CAPER

2017 Summer Research Planning Workshop

Threat Hunting in a Utility Landscape

Ben Sooter

7 August 2017

Introducing EPRI…

EPRI is a company that…

…brings together great people…

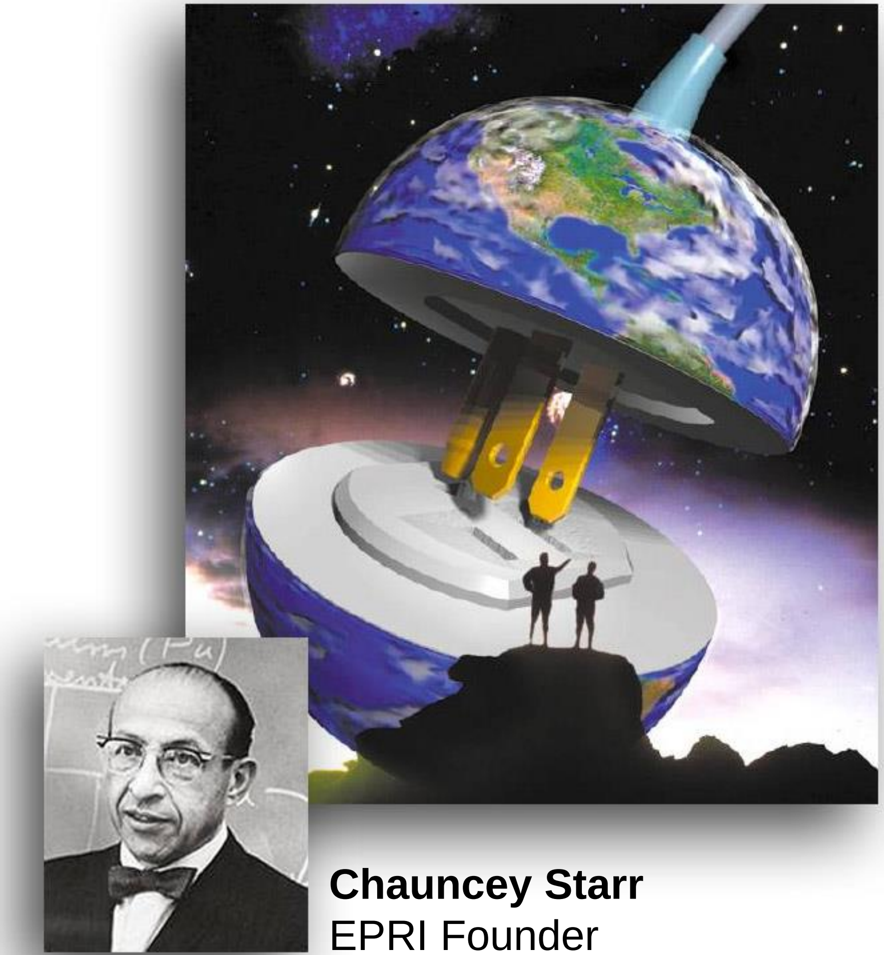
…with new and exciting ideas…

…to help energize the world!

"Together…Shaping the Future of Electricity"

Our History…

- Founded in 1972
- Independent, nonprofit center for public interest energy and environmental research
- **Collaborative** resource for the electricity sector
- Major offices in Palo Alto, CA; Charlotte, NC; Knoxville, TN
  - Laboratories in Knoxville, Charlotte and Lenox, MA



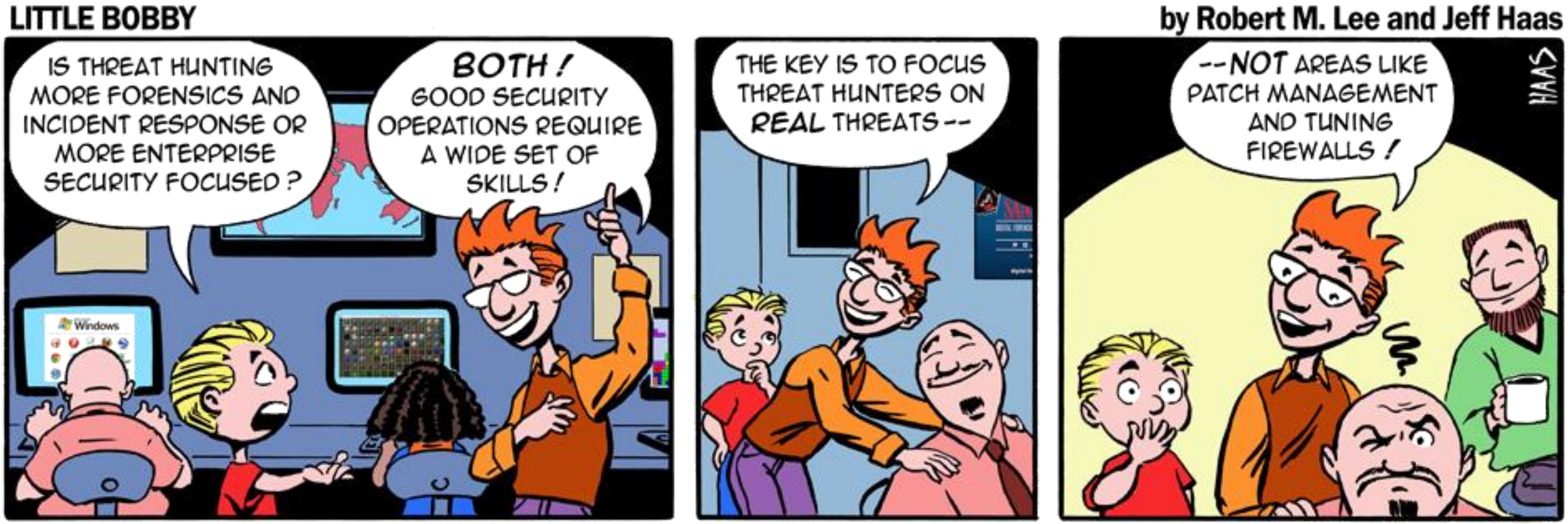
Chauncey Starr
EPRI Founder

Our Members…

- 450+ participants in more than 30 countries
- EPRI members generate approximately 90% of the electricity in the United States
- International funding approximately 25% of EPRI’s research, development and demonstrations
- Research funded by more than 1,000 energy organizations

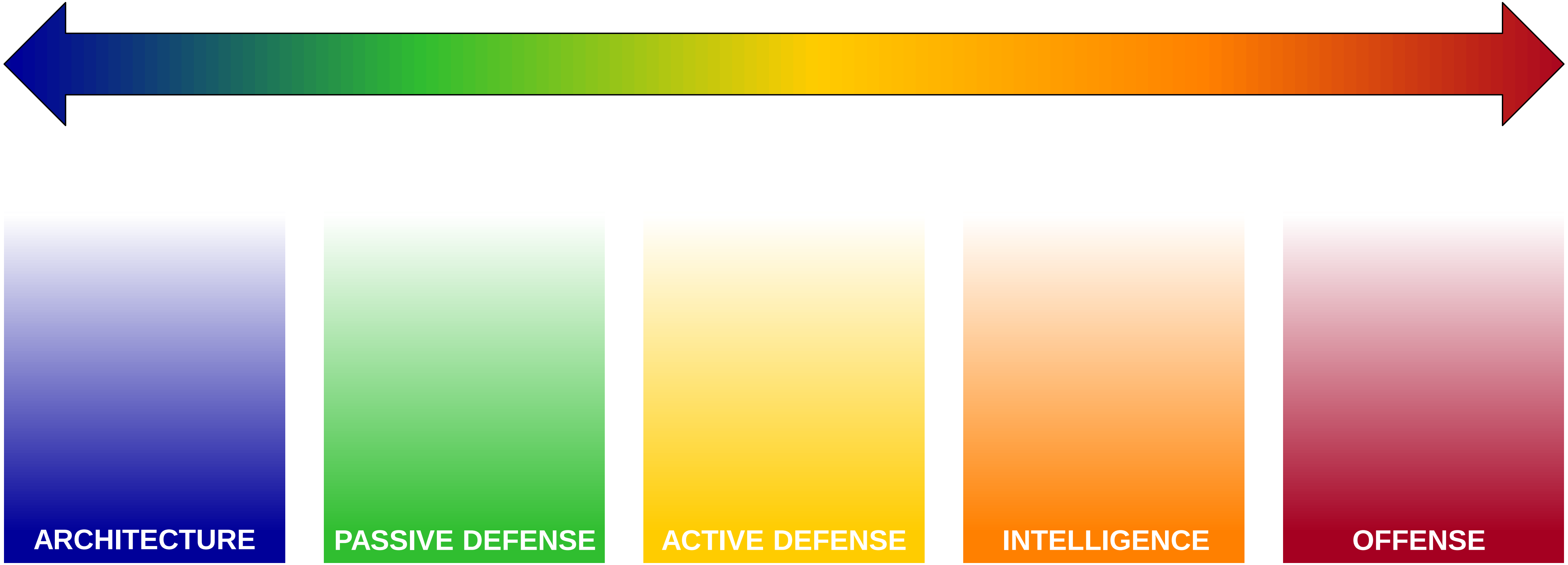
What is Threat Hunting

- Threat Hunting is the act of proactively and iteratively searching through networks and datasets to detect threats that evade existing automated tools.


LITTLE BOBBY
by Robert M. Lee and Jeff Haas
IS THREAT HUNTING MORE FORENSICS AND INCIDENT RESPONSE OR MORE ENTERPRISE SECURITY FOCUSED?
BOTH! GOOD SECURITY OPERATIONS REQUIRE A WIDE SET OF SKILLS!
Windows
THE KEY IS TO FOCUS THREAT HUNTERS ON REAL THREATS --
--NOT AREAS LIKE PATCH MANAGEMENT AND TUNING FIREWALLS!
HAAS

http://www.littlebobbycomic.com/projects/week-97/

The Sliding Scale of Cyber Security



ARCHITECTURE

The planning, establishing, and maintenance of systems with security in mind

PASSIVE DEFENSE

Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction

ACTIVE DEFENSE

The process of analysts monitoring for, responding to, and learning from adversaries internal to the network

INTELLIGENCE

Collecting data, exploiting in into information, and producing intelligence

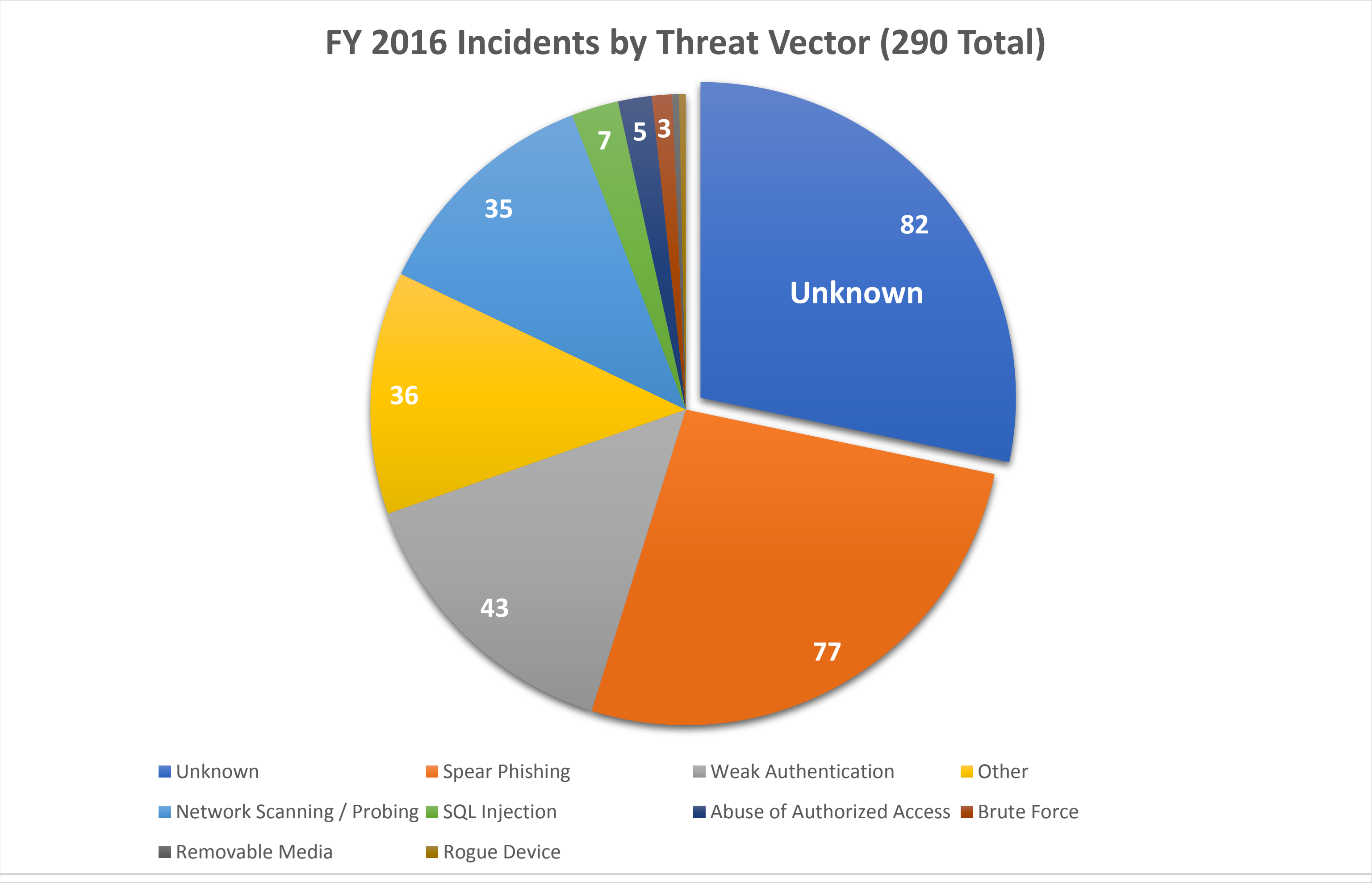
OFFENSE

Legal countermeasures and self-defense actions against an adversary

https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240

Why we need Threat Hunting

- ICS-Cert Year in Review (FY 2016)



FY 2016 Incidents by Threat Vector (290 Total)

Why we need Threat Hunting

	2015	2016
Substations	50+	1
Customers	225K	Portion of Capitol region
MW Impact	135 MW	200 MW

- Cyber Attacks on the Ukraine Electric System

2015	2016
Malware Role	Malware Role
Highly Coordinated	Highly Targeted
Electric System Impacts	Modular and Customizable
Significance First public cyber attack on civilian power infrastructure	Significance First public discovery of modularized malware targeting electric power industry

Utility Hunting Maturity Model (UHMM)

UHMM 0 Initial	UHMM 1 Minimal	UHMM 2 Operational	UHMM 3 Procedural	UHMM 4 Innovative	UHMM 5 Leading
• Relies primarily on automated alerting • Little or no routine data collection	• Incorporates IT threat intelligence indicator searches • Moderate or high level of routine data collections of IT systems	• Incorporates OT threat intelligence indicator searches • Moderate or high level of routine data collections of IT and OT systems	• Follows data analysis procedures created by others • High or very high level of routine data collection of IT and OT systems	• Creates new data analysis procedures • High or very high level of routine data collection of IT and OT systems	• Automates the majority of successful data analysis procedures • High or very high level of routine data collection of IT and OT systems

A Simple Hunting Maturity Model - http://detect-respond.blogspot.com/2015/10/a-simple-hunting-maturity-model.html

Case Study: Anonymous Utility Incident Response

- Problem:
  - Utility called with a case of conficker
  - Could not determine infection vector
- Unsuccessful Remediation:
  - Remote access to unmanned site to clean infection
  - Returned within 2 hours each time
- Hypotheses:
  - The customer was infecting themselves
  - The vendor was remoting in and infecting
  - Transient devices were coming and going

Case Study: Windfarm

- Problem:
  - Windfarm identified abnormal behavior
  - Systems were patching themselves
- Hypotheses:
  - IT was not coordinating patching
  - Rogue operator patching systems
  - Adversary patching systems

Case Study: Plant

- Problem:
  - A plant acquired malware on an air gapped ICS network
  - Could not determine the infection vector
- Unsuccessful Remediation:
  - All windows based computers on the network were shutdown, wiped, and restored from backups
  - Returned within an hour each time
- Hypotheses:
  - The vendor was remoting in and infecting
  - The backups were previously infected
  - A rogue device was plugged into the protected network

Together…Shaping the Future of Electricity