F.I.D.O.

Fully Integrated Defense Operation

Rob Fry - Sr Security Architect

NETFLIX

Agenda

- “The Human Problem”
- “The Technical Problem”
- F.I.D.O. High Level
- Correlation
- What’s Next?
- Q & A

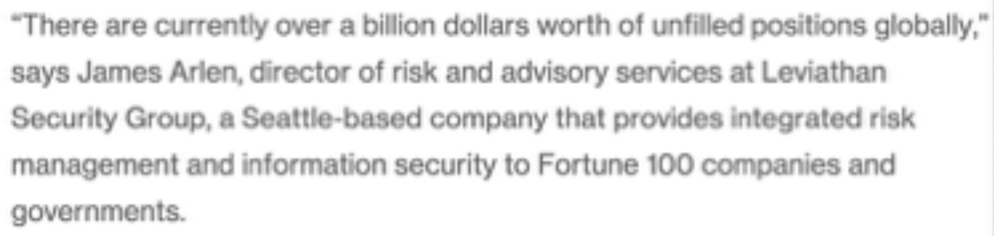
Disclaimers

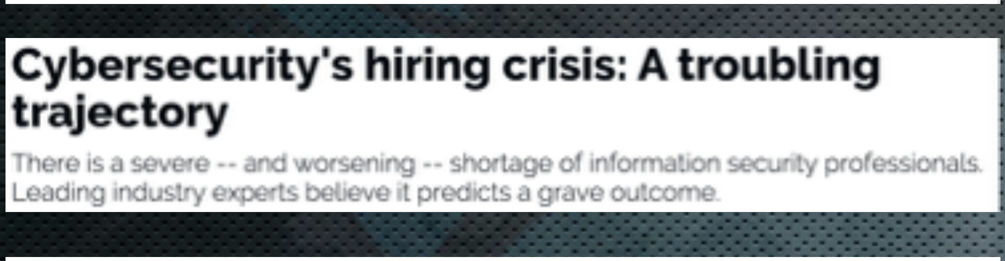
- The facts expressed here belong to everybody, the opinions to me. The distinction is yours to draw.
- Any similarity to actual companies or technology, living or dead, is purely coincidental.
- Every statement in this presentation is possibly true.
- Any disclaimer issued by me is subject to change without notice.
- Netflix's FIDO - Fully Integrated Defense Operation - is not a part of, or service of, the FIDO Alliance
- Disclaimer does not cover misuse, accident, lightning, flood, tornado, tsunami, volcanic eruption, earthquake, hurricanes, or other acts of God, neglect, damage from improper use, incorrect line voltage, unauthorized use, unauthorized repair, improper installation, typos, broken antenna or marred cabinet, missing or altered serial numbers, electromagnetic radiation from nuclear blasts, sonic boom vibrations, customer adjustments that are not covered in this list, and incidents owing to an airplane crash, ship sinking or taking on water, motor vehicle crashing, dropping the item, falling rocks, leaky roof, broken glass, disk failure, accidental file deletions, mud slides, forest fire, hitting of a deer, milk coming out of your nose due to laughing while drinking, or projectiles, which can include, but are not limited to, arrows, bullet shots, BBs, shrapnel, lasers, napalm, torpedoes, emissions of X-rays, Alpha, Beta and Gamma rays, knives, stones, etc.

NETFLIX

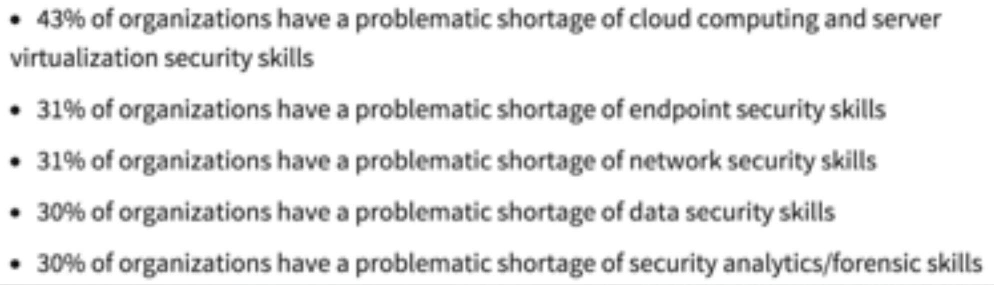
F.I.D.O.

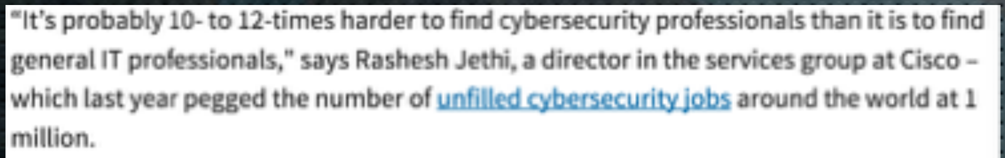
The Human Problem

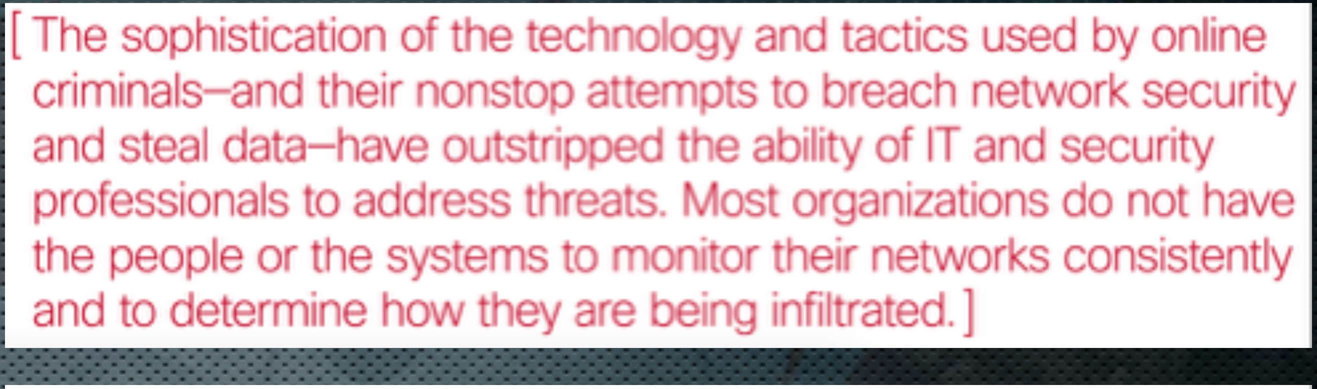

"There are currently over a billion dollars worth of unfilled positions globally," says James Arlen, director of risk and advisory services at Leviathan Security Group, a Seattle-based company that provides integrated risk management and information security to Fortune 100 companies and governments.

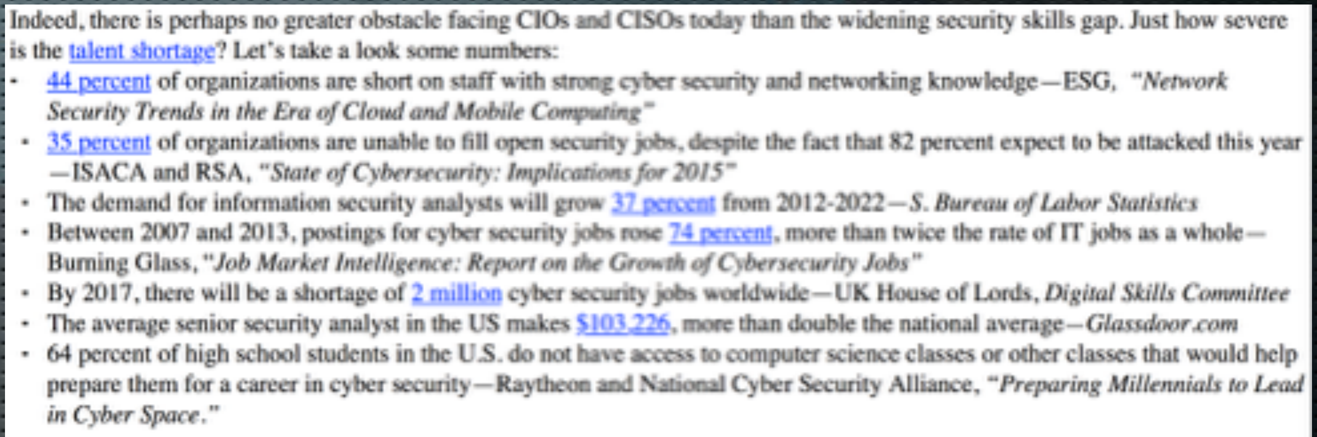

Cybersecurity's hiring crisis: A troubling trajectory

There is a severe -- and worsening -- shortage of information security professionals. Leading industry experts believe it predicts a grave outcome.


- 43% of organizations have a problematic shortage of cloud computing and server virtualization security skills
- 31% of organizations have a problematic shortage of endpoint security skills
- 31% of organizations have a problematic shortage of network security skills
- 30% of organizations have a problematic shortage of data security skills
- 30% of organizations have a problematic shortage of security analytics/forensic skills


"It's probably 10- to 12-times harder to find cybersecurity professionals than it is to find general IT professionals," says Rashesh Jethi, a director in the services group at Cisco – which last year pegged the number of unfilled cybersecurity jobs around the world at 1 million.


[The sophistication of the technology and tactics used by online criminals–and their nonstop attempts to breach network security and steal data–have outstripped the ability of IT and security professionals to address threats. Most organizations do not have the people or the systems to monitor their networks consistently and to determine how they are being infiltrated.]


Indeed, there is perhaps no greater obstacle facing CIOs and CISOs today than the widening security skills gap. Just how severe is the talent shortage? Let's take a look some numbers:

- 44 percent of organizations are short on staff with strong cyber security and networking knowledge—ESG, *"Network Security Trends in the Era of Cloud and Mobile Computing"*
- 35 percent of organizations are unable to fill open security jobs, despite the fact that 82 percent expect to be attacked this year —ISACA and RSA, *"State of Cybersecurity: Implications for 2015"*
- The demand for information security analysts will grow 37 percent from 2012-2022—*S. Bureau of Labor Statistics*
- Between 2007 and 2013, postings for cyber security jobs rose 74 percent, more than twice the rate of IT jobs as a whole—Burning Glass, *"Job Market Intelligence: Report on the Growth of Cybersecurity Jobs"*
- By 2017, there will be a shortage of 2 million cyber security jobs worldwide—UK House of Lords, *Digital Skills Committee*
- The average senior security analyst in the US makes $103,226, more than double the national average—*Glassdoor.com*
- 64 percent of high school students in the U.S. do not have access to computer science classes or other classes that would help prepare them for a career in cyber security—Raytheon and National Cyber Security Alliance, *"Preparing Millennials to Lead in Cyber Space."*

Source: Cisco 2014 ASR, Network World, ISAC, swimlane.com, Security Week

The Human Problem

- Vendors and organizations are not doing enough to lower the bar
- 62% of organizations have not increased security training
- 83% of enterprises lack the resources or skills to protect assets
- Majority of the work is done manually… self-defeating
- Response time windows are too high
- Enforcement, mitigation is largely manual

NETFLIX

F.I.D.O.

The Technical Problem

Too Many Alerts, Too Little Time/Resources

Network defenders are overwhelmed by the volume of security alerts

- Typical Fortune 1000 organization experiences thousands of new security events everyday[1]
- Data review is time consuming

Current industry best practices rely on analysts using SIEM technologies + manual use of threat intel feeds

- Too many false positives
- Very little guidance on how to filter the signal from the noise

Source: (1) IBM 2014 Cyber Security Intelligence Index

NETFLIX

The Technical Problem

“There are 400 alerts in my SIEM, and I have time/resources to investigate 10. Which 10 do I choose?” (1)

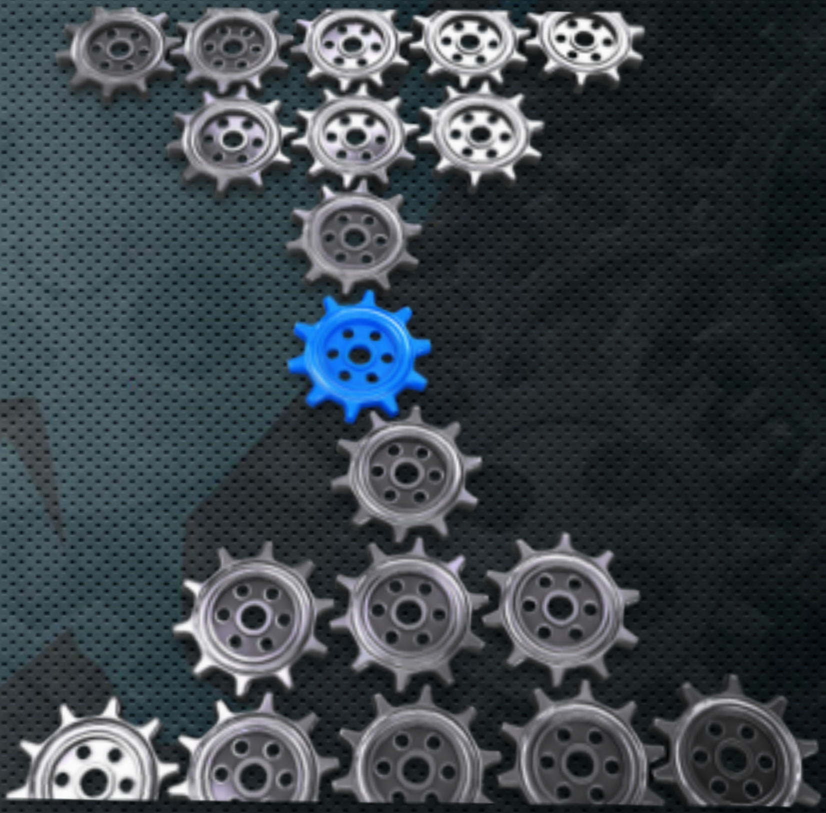
Source: (1) CISO from Fortune 200 Company

The Technical Problem

But... it Works in the Movies

F.I.D.O. = Orchestration

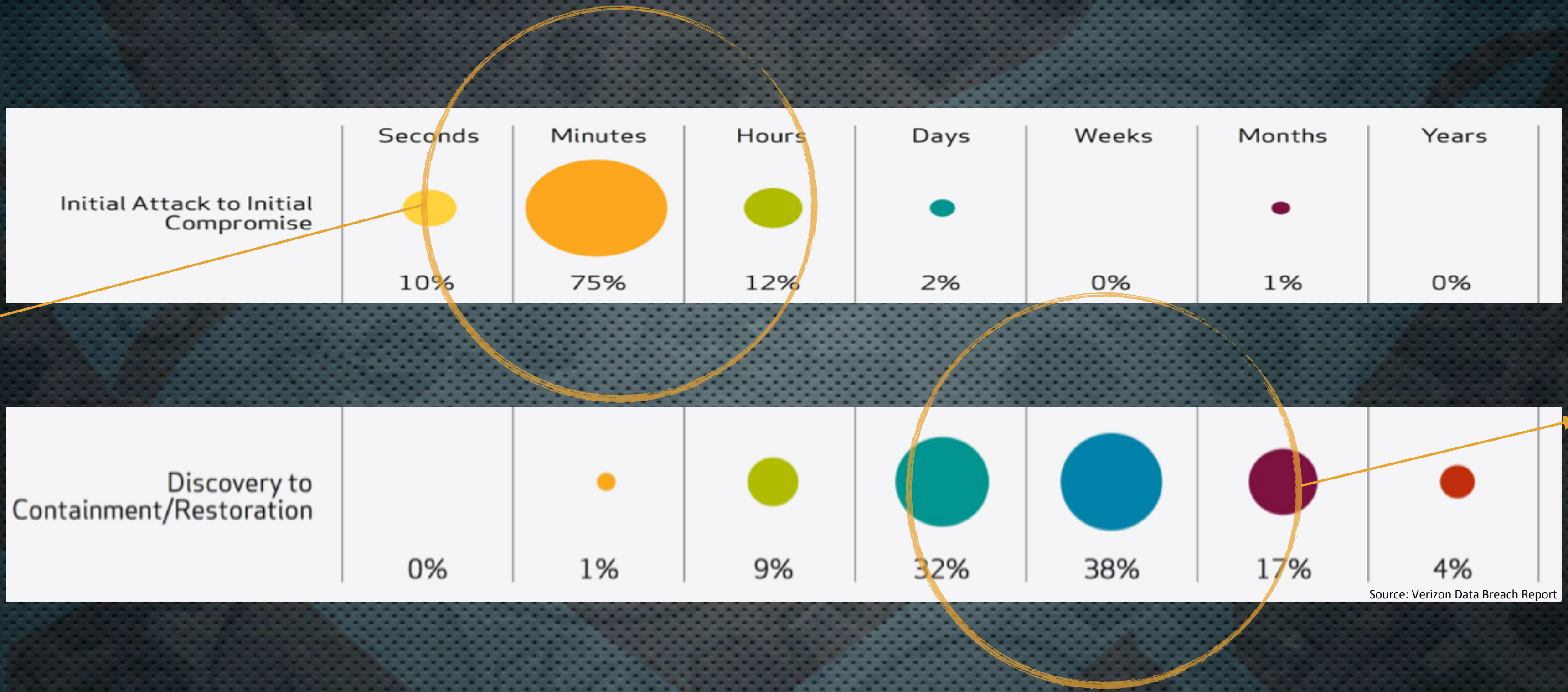
- The work of a human, but at machine speed
- Data enrichment
- Get more out of security investment
- Adds consistency
- Filter out false positives
- Threat, user, machine and asset scoring



F.I.D.O. = Orchestration

Reduce Response Time

Attackers Ability

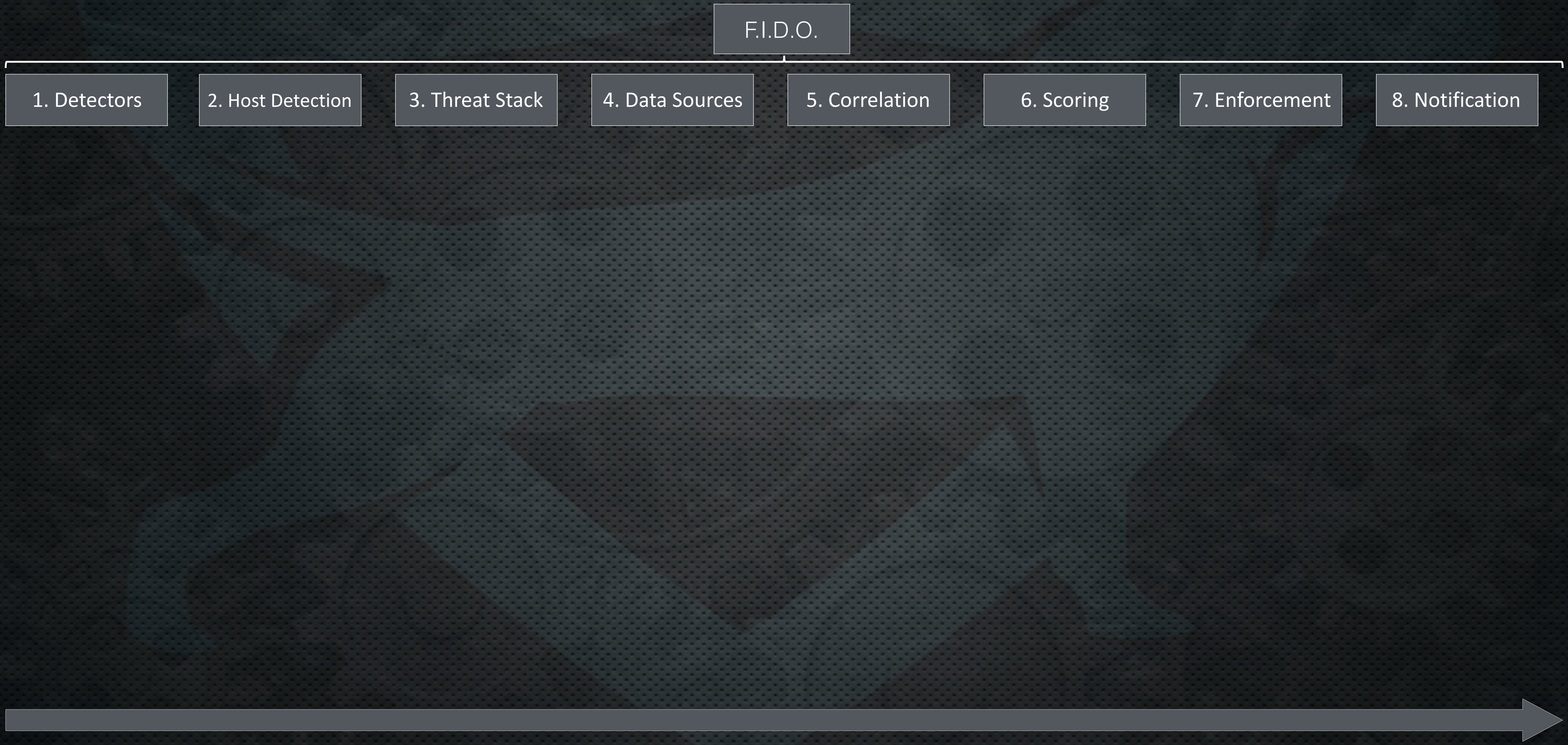


	Seconds	Minutes	Hours	Days	Weeks	Months	Years
Initial Attack to Initial Compromise	10%	75%	12%	2%	0%	1%	0%
Discovery to Containment/Restoration	0%	1%	9%	32%	38%	17%	4%

Source: Verizon Data Breach Report

Defenders Ability

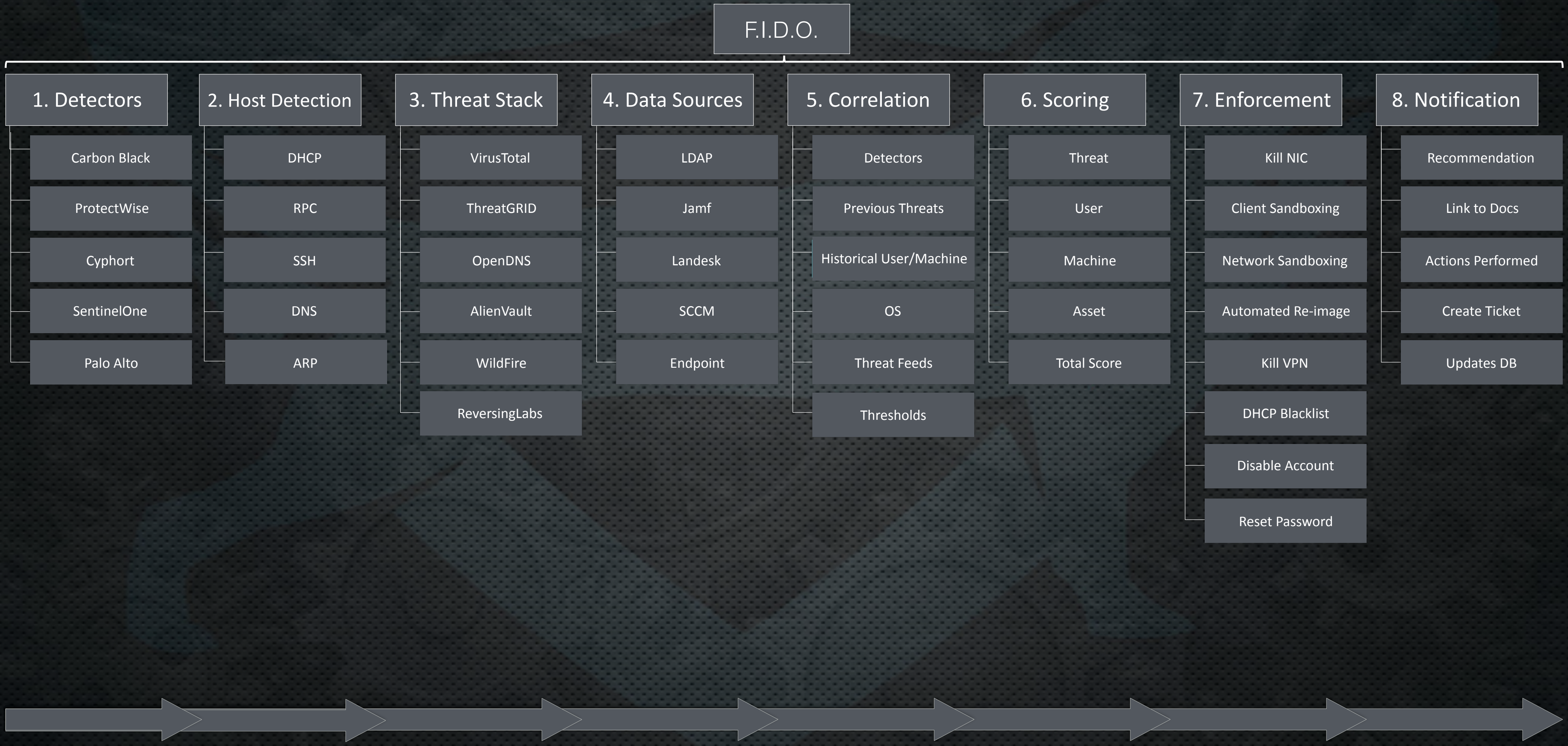
F.I.D.O. High Level



F.I.D.O.

1. Detectors
2. Host Detection
3. Threat Stack
4. Data Sources
5. Correlation
6. Scoring
7. Enforcement
8. Notification

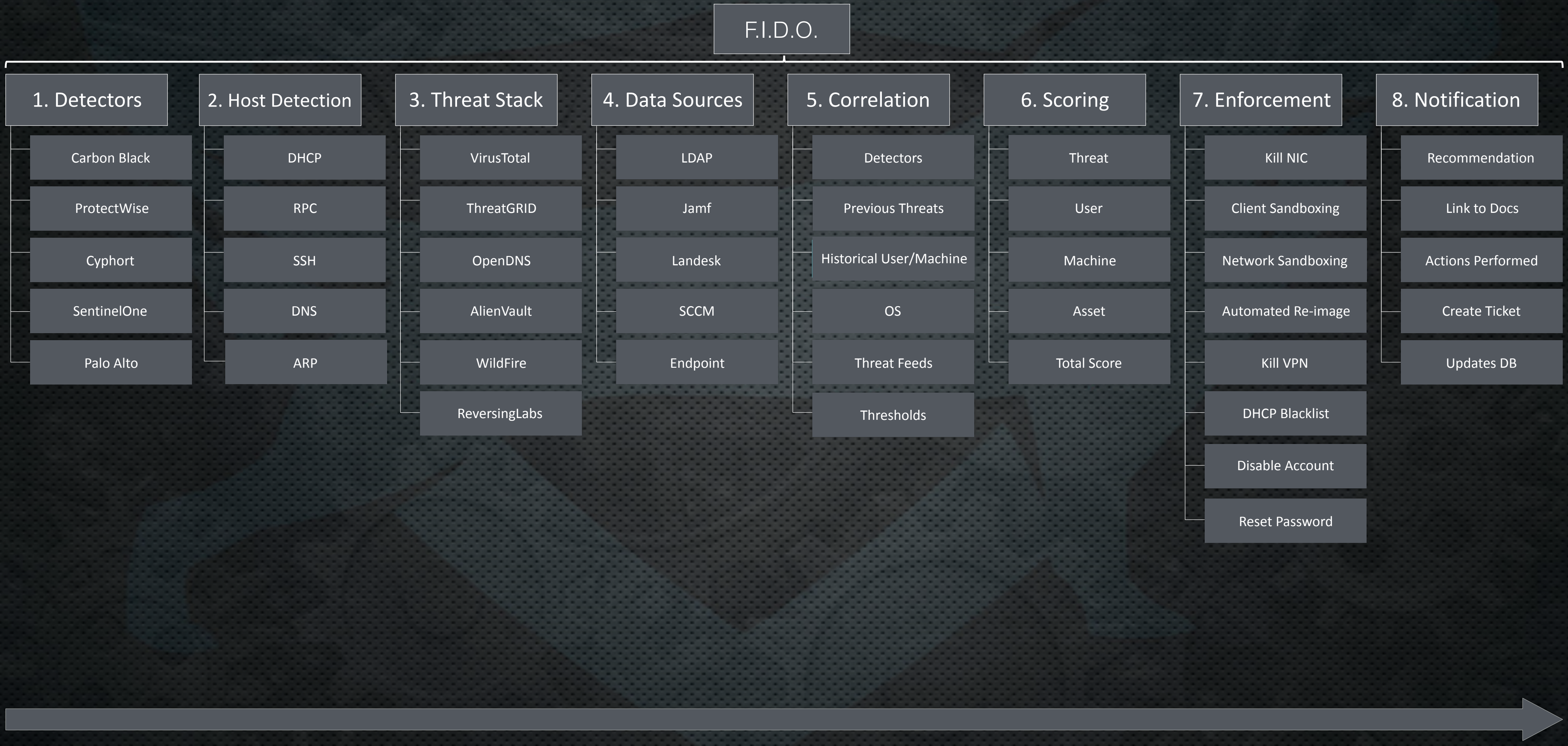
F.I.D.O. High Level



F.I.D.O.

1. Detectors
   - Carbon Black
   - ProtectWise
   - Cyphort
   - SentinelOne
   - Palo Alto
2. Host Detection
   - DHCP
   - RPC
   - SSH
   - DNS
   - ARP
3. Threat Stack
   - VirusTotal
   - ThreatGRID
   - OpenDNS
   - AlienVault
   - WildFire
   - ReversingLabs
4. Data Sources
   - LDAP
   - Jamf
   - Landesk
   - SCCM
   - Endpoint
5. Correlation
   - Detectors
   - Previous Threats
   - Historical User/Machine
   - OS
   - Threat Feeds
   - Thresholds
6. Scoring
   - Threat
   - User
   - Machine
   - Asset
   - Total Score
7. Enforcement
   - Kill NIC
   - Client Sandboxing
   - Network Sandboxing
   - Automated Re-image
   - Kill VPN
   - DHCP Blacklist
   - Disable Account
   - Reset Password
8. Notification
   - Recommendation
   - Link to Docs
   - Actions Performed
   - Create Ticket
   - Updates DB

F.I.D.O. High Level



- F.I.D.O.
  - 1. Detectors
    - Carbon Black
    - ProtectWise
    - Cyphort
    - SentinelOne
    - Palo Alto
  - 2. Host Detection
    - DHCP
    - RPC
    - SSH
    - DNS
    - ARP
  - 3. Threat Stack
    - VirusTotal
    - ThreatGRID
    - OpenDNS
    - AlienVault
    - WildFire
    - ReversingLabs
  - 4. Data Sources
    - LDAP
    - Jamf
    - Landesk
    - SCCM
    - Endpoint
  - 5. Correlation
    - Detectors
    - Previous Threats
    - Historical User/Machine
    - OS
    - Threat Feeds
    - Thresholds
  - 6. Scoring
    - Threat
    - User
    - Machine
    - Asset
    - Total Score
  - 7. Enforcement
    - Kill NIC
    - Client Sandboxing
    - Network Sandboxing
    - Automated Re-image
    - Kill VPN
    - DHCP Blacklist
    - Disable Account
    - Reset Password
  - 8. Notification
    - Recommendation
    - Link to Docs
    - Actions Performed
    - Create Ticket
    - Updates DB

F.I.D.O. High Level

Success?

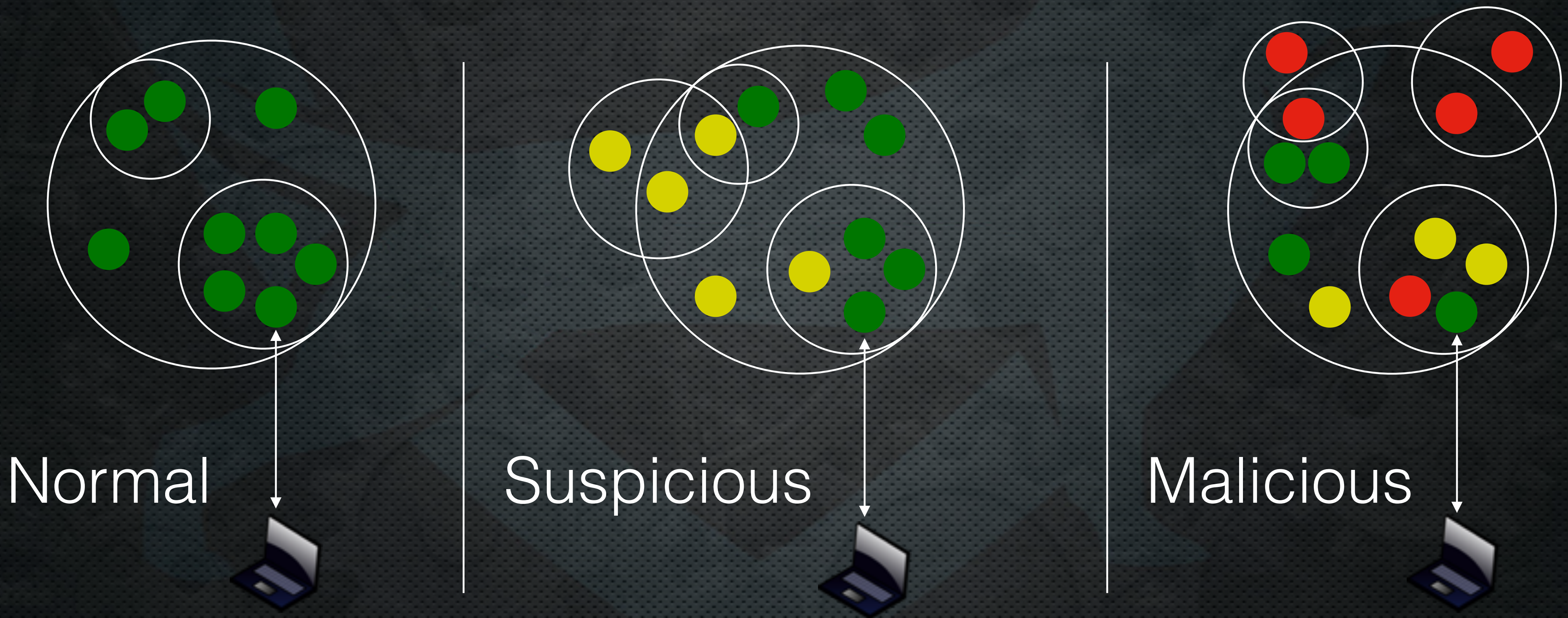
Pre-F.I.D.O.	Post-F.I.D.O.
1. Response measured in days to week	1. Response measures less than an hour
2. Aggregation of data took hours	2. Aggregation of data takes minutes
3. 80% of alerts not processed	3. All alerts processed
4. Minimal endpoint/user information	4. Detailed endpoint/user information
5. Little or no scoring information	5. Detailed scoring information

Correlation

- F.I.D.O. is not ML, but we are working on it
- ML for scoring first
- ML for security is hard
- Correlation can be repeatable
- Correlation is what we do… codify it

Correlation Simple Example

Patterns in the data



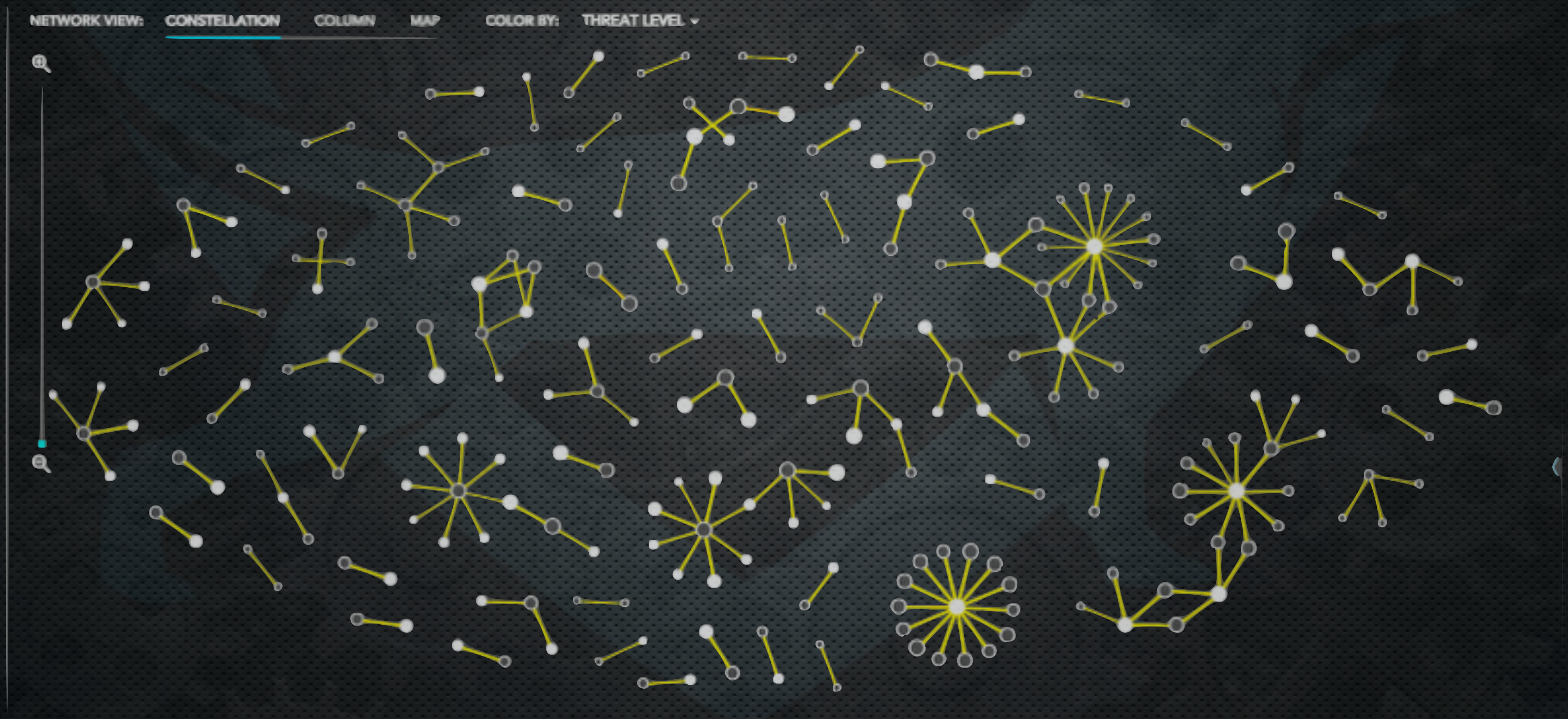
Normal

Suspicious

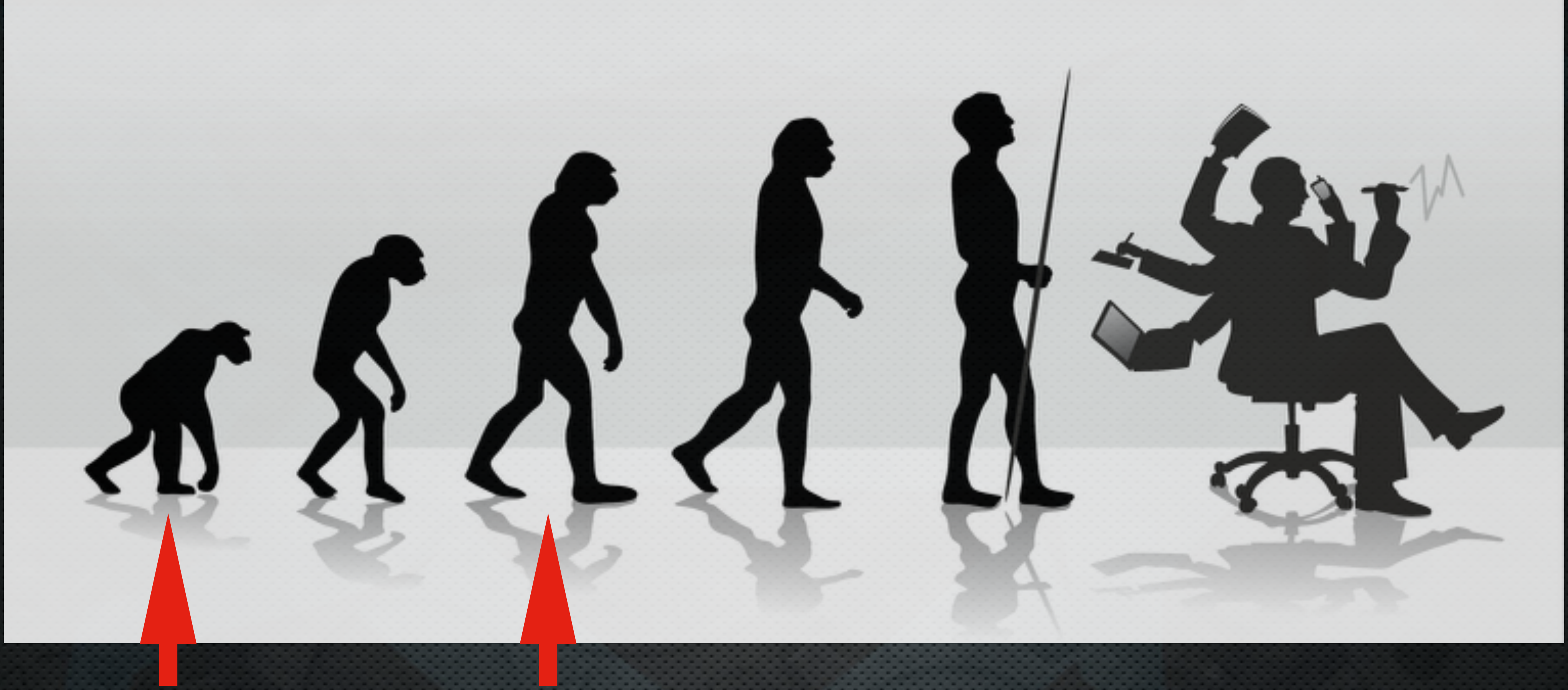
Malicious

Correlation Initiatives

Patterns in the data



Evolution of Correlation



Although somedays I feel like it's here.

F.I.D.O. is probably here.

Correlation Initiatives

Too much opportunity

especially for one person.

- More data, more data points
- Move past 300 vectors
    - More indicators
    - Move laterally across data (detector, threat feed, whatever)
    - Drill in multiple layers deep
- Better data enrichment algorithms for higher quality associations
- Independent processes for correlation (parallelism, retrospection)
- Continue to evaluate ML for correlation

What’s Next?

Still too much opportunity

especially for one person.

What's Next?

Still too much opportunity

especially for one person.

- Go from prototype to full stack
- More contributors, more partnerships
- Tighter integrations
- Web UI
- ML for scoring
- More telemetry

Q&A

- Questions?
- Thank you!
- rob.fry@netflix.com