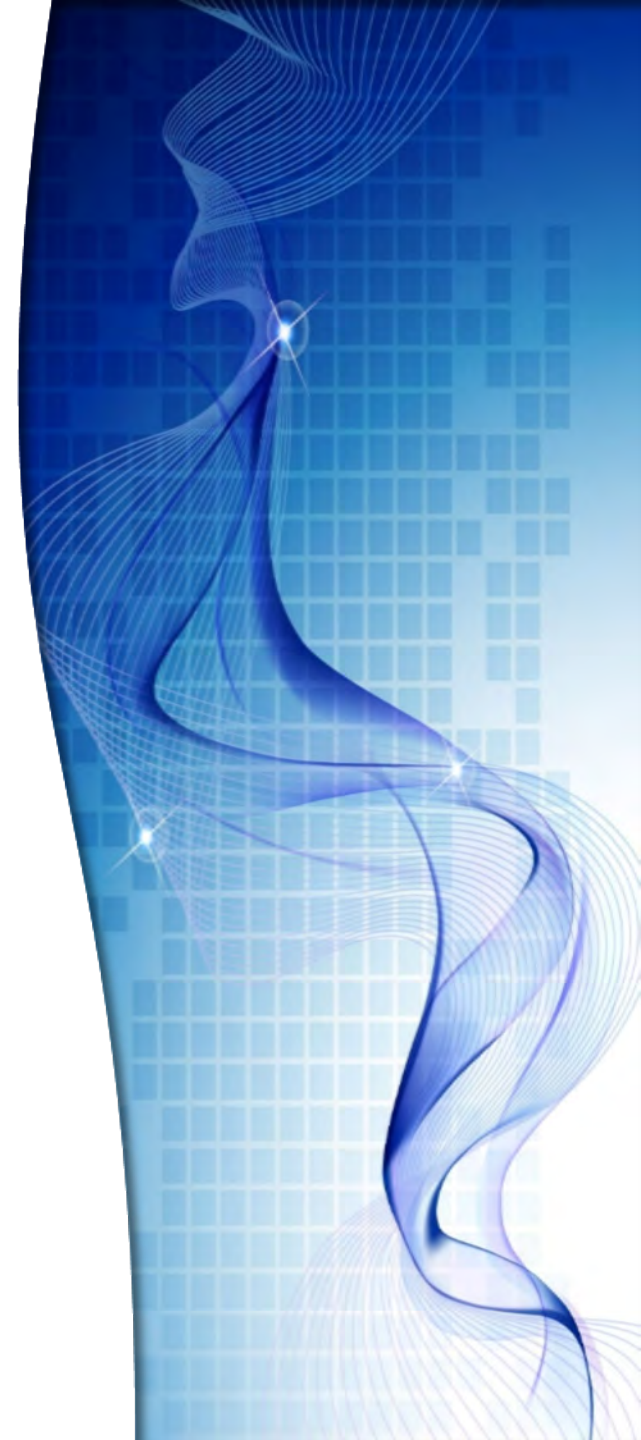


# Live Mobile Hack Demonstration (and DarkWeb ...)

**ES**<sup>2</sup>

15<sup>th</sup> November 2018



# Upcoming ES2 Events ...

## ES2 & AlienVault hosts Pre-ASIA Drinks

22<sup>nd</sup> November 2018

4:00pm – 8:00pm

The Factory,

Level 1, 69 King Street, Perth



Celebrate WA Cyberweek with ES2 & AlienVault



## ES2 People Launch

29<sup>th</sup> November 2018

5:00pm – 7:30pm

The Sherry (Upstairs), Flour Factory

16 Queen Street, Perth

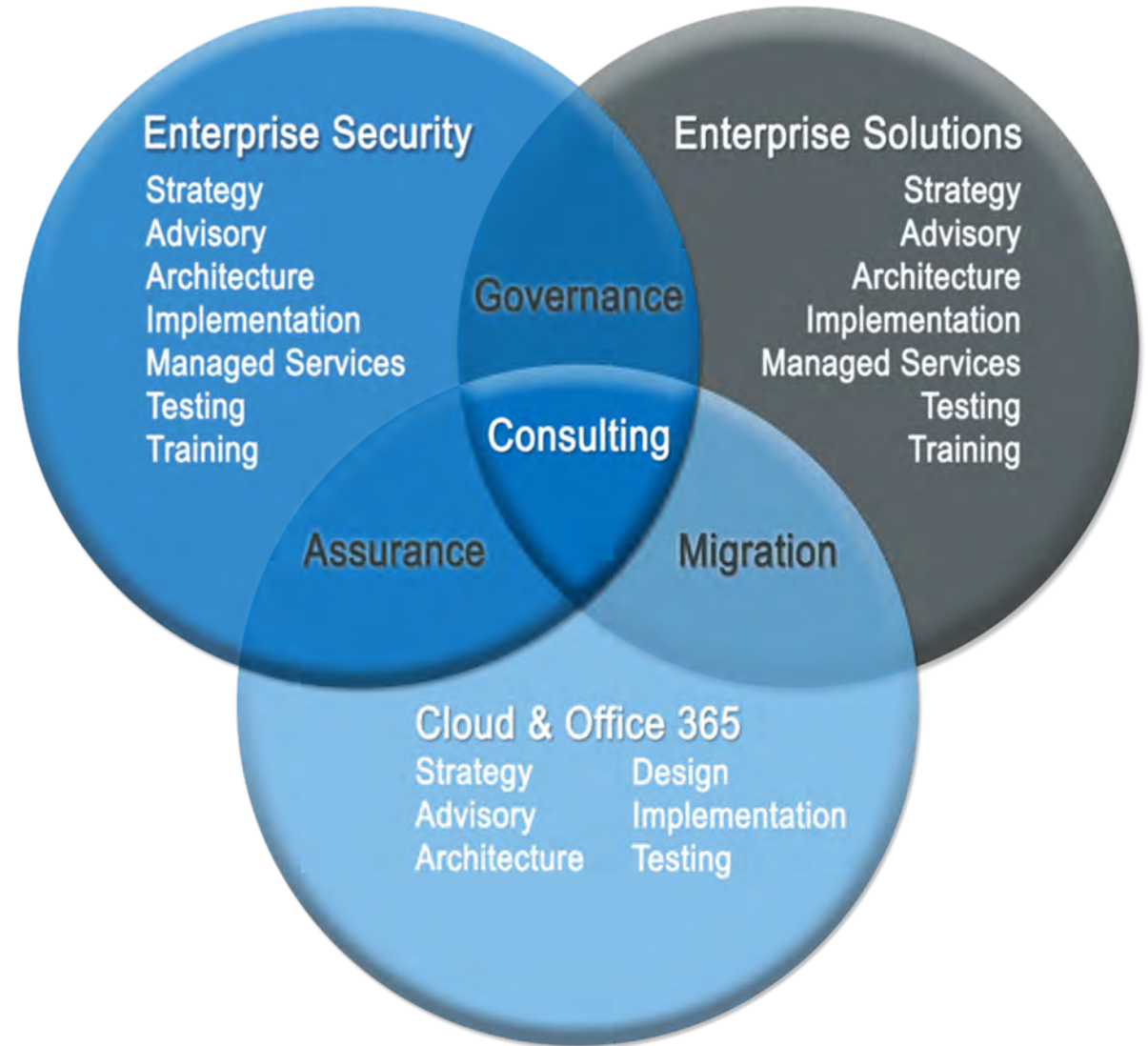


ES2 PEOPLE LAUNCH

— WE KNOW PEOPLE —

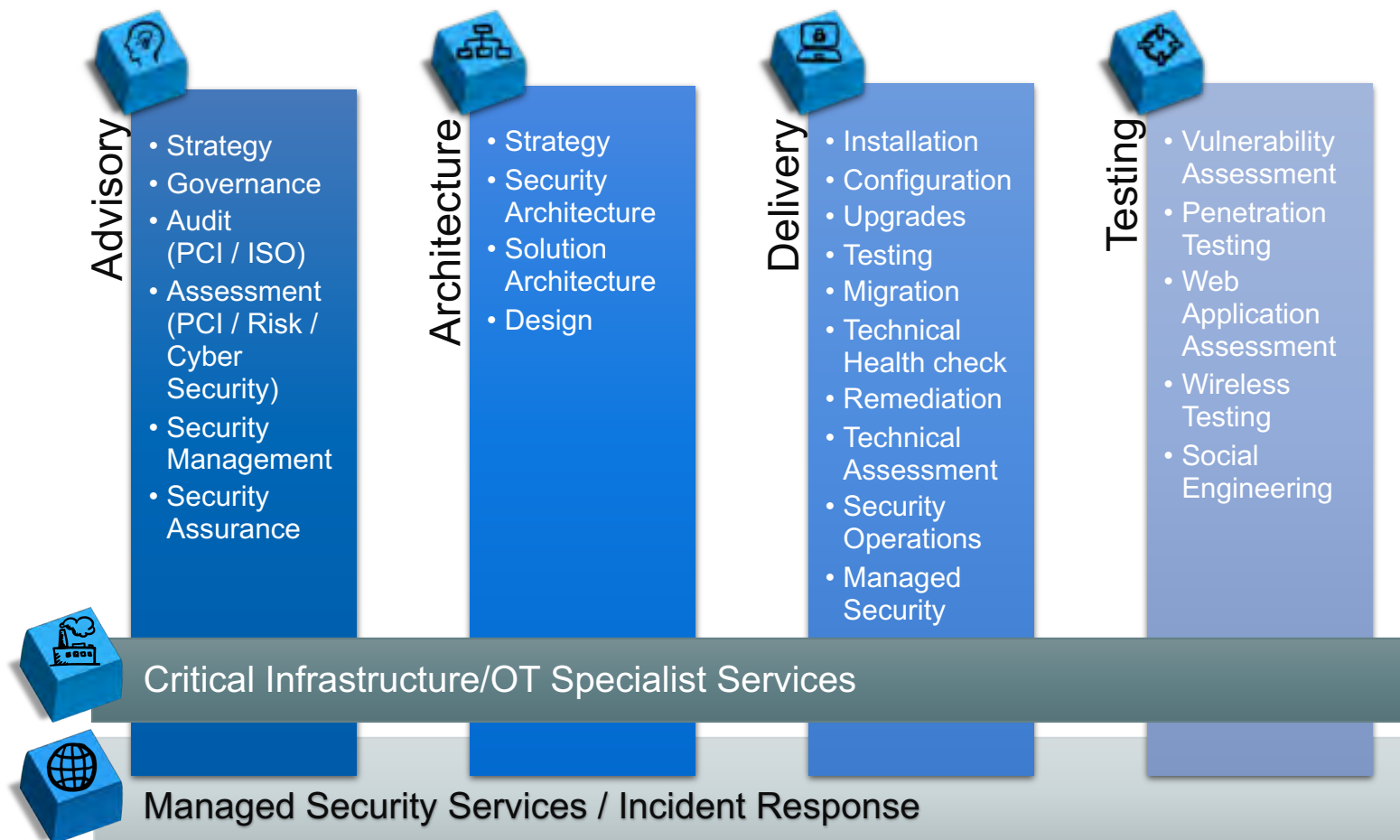
# About Us

- Enterprise Security
- Enterprise Solutions
- Training



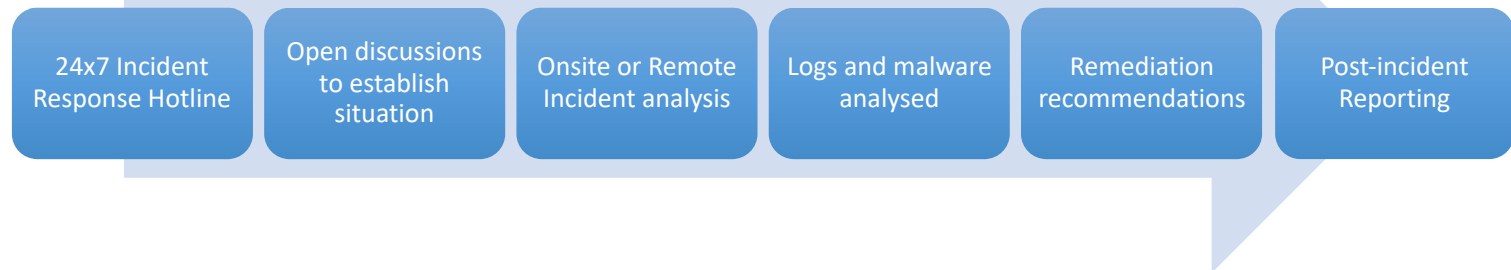
# Our Services

- Advisory
- Architecture
- Engineering
- Testing
- OT Specialists
- Managed Security Services
- Incident Response



# Knowing who to contact

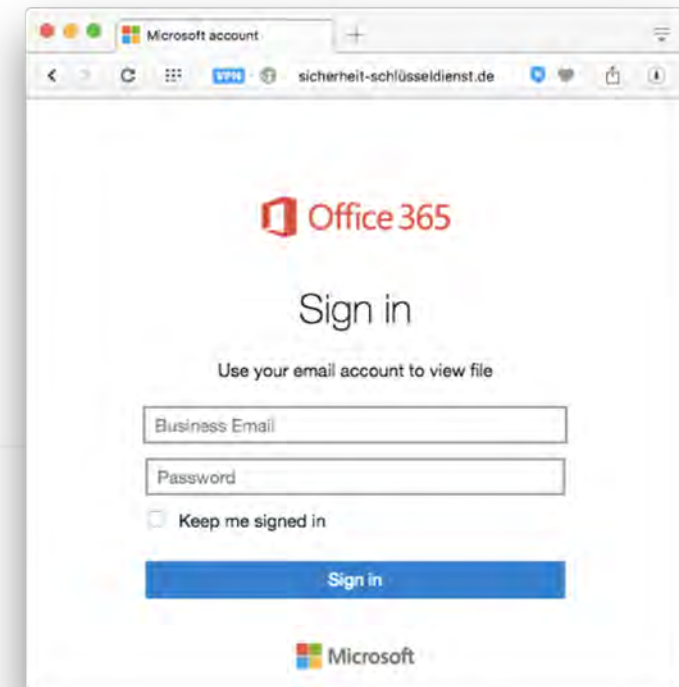
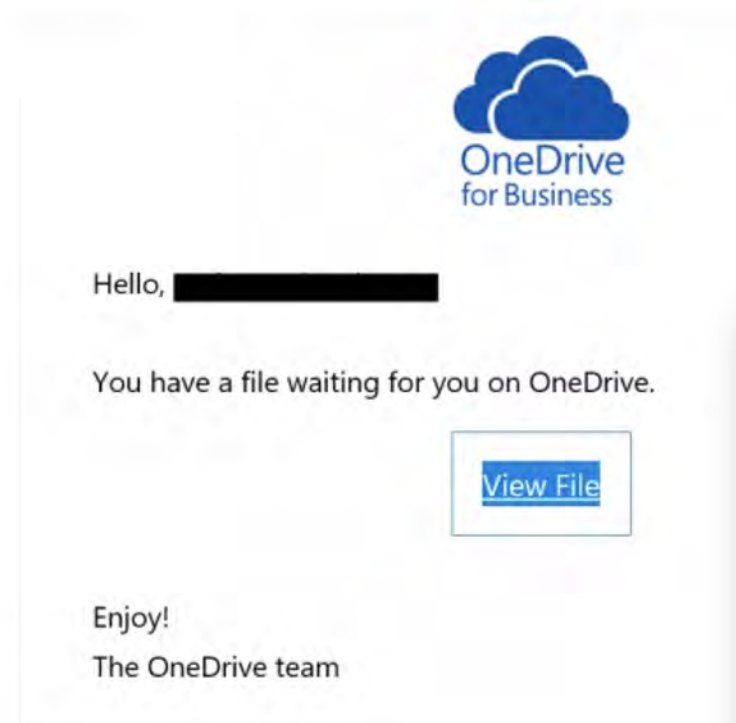
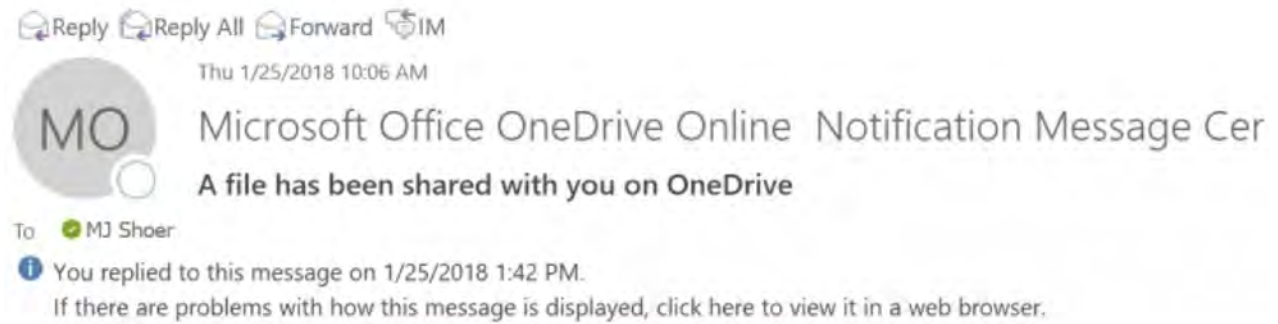
- Staff
- Clients
- Partners
- ACORN
- CERT Australia
- ES2 Incident Response
- Cyber Insurance
- Privacy Commissioner





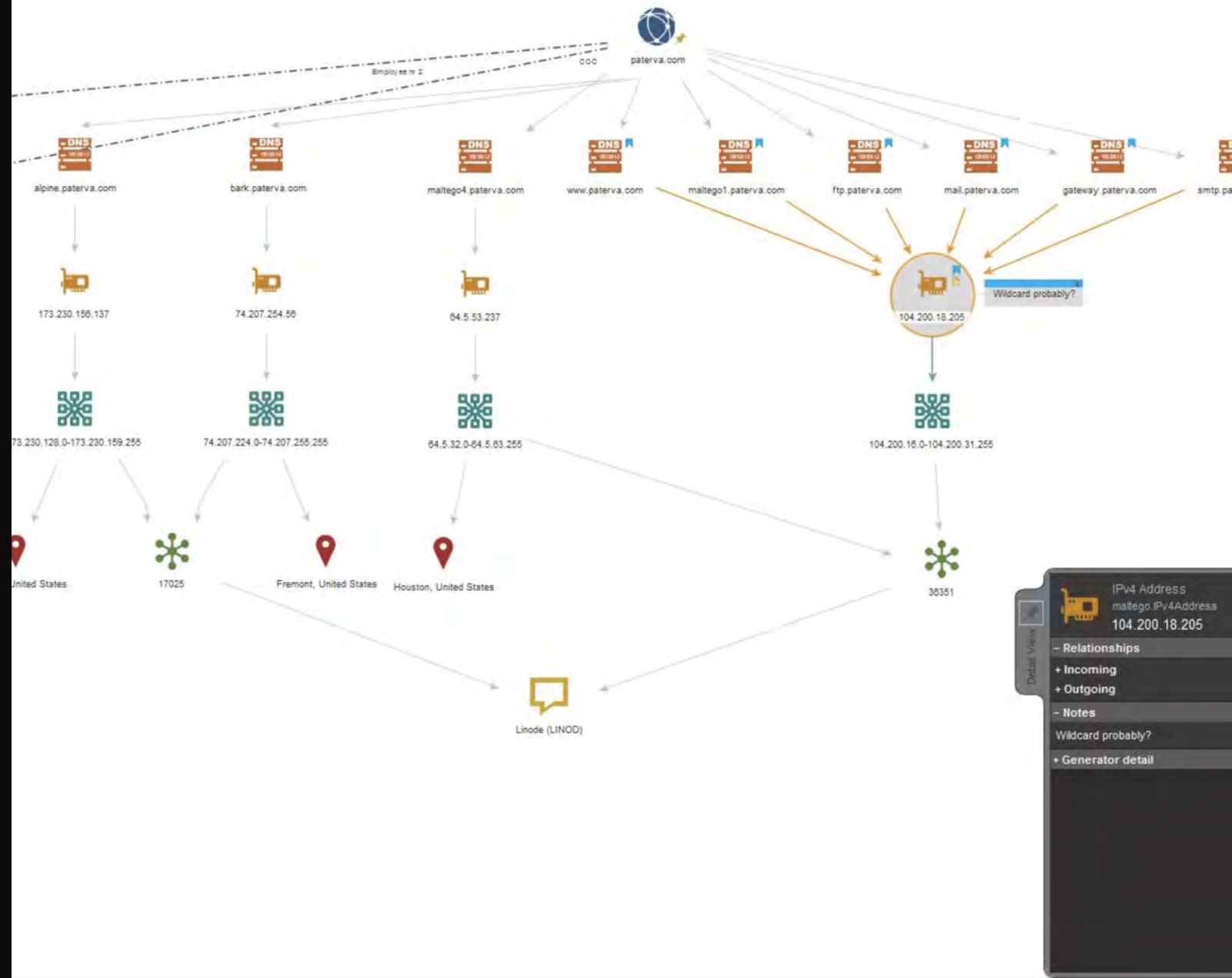
# Email Attacks

- Your password has been changed
- Unusual inbox activity, like you stop receiving email to your inbox, but can still send emails.
- You are receiving unexpected emails, that appear different to your usual junk mail
- You get people you know reaching out complaining about unusual emails or random links



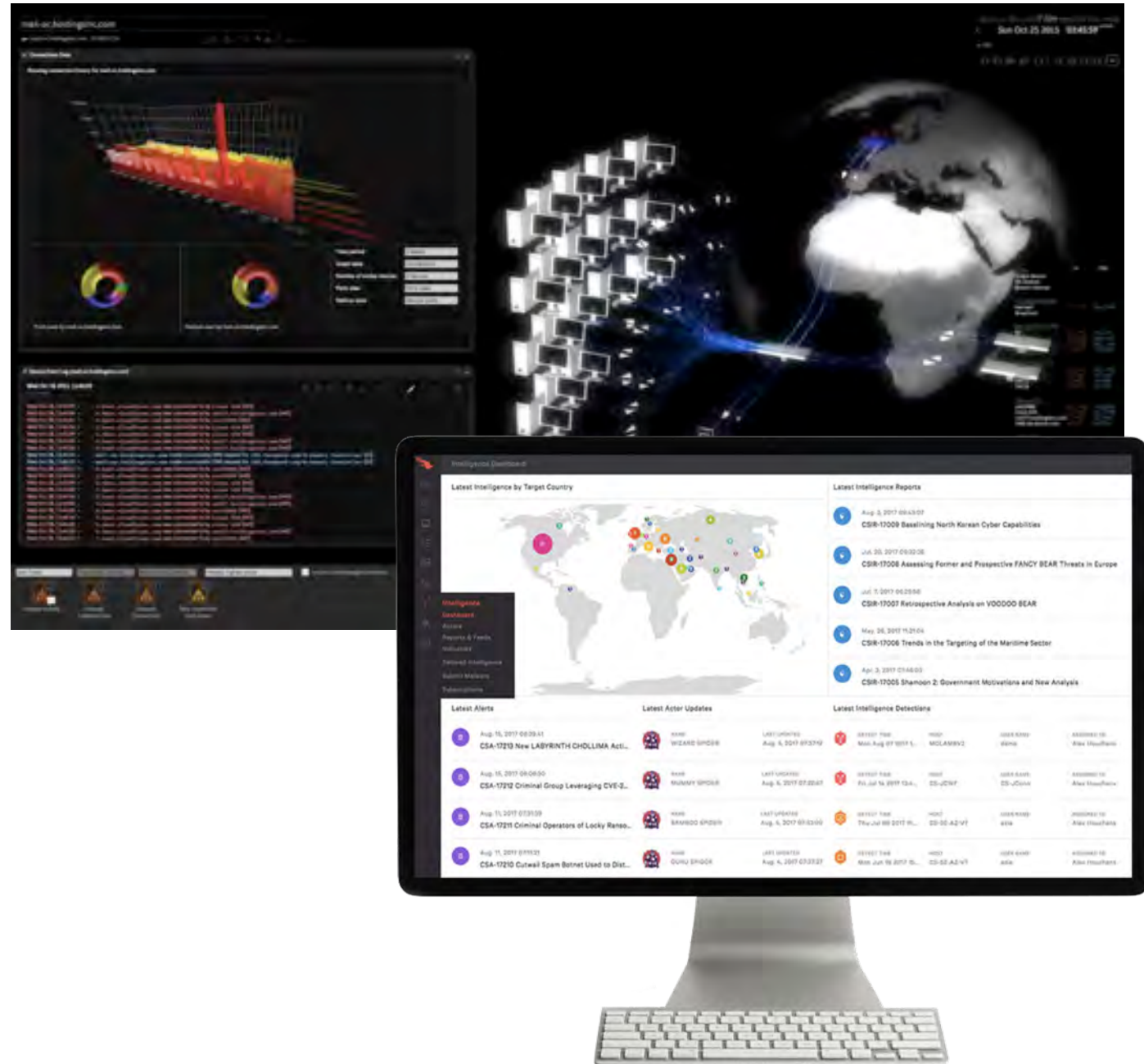
# Know your environment

- Open Source Intelligence (OSINT)
- Technical Review
- Social Engineering
- Incident Response Planning
- Incident Response Exercises
- Pre-Paid Incident Response



# Becoming the Hunter

- AI & Machine Learning
- Threat Visualization
- Breach Analytics Playback
- Real-time threat detection and autonomous response
- Endpoint Detection and Response
- Threat Intelligence
- Managed Threat Hunting





# Live Demo

- Michael Ransom (OSCP, CREST)
- Penetration Tester



# Dark Web

- Usernames/Password
- Hacked Accounts
- Remote Access
- Company Data
- Privacy Data

## THE CLEAR, DEEP & DARK WEB

### Clear Web

**4 % of WWW content**

- - Indexed by Search Engines
- - Social media



### Deep Web

**95 % of web content**

- Not searchable by most engines
- Password protected content
- Web mail, Forums, Online banking, video on demand, corporate intranets, and subscription-based online news etc.



### Dark Web

**1 % of web content**

- Not searchable by most engines
- Home to TOR, IRCs, BitTorrent, hacker forums, C2s, and more.
- *Where attacks are planned, tools purchased, information traded, and malware is developed, tested, sold and updated.*



# DARK WEB DEMO



Demonstration of using a specific browser to access dark net sites showing the lack of indexing, the need for security and then showing Credit Card information for sale on Silk Road.

# Financial Value

- Usernames/Password
- Hacked Accounts
- Remote Access
- Company Data
- Privacy Data

# \$1,200

## is all you are worth on the dark web

Hacked accounts of these popular brands and stolen personal info are for sale on the dark web. The Dark Web Market Price Index tracks their average sale price, showing fraudsters can buy up someone's entire online identity for just \$1,200.

<div>Online Shopping</div> <div><div>amazon</div><div>ebay</div><div>Costco</div><div>Walmart</div><div>macy's</div></div> <div><div>Subtotal</div><div>\$164.65</div></div>	<div>Travel</div> <div><div>UBER</div><div>Booking.com</div><div>Expedia</div><div>airbnb</div></div> <div><div>Subtotal</div><div>\$45.53</div></div>	<div>Entertainment</div> <div><div>Apple</div><div>NETFLIX</div><div>Spotify</div></div> <div><div>Subtotal</div><div>\$28.59</div></div>	
<div>Personal Finance</div> <div><div>PayPal</div><div><div><div></div></div><div><div></div></div></div></div> <div><div>Subtotal</div><div>\$710.65</div></div>	<div>Social Media</div> <div><div>facebook</div><div>Twitter</div><div>LinkedIn</div><div>Instagram</div></div> <div><div>Subtotal</div><div>\$10.21</div></div>	<div>Proof of Identity</div> <div><div><div></div><div></div></div></div> <div><div>Subtotal</div><div>\$92.20</div></div>	<div>Communication</div> <div><div>verizon</div><div>AT&amp;T</div><div>S</div><div>T-Mobile</div></div> <div><div>Subtotal</div><div>\$72.17</div></div>
<div>Delivery</div> <div><div>DHL</div><div><div>ups</div><div>FedEx</div></div></div> <div><div>Subtotal</div><div>\$15.59</div></div>	<div>Food Delivery</div> <div><div>GRUBHUB</div><div><div></div></div></div> <div><div>Subtotal</div><div>\$12.80</div></div>	<div>Email</div> <div><div>Aol.</div><div>M</div><div>Outlook</div><div>YAHOO! MAIL</div></div> <div><div>Subtotal</div><div>\$9.53</div></div>	<div>Dating</div> <div><div>match.com</div><div><div></div><div>dating.com</div></div></div> <div><div>Subtotal</div><div>\$8.82</div></div>

Source: Dark web market listings collected on 5-11 February, 2018. Markets monitored were Dream, Point and Wall Street Market. Prices collected in USD as displayed on listings.

TOPIQVPN

# Incident Avoidance

- Identify
- Protect
- Detect
- Respond
- Recover

## Top 10 Best Practice

- Cyber Security Review
- Social Engineering
- Penetration Testing
- Privacy Assessment
- Secure Code Review
- Policies
- Email Security
- Security Monitoring
- ES2 Cyber Incident Response
- Cyber Incident Response Plan





# Thank You

- Accountability
- Outcome Driven
- Trusted Advisor

