ISE® WEST EXECUTIVE FORUM

Nominee Showcase Presentation

Netflix

F.I.D.O.: Building Defense on the Inside

Rob Fry

Sr Security Architect

Company Overview

Netflix is the world's leading Internet television network with over 65 million members in over 50 countries enjoying more than 100 million hours of TV shows and movies per day, including original series, documentaries and feature films. Members can watch as much as they want, anytime, anywhere, on nearly any Internet-connected screen. Members can play, pause and resume watching, all without commercials or commitments.

- Subscribers watch 10 billion hours per month
- Library consumes 'well over' a petabyte
- Service uses 37% of Internet traffic (during peak hours)
- By 2017 Netflix will be global servicing 200+ countries

Presentation Overview

- Defining the Problem
- Orchestration and Automation
- F.I.D.O. High-level
- Success & Lessons Learned

Why Create F.I.D.O.?

Verizon Data Breach Report 2014 reveals failings not only in the organization's ability to detect an attack, but also in their ability to quickly respond and efficiently shut it down.

Attackers's Ability

Defender's Ability

Source: Verizon Data Breach Report

Current Approaches Are Failing

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 + threat intel feeds

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

"There are 400 alerts in my SIEM, and I have time/resources to investigate 10. Which 10 should I choose?" (2)

Source: (1) IBM 2014 Cyber Security Intelligence Index, (2) CISO from Fortune 200 Company

Hiring Availability –vs– Company Culture

Hard Work – Not Relevant

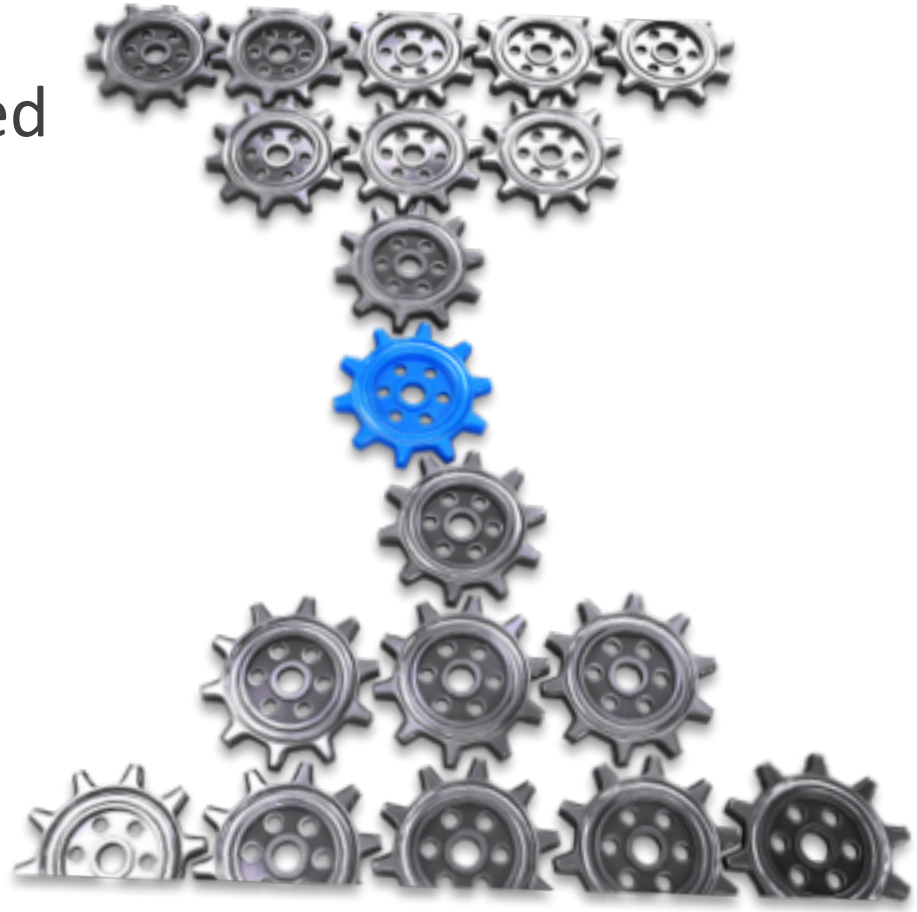
- We don't measure people by how many hours they work or how much they are in the office
- We do care about accomplishing great work
- Sustained B-level performance, despite "A for effort", generates a generous severance package, with respect
- Sustained A-level performance, despite minimal effort, is rewarded with more responsibility and great pay

NETFLIX

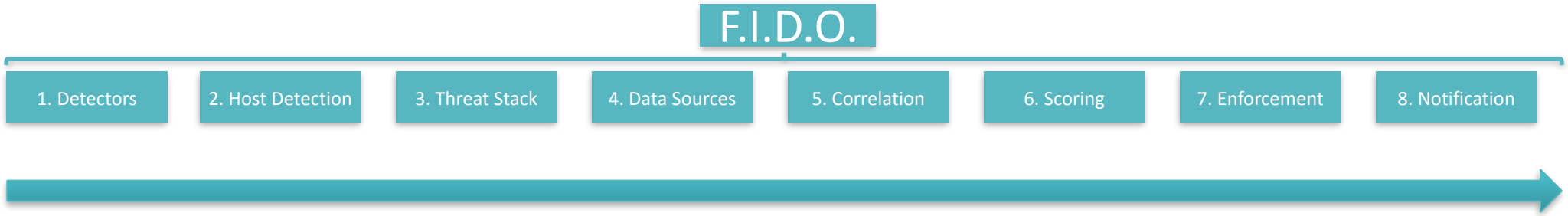
34

F.I.D.O. = Orchestration

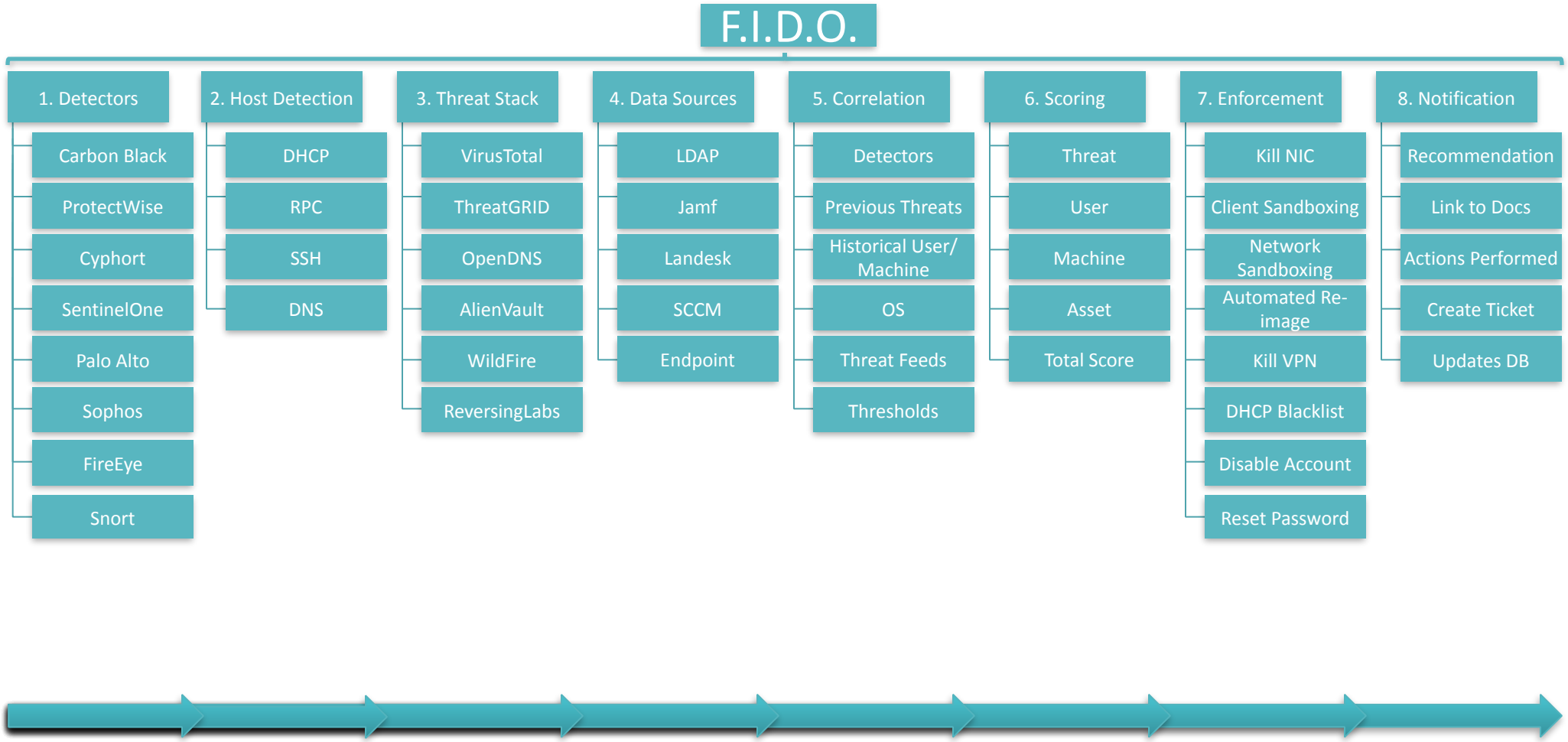
- The work of a human, but at machine speed
- Get more out of security investment
- Adds consistency
- Filter out false-positives
- Threat, user, machine and asset scoring



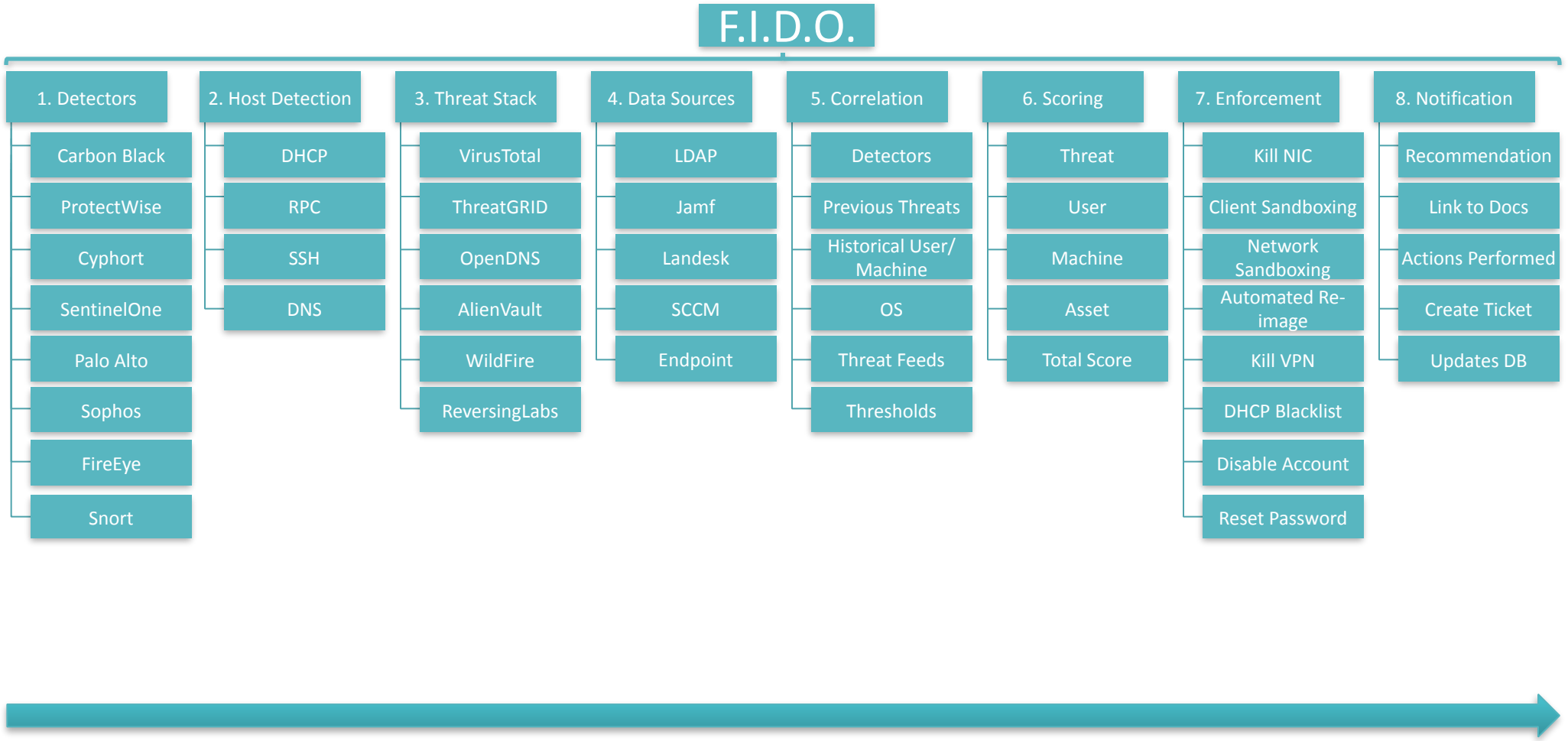
F.I.D.O. High-level



F.I.D.O. High-level



F.I.D.O. High-level



Scoring Matrix

Threat Score	=	(Silo 1 * Silo Weight %) + (Silo 2 * Silo Weight %) + (Silo 3 * Silo Weight %) + (Silo 4 * Silo Weight %)
Machine Score	=	(Silo 3 * Silo Weight %) + (Silo 4 * Silo Weight %) + (Silo 5 * Silo Weight %) + (Silo 7 * Silo Weight %)
User Score	=	(Silo 3 * Silo Weight %) + (Silo 4 * Silo Weight %) + (Silo 6 * Silo Weight %) + (Silo 7 * Silo Weight %)
Total Score	=	Threat Score + Machine Score + User Score

F.I.D.O. Success?

Pre-F.I.D.O.	Post-F.I.D.O.
1. Response measured in days to a week	1. Response measured 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

F.I.D.O. Lessons Learned

- “Do more, with less” or “Do more, with more”
- The threshold of ideas has been breached
- Moves security to a DevOps model
- Reciprocal value in vendor quality

Thank you and Questions

Questions?