IBTTA

TOLLING. MOVING SMARTER.

ANNUAL TECHNOLOGY SUMMIT | ORLANDO, FL | MARCH 31-APRIL 2, 2019

Detection of a Breach

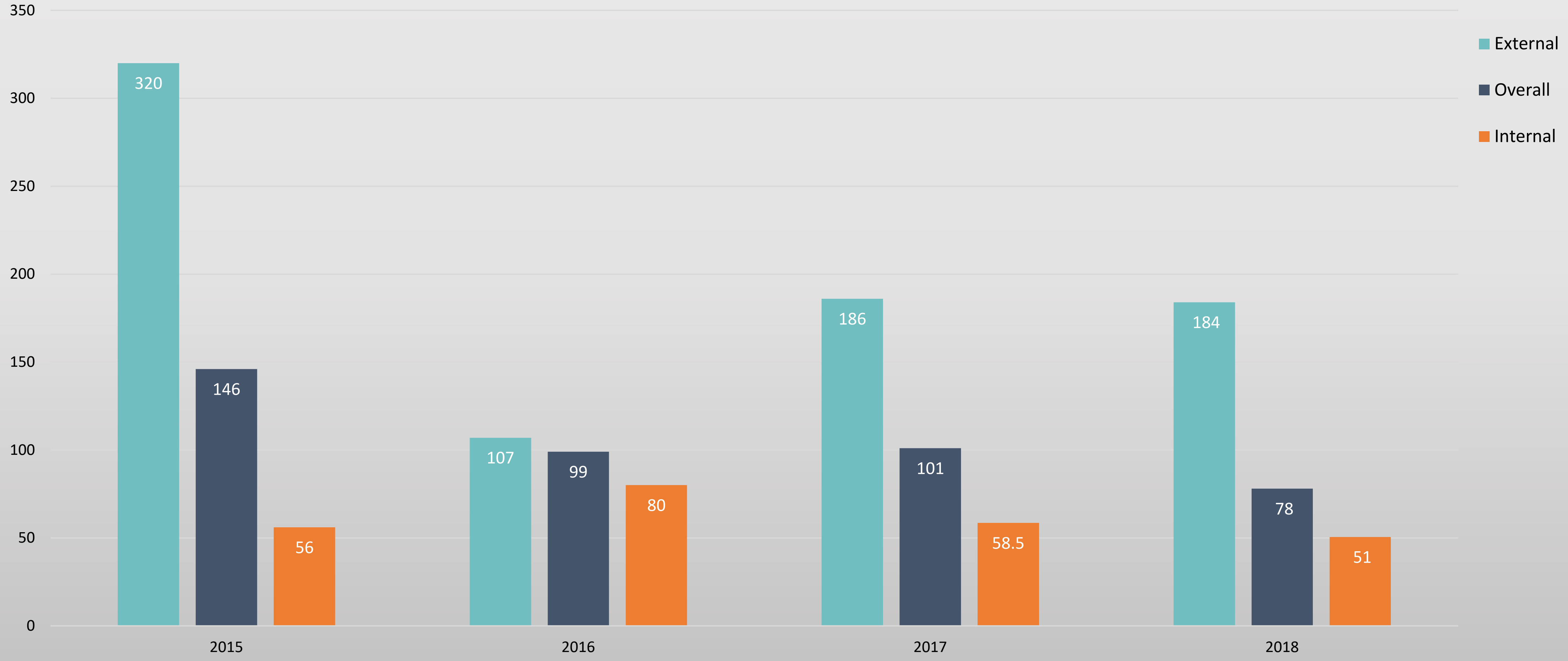
Lyle Sudin, Senior Manager – FireEye Mandiant

FIREEYE™

Current State of the Industry

- **You have something valuable to attackers**
  - Personal information
    - Names, mailing addresses, email addresses, social security numbers
  - Financial information
    - Credit card and bank account data
  - Intellectual property and proprietary data
    - Technical information
- **You are a target**
  - 8% of Mandiant breach response engagements were for the Transportation and utility sectors
- **Breaches are inevitable**
  - How do you ensure you can respond as effectively as possible?
  - Average cost of a breach in the US is $7.91 million
  - Focus on improving your cyber security incident detection and response

Internal vs. External Detection



Dwell Time by Detection Source

How do you build an effective detection program?

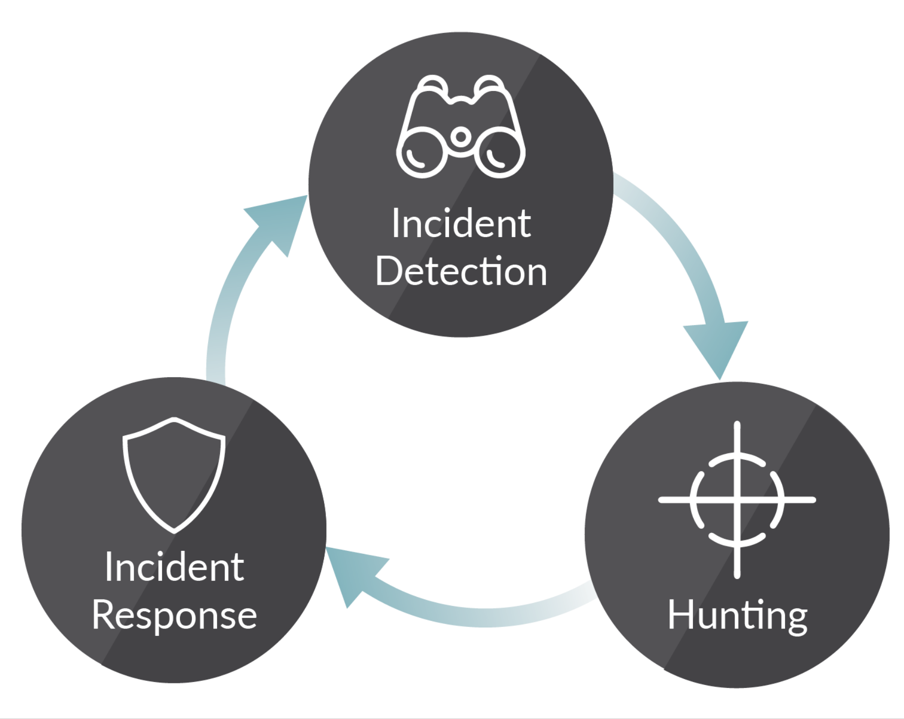
- **Effective breach response is a combination of people, processes, and technology**
  - Many organizations focus solely on technology
  - Training and experience are required for your incident responders to effectively respond
  - Documented processes are required to respond consistently and efficiently
- **The industry is changing but attackers are also changing**
  - Attackers are achieving their objectives without malware
  - Less than 50% of Mandiant investigations conclude malware was the breach factor
- **How do you prepare for a breach?**
  - Build an effective cyber defense program
  - Conduct Red team assessments to provide your incident responders with experience in responding to attacks
  - Conduct regular executive and technical tabletop exercises – effective incident response is limited to the SOC
  - Regularly analyze your visibility, including technology and logging
  - Ensure you have an Incident Response retainer and cyber insurance

Effective Cyber Defense

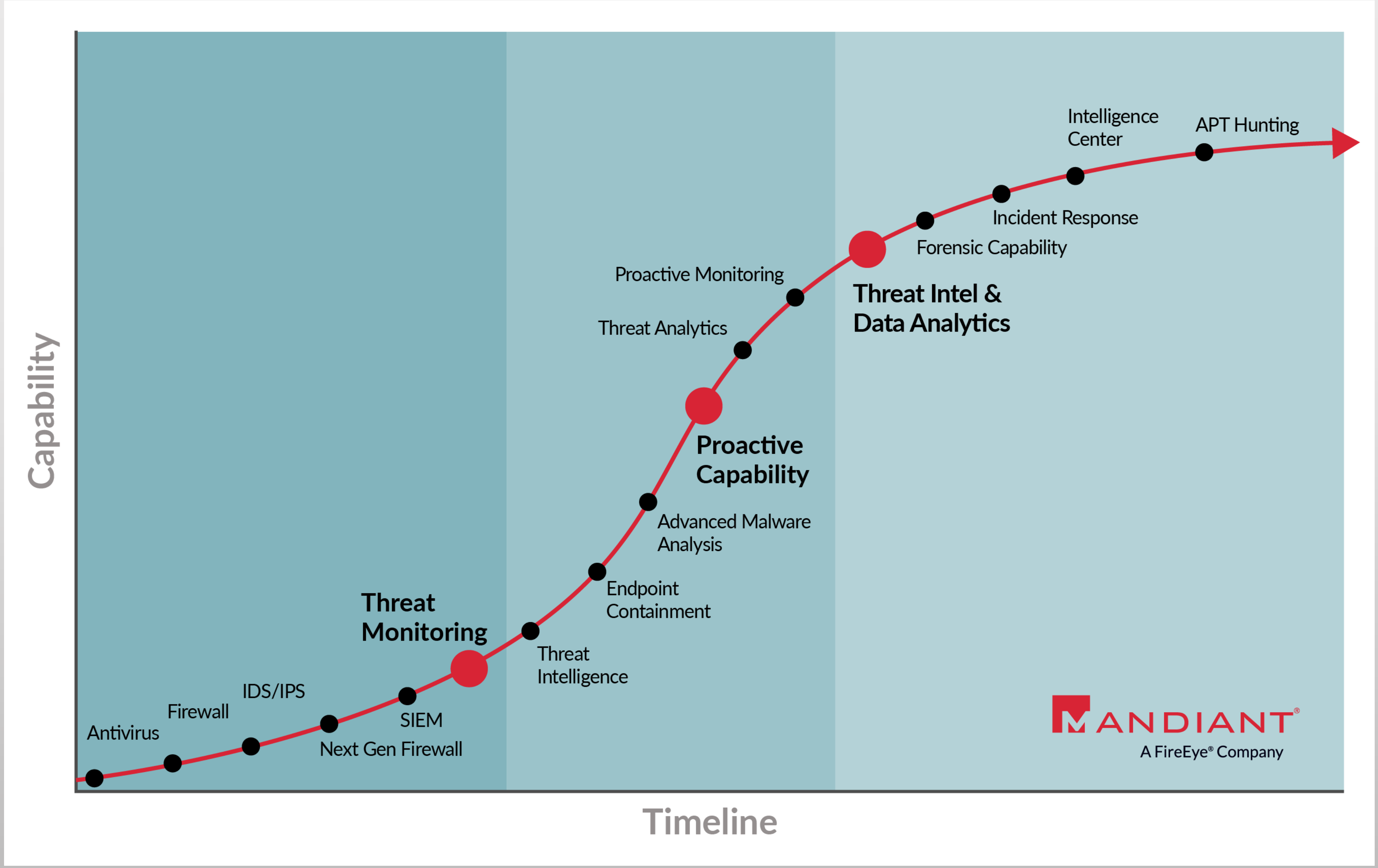
Detect and Respond to Every Incident in < 10 Minutes

Minimize organizational risk and allow business to function while under continuous attack

- **Predictive** – Continuously measure enterprise attack surface and model potential threat vectors targeted at critical assets and data
- **Proactive** – Hunt for intrusions. Discover and remediate / compensate for vulnerabilities. Leverage Threat Intelligence to understand attacker goals and techniques
- **Responsive** – Rapid analysis and containment of threats



Maturity of a Cyber Defense Program



Framework for an Effective Cyber Defense Capability

Capability	Description
GOVERNANCE	• Organizational structure that aligns with the overall business organization and mission statement • Clear security policy and guidance that safeguard critical systems and information while enabling business functions technologies
COMMUNICATION	• Mechanisms and processes that promote effective information sharing between internal and external entities
VISIBILITY	• Technologies and processes that provide an organization awareness of activities occurring on systems and networks • Methods by which the Computer Incident Response Team (CIRT) maintains an awareness of the threat landscape and applies that understanding to defending critical infrastructure
INTELLIGENCE	• Cyber threat intelligence capabilities that enable a detailed understanding of the adversary's capabilities, techniques, and intent • Intelligence that informs and enhances security planning, vulnerability management, and incident response
RESPONSE	• Processes and technologies that the CIRT uses to identify, categorize, investigate, and remediate adverse security events
METRICS	• Objective measures of the efficiency of people, processes, and technology using a system that can be easily tracked and automated • Focused incident response metrics that are tied to overall business and security goals and objectives, driving continuous improvement