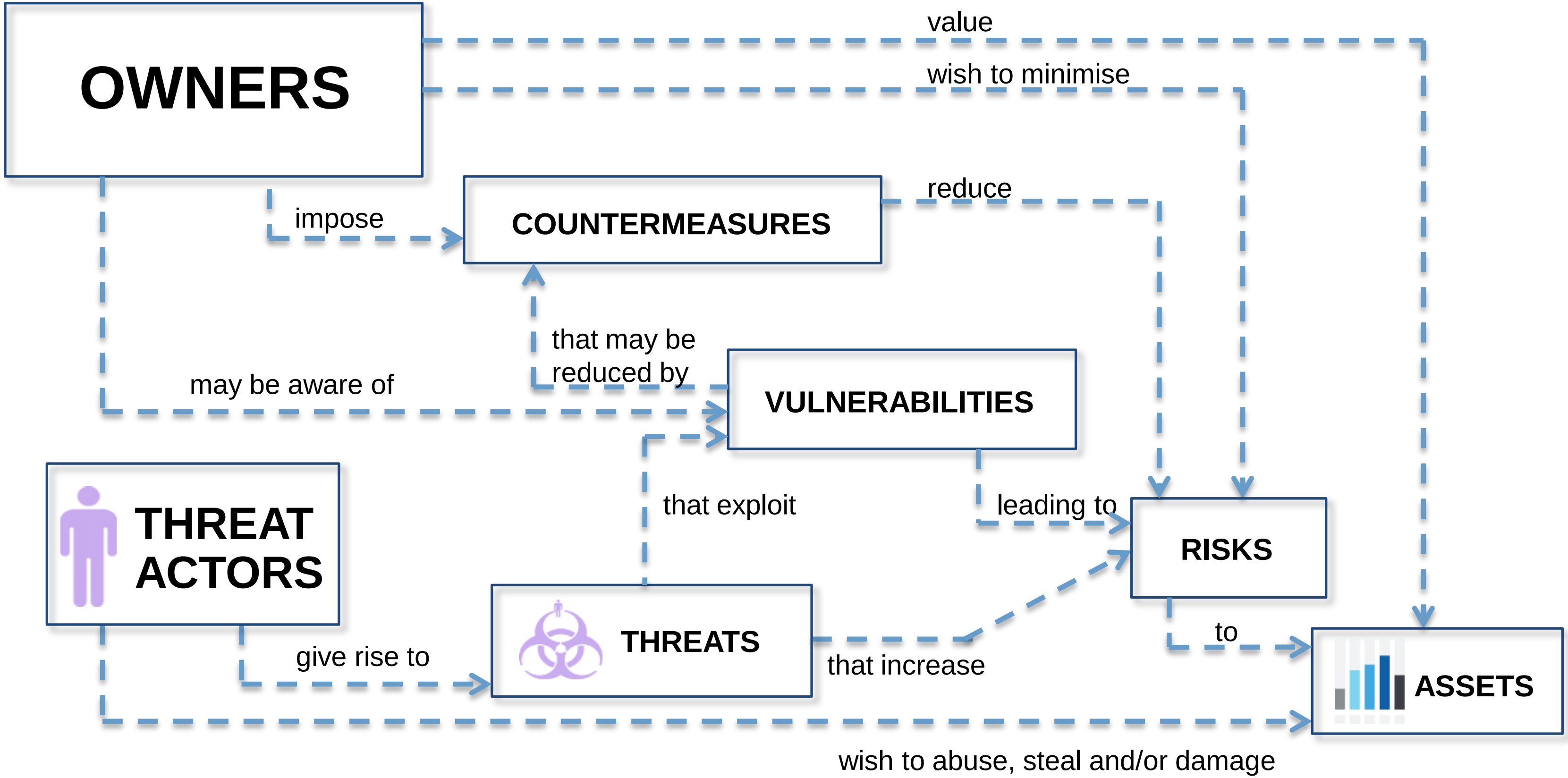


# End-user Requirements

- High TP rate / low FP rate
- Kill-chain Analysis
- Real-time Event Correlation
- Malware Analysis
- Digital Forensics
- Incident Response
- Actionable Intelligence
- Data Theft Protection



# Understand Your Environment



websense®

# Thank you…

https://twitter.com/carlLsecurity

BRAVE THE NEW WORLD.