RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Malware Defense and Automation: Fully Integrated Defense Operation (F.I.D.O.)

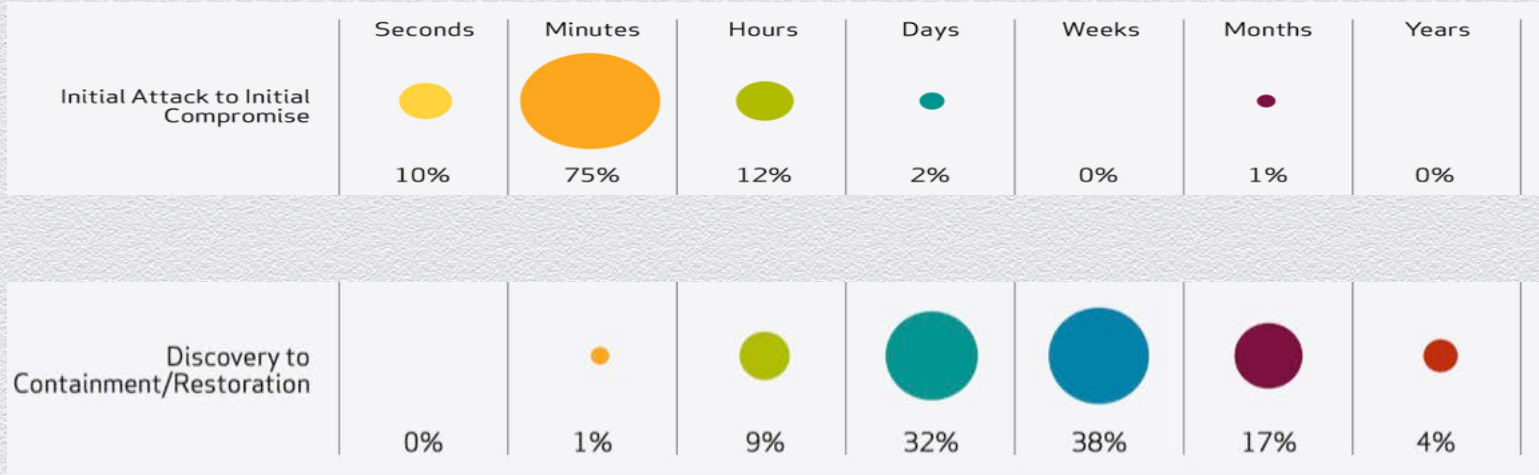
SESSION ID: TECH-F03A

Rob Fry

Sr Information Security Architect
Netflix

Why Create F.I.D.O.?

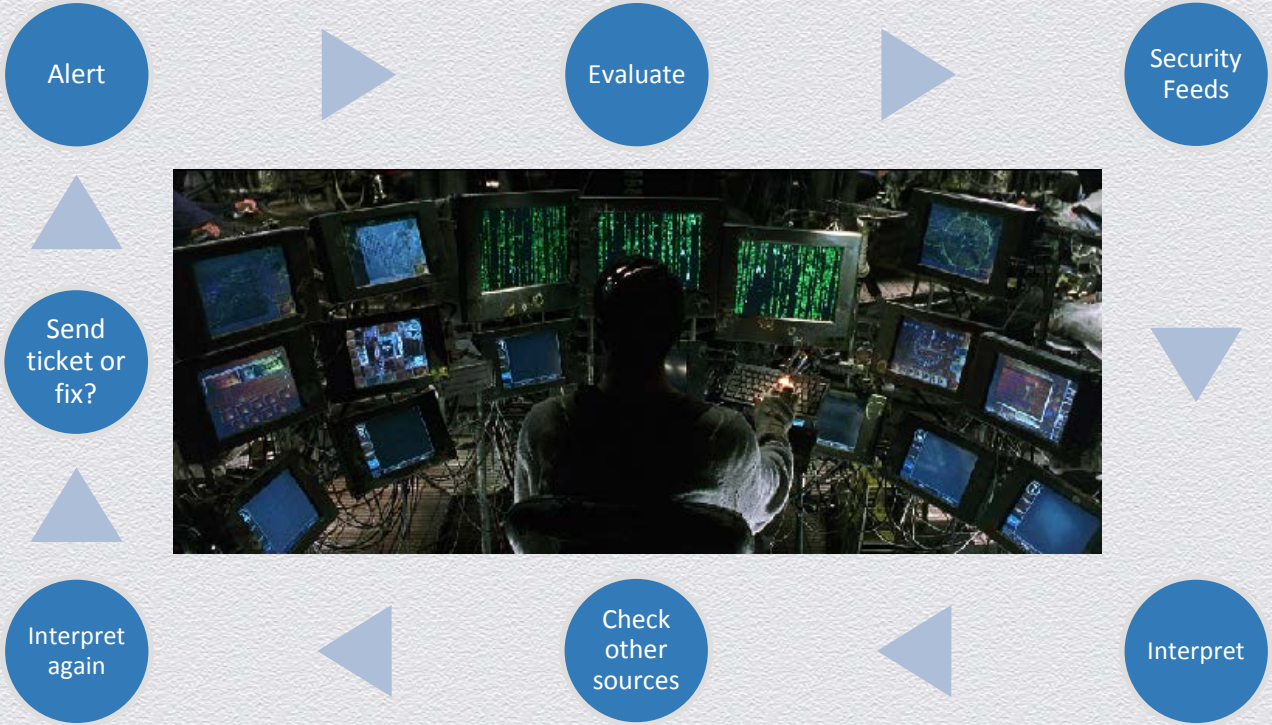
Reduce Response Time



*source: Verizon 2012 Data Breach Investigations Report

NETFLIX

What is your workflow?



NETFLIX

Flaws with Current Detection and Remediation:

- Lack of vision
- Integration inadequacy
- Decentralized
- Analytic shortcomings
- Differing formats & alerting
- Security systems are proprietary
- Slow or disjointed response
- Little to no automation

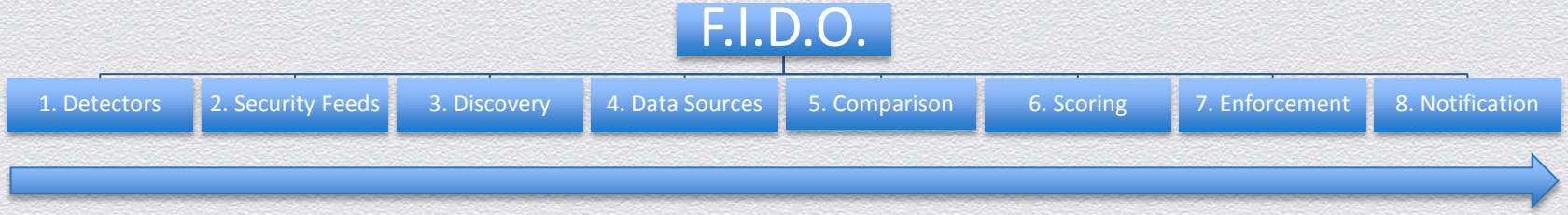
NETFLIX

F.I.D.O. Orchestration:

- Cross-reference with the other internal systems
- Normalize data and alerts
- Trust nothing, evaluate and validate everything
- Event correlation
- Automate the evaluation and deliver an effective response
- Centralize communications and interactions
- Partner with vendors for APIs & integration

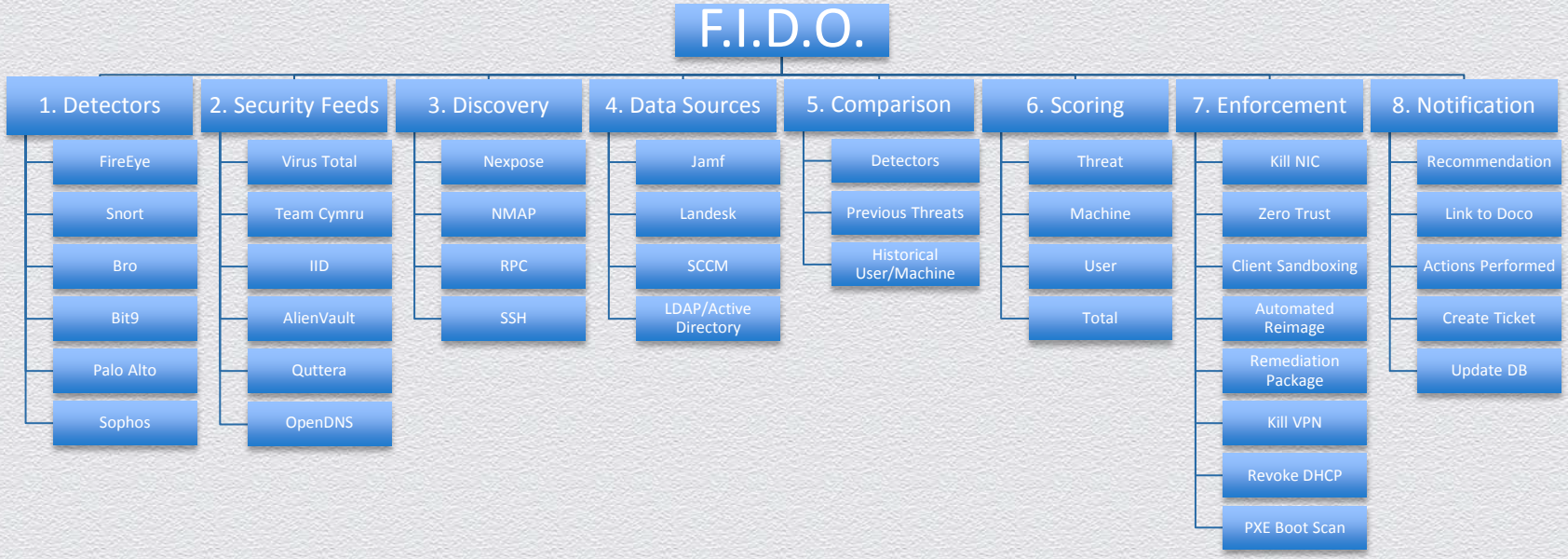
NETFLIX

F.I.D.O. High-level



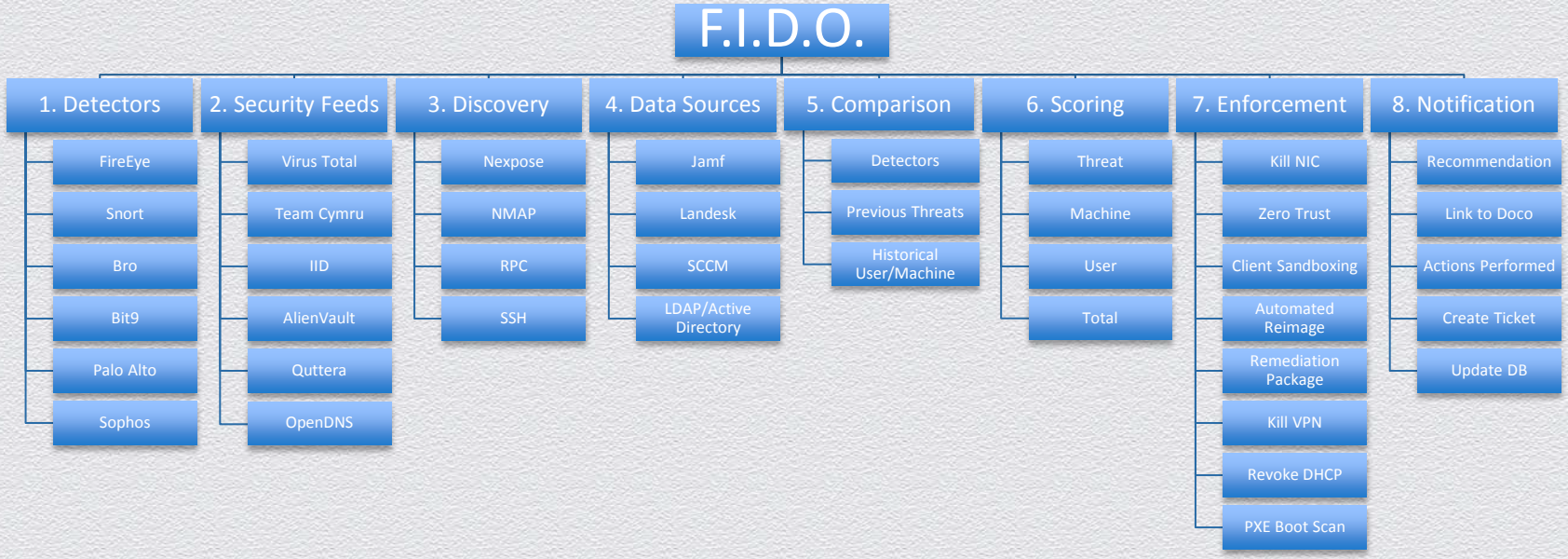
NETFLIX

F.I.D.O. High-level



NETFLIX

F.I.D.O. High-level



F.I.D.O. Next Steps

- github.com/Netflix/Fido… contribute
- Expand outside corporate perimeter
- Continue to integrate… Bro and more threat feeds
- Evaluation engine for threat feeds
- Updater for detectors
- Improve and expand scoring engine algorithms
- F.I.D.O. console

NETFLIX

Conclusion

- Integration and automation are key to reducing response time
- Create a consistent method of evaluation
- Compare any and all data
- Combine user, machine and threat information for scoring
- Eliminate overhead between teams
- Don’t just gather information… respond
- Tell your vendors

NETFLIX

Thank you!

- rob.fry@netflix.com
- Feedback is always appreciated
- Ideas? Please let me know

NETFLIX