RSAConference2018

Singapore | 25–27 July | Marina Bay Sands

#RSAC

SESSION ID: TTA-F03

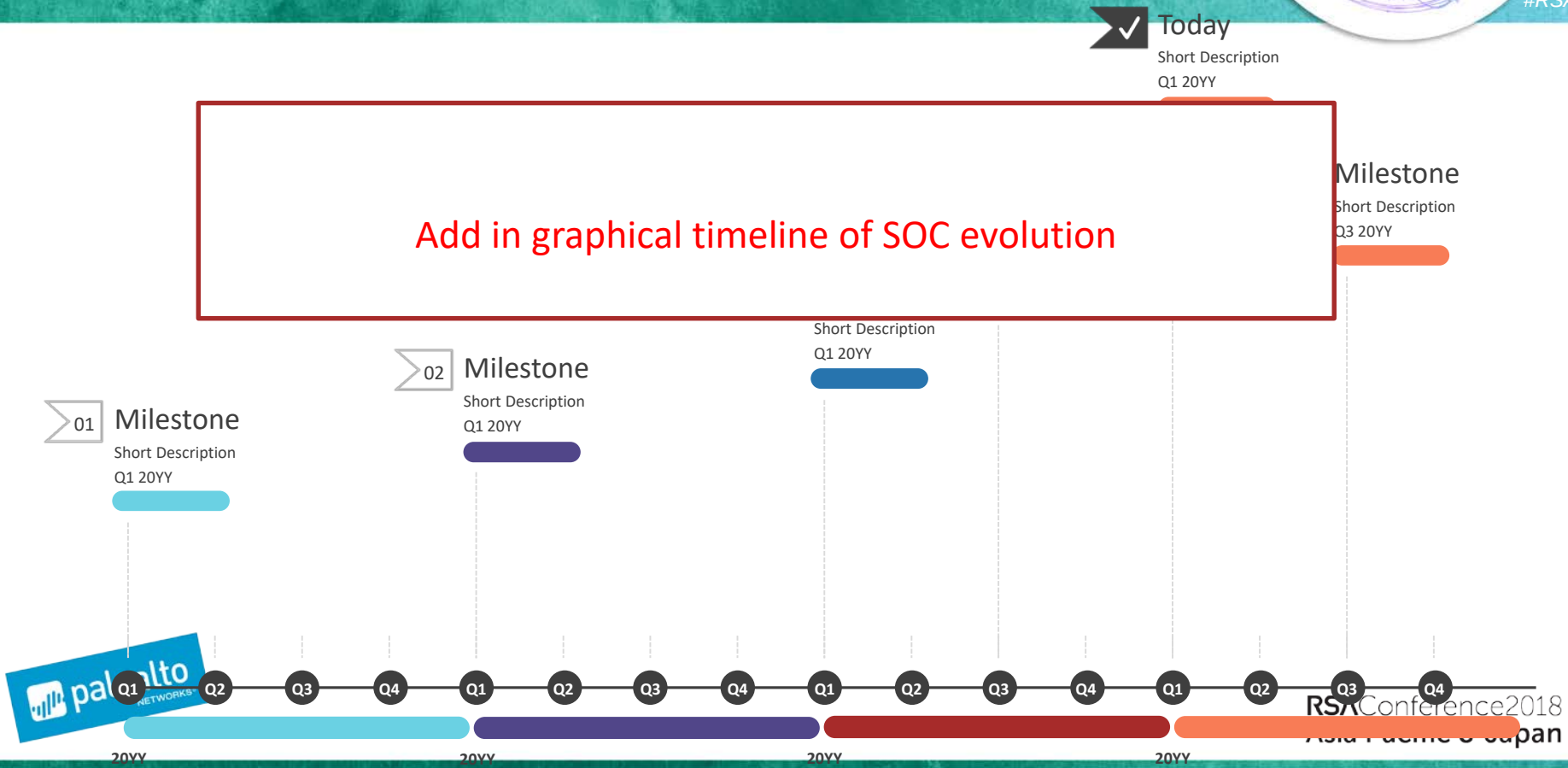
Security Operations 2018: What is Working? What is Not.

Kerry Matre

Security Operations Strategist
Palo Alto Networks


Reconnaissance
Internet Scans
Preventions
Firewall
Trojan
Proofpoint

How did we get here?



#1 Naming makes no difference

Most Popular:

- Security Operations Center (SOC)
- Cyber Defense Center (CDC)

Components:

- Defense Center = Protective
- Intelligence Center = High Caliber Analysis
- Threat = Risk Based
- Cyber = Electronic vs. Physical
- Fusion Center = Coordination with a NOC

#2 Mission Matters

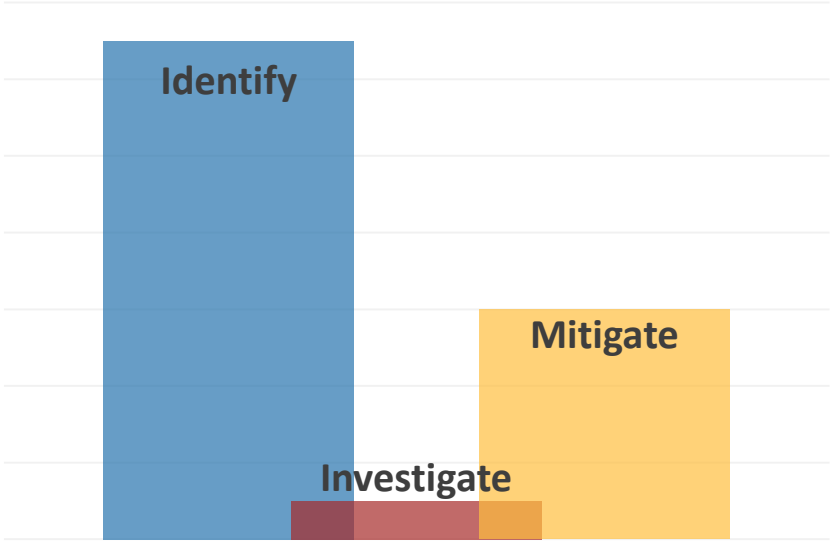
Yes!

- Identify
- Investigate
- Mitigate

NO!

- Engineering
- Network Operations
- Forensics
- Incident Response
- Compliance
- Integrations/Development

Analyst time allocation



- Feeds != Use Cases
- Overwhelmed by false positives
- Detune sensors
- Ignore alerts
- Fire-and-forget mitigation
- Console burnout

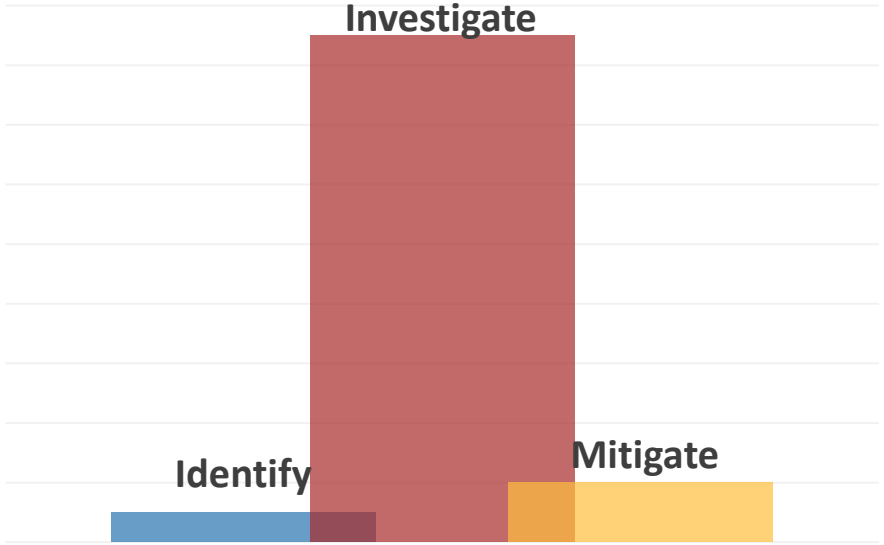
#3 Prevention-based Architectures

- Consistent Protection (Network, Endpoint, Cloud)
- Centralized Management
- Automated Threat Prevention
- Prevention Based on Users, Applications and Data

paloalto NETWORKS

Ideal analyst time allocation

- Better outcomes
- Faster remediation
- Smart people working on smart things
- More job satisfaction



#4 Formalized Hunting

"Smart people looking for things missed all other ways"

- Time to do it – 2 week, goal-oriented sprints
- Process driven, agile
- Driven by piece of Intel
- Hunt ends with what was learned & feedback into the controls

How many tools do you use?

#5 Too many tools

- Average 40 tools
- Very small feature use
- Consolidation on a platform

Build your own?

- High cost
- Low results

#6 Working with the business

- SOC/NOC Integration
- Business Unit alignment
- IT Integration
- Business liaison
- Automation developer
- Operations engineer

#7 Metrics that matter

The right metrics drive change.

Bad Metrics

- Mean Time to Resolution (MTTR)
- # of incidents handled
- # of alerts
- # of feeds

Two types of metrics

Configuration Confidence

Operational Confidence

Good Metrics

Configuration Confidence

- Are controls running?
- Control changes
- Configured to best practices
- Feature use
- % of traffic visible

Operational Confidence

- Events per analyst hour (EPAH)
- Duplicate incidents
- Alerts for known threats
- Deviation from SOC procedures

Actual Results: There is good news!

- Drastically reduced events
  - 90% reduction in support tickets to reimage machines from malware infections
  - Reduced threat alerts from ~20 million per day to ~1.2 million per day; nearly 80% reduction in noise
  - Automatic blocking of 95% of events
- Stabilized headcount
  - Reduced EPAH from 200 to 20
  - 40% gain in administration efficiency
- Playbook and threat prevention automation
  - Implementation of security controls based on IoCs reduced from days to minutes due to automated threat prevention.
  - Threat intelligence processing reduced by 50% from automation
  - EDLs' turned threat response to blocks within 5 minutes

Apply What You Have Learned Today

- Next week you should:
  - Define or clarify the mission of your SOC and get buy-in from the business.
- In the first three months following this presentation you should:
  - Question your metrics. Align them to Configuration and Operational confidence.
  - Evaluate your toolsets and usage. Enable existing features.
- Within six months you should:
  - Adopt a prevention-based architecture for better protection and to reduce noise in the SOC.
  - Create an agile, defined hunting process.
  - Hire a business liaison; move controls closer to the business.

paloalto NETWORKS