

RSAConference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: SPO3-W02

Building The Midgardian Citadel: Active Detection and Response

Dave Baumgartner

Vice President, Cyber Security
Target

Grady Summers

Senior Vice President, Cloud Analytics
FireEye, Inc
@GradyS

CHANGE

Challenge today's security thinking

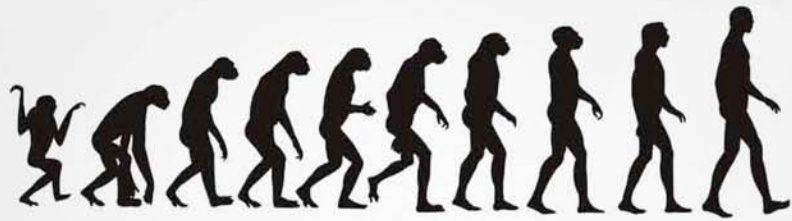


A black and white illustration of a warrior on a horse. The warrior is wearing a helmet and armor, and is riding a dark horse. The horse is galloping towards the right. The background shows a mountainous landscape with some trees and a large, dark, shadowed area on the left. The overall style is reminiscent of a classic comic book or pulp magazine illustration.

THE MIDGARDIAN CITADEL

THE JOURNEY

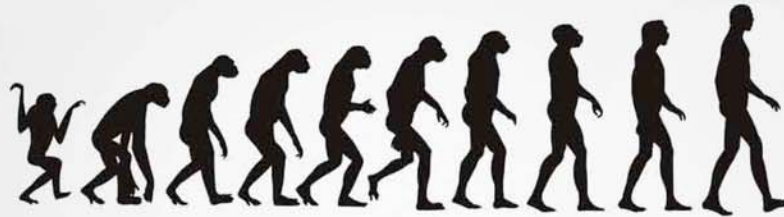




Ops-Centric -> IR-centric

Passive -> Active

Collect tool output -> Collect it all



Rely on products -> Rely on threat intel

Silos -> Fusion

Tools -> People

Signatures -> Signatureless





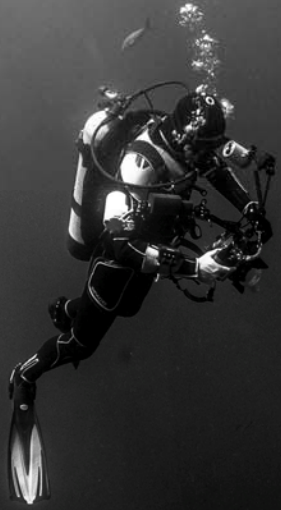
PILLARS OF THE FORWARD-LEANING SOC

Intelligence-Driven

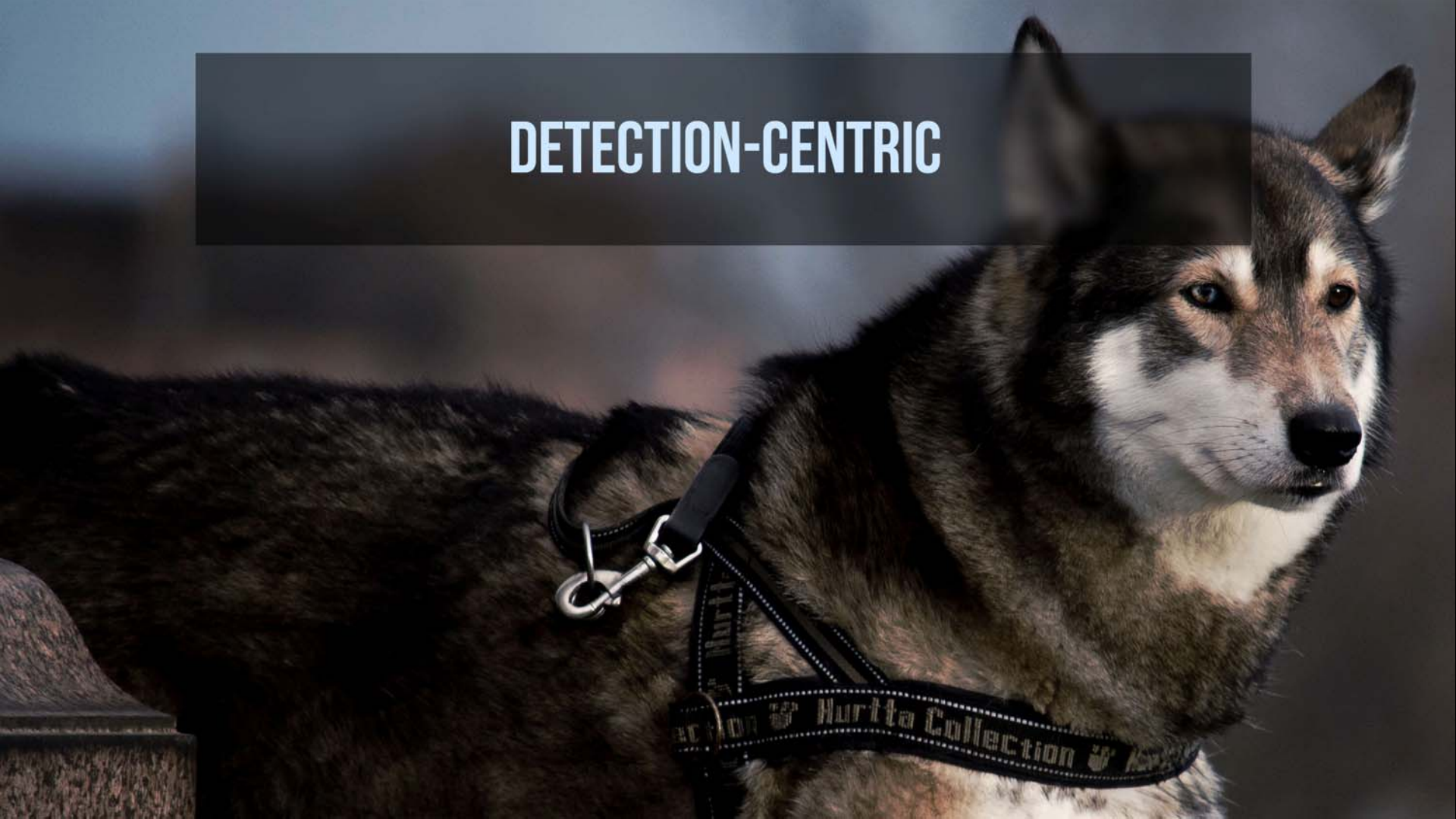
Detection-Centric

Continuous Improvement

INTELLIGENCE-DRIVEN



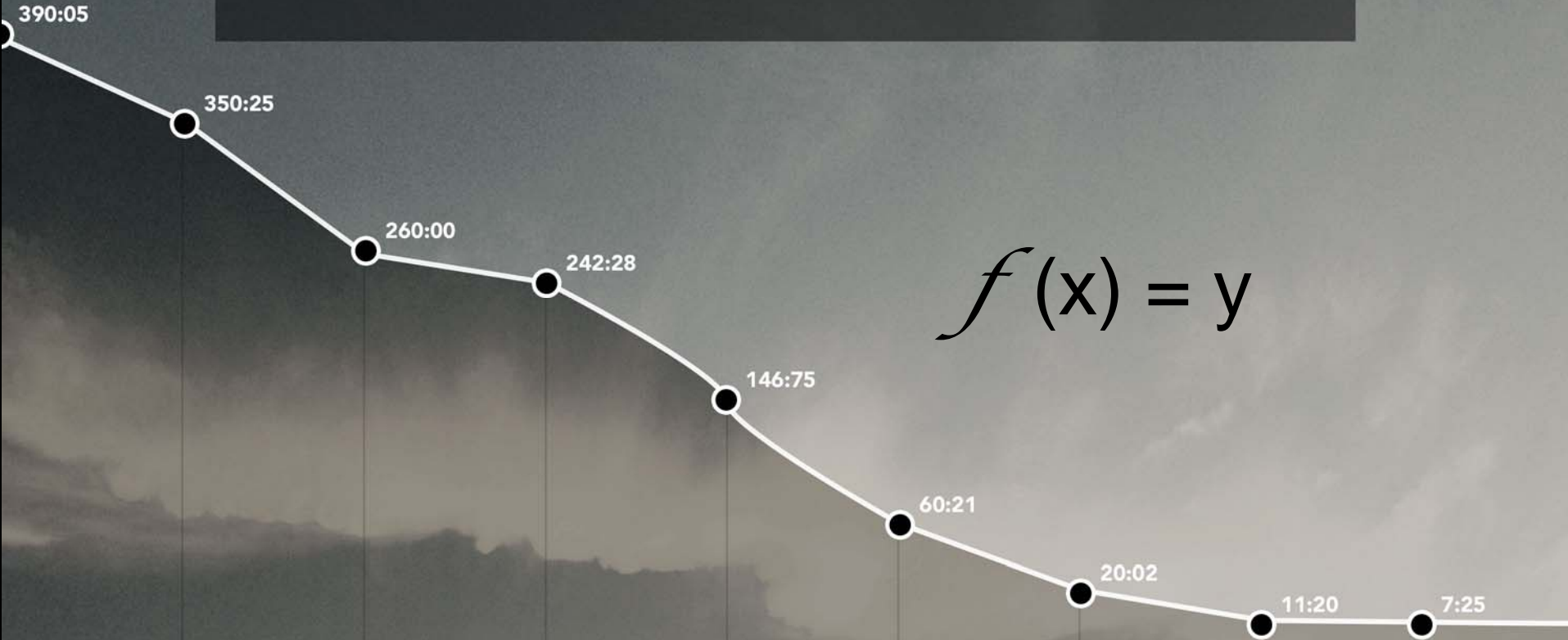
DETECTION-CENTRIC



CONTINUOUS IMPROVEMENT



CONTINUOUS IMPROVEMENT



$$f(x) = y$$

TEST YOURSELF CONSTANTLY





HOW DO YOU DO THIS RAPIDLY?

- Focus on the Urgent, not the Important
- Leverage small SWAT teams, not big projects
- Assign your most experienced executives and team members
 - If they are too busy, see bullet 1
- Test, measure, improve, repeat – weekly
- Find a firm you trust



RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

TECHNOLOGY



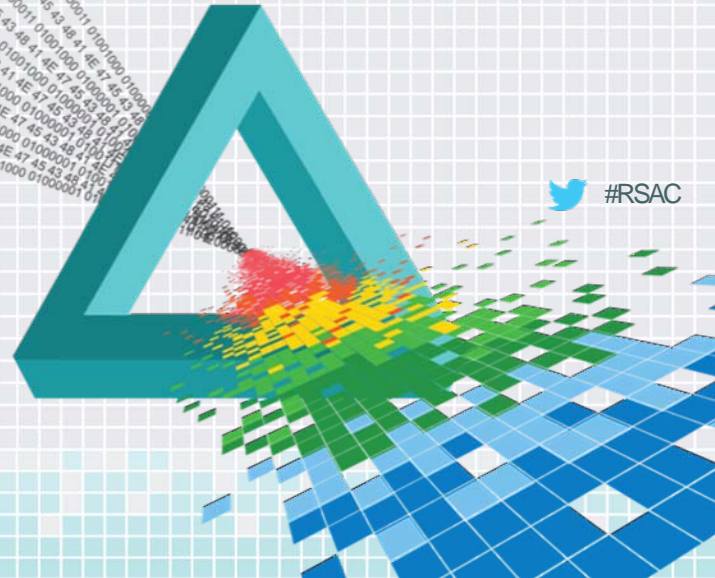
Apply What You Have Learned Today

- ◆ Next week you should:
 - ◆ Define the mission and purpose of your SOC
 - ◆ List everything that your team is working on, and streamline
- ◆ In the first two weeks following this presentation you should:
 - ◆ Identify the “output metrics” that you should be measuring
 - ◆ Determine your detect-to-contain time and set a goal
- ◆ Within a month you should:
 - ◆ Establish how you will be testing and measuring your capability
 - ◆ Show demonstrated improvement

RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

Questions?



 #RSAC