LESS IS MORE IN CYBER!

Simon Mullis
Global Technical Lead, Alliances
FireEye, Inc.
Simon.Mullis@FireEye,com

Current State of Cyber Security

Coordinated Persistent Threat Actors

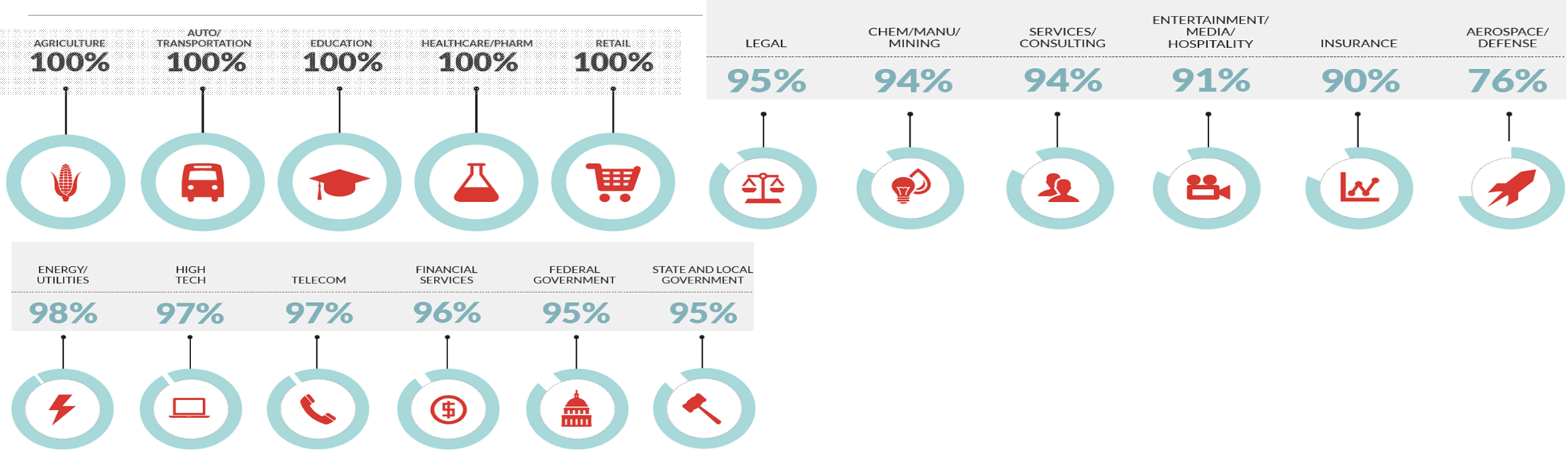
Dynamic, Polymorphic Malware

NEW THREAT LANDSCAPE

Multi-Vector Attacks

Multi-Staged Attacks

Real world Real threats: Levels of compromise in 2014

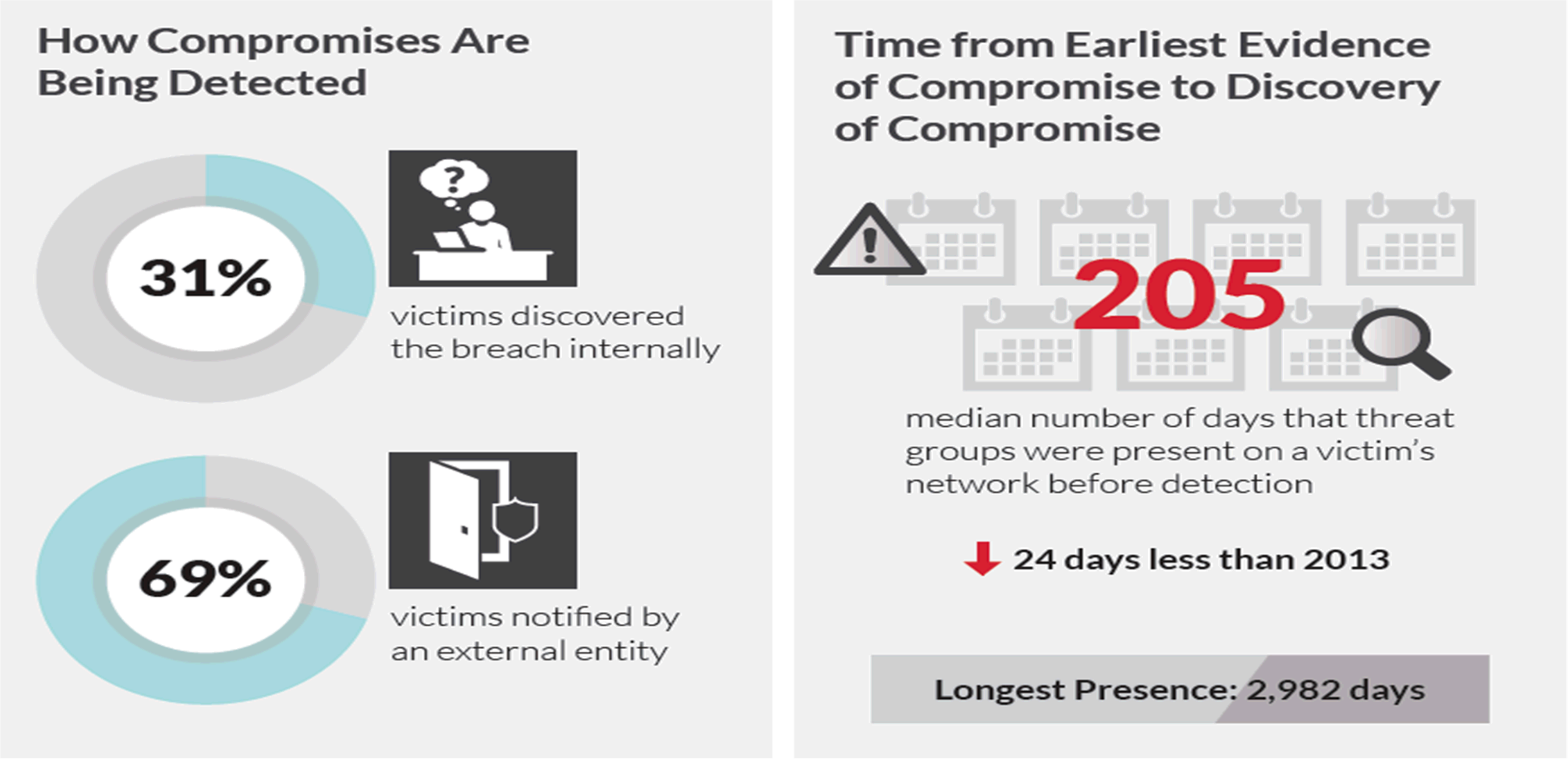


AGRICULTURE	100%
AUTO/ TRANSPORTATION	100%
EDUCATION	100%
HEALTHCARE/PHARM	100%
RETAIL	100%
LEGAL	95%
CHEM/MANU/ MINING	94%
SERVICES/ CONSULTING	94%
ENTERTAINMENT/ MEDIA/ HOSPITALITY	91%
INSURANCE	90%
AEROSPACE/ DEFENSE	76%
ENERGY/ UTILITIES	98%
HIGH TECH	97%
TELECOM	97%
FINANCIAL SERVICES	96%
FEDERAL GOVERNMENT	95%
STATE AND LOCAL GOVERNMENT	95%

Table 1: Advanced malware concentration by industry

Had Advanced Malware					
Agriculture	50%	Aerospace/Defense	30%	Entertainment/Media/Hospitality	18%
Auto/Transportation	40%	Services/Consulting	29%	Insurance	18%
Education	37%	Financial Services	28%	Chem/Manu/Mining	17%
Gov (Fed)	36%	Energy/Utilities	27%	Retail	17%
Telecom	36%	Gov (State/Local)	27%	Legal	10%
High Tech	32%	Healthcare /Pharm	22%	Average	27%

M-Trends 2015



How Compromises Are Being Detected

31% victims discovered the breach internally

69% victims notified by an external entity

Time from Earliest Evidence of Compromise to Discovery of Compromise

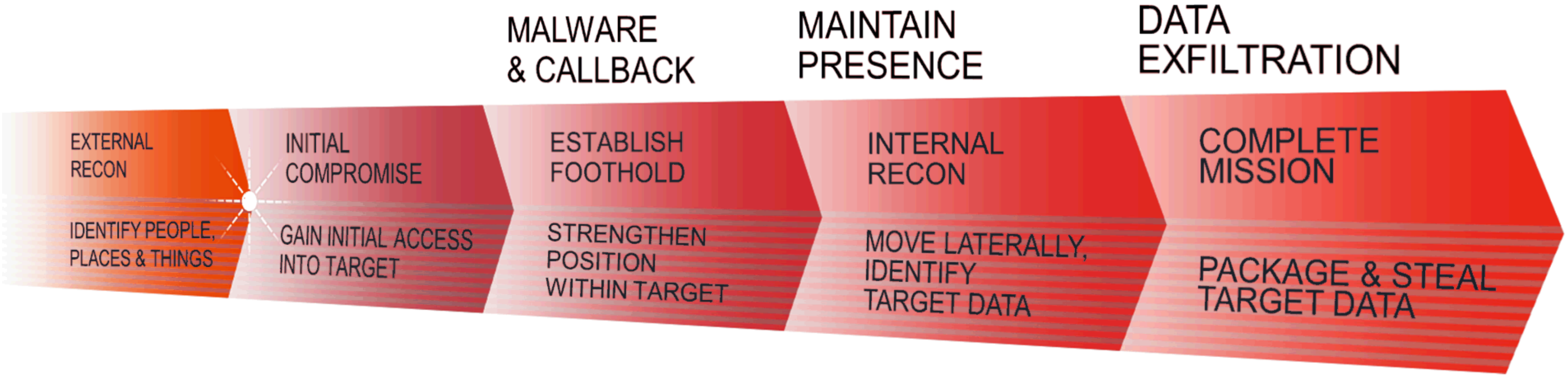
205 median number of days that threat groups were present on a victim's network before detection

↓ 24 days less than 2013

Longest Presence: 2,982 days

AVOIDING DISCOVERY

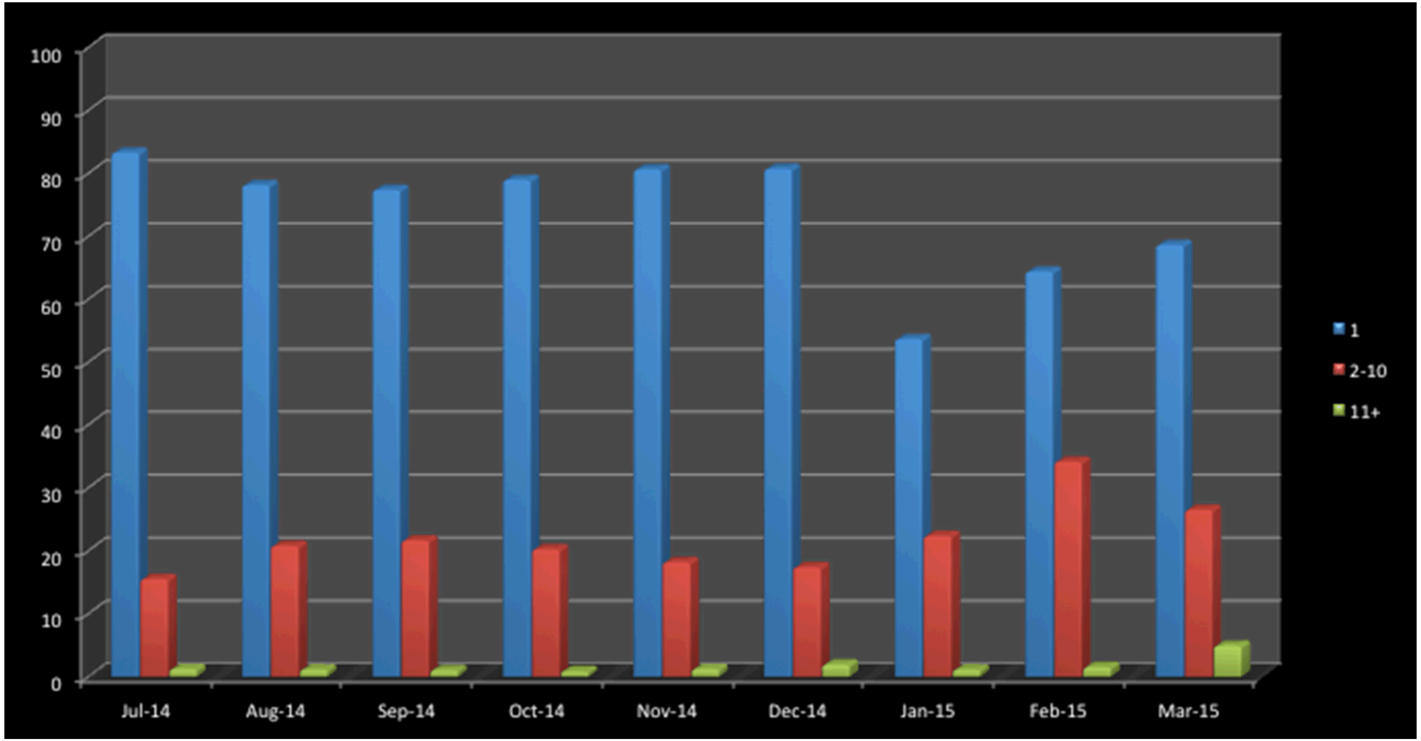
ATTACKERS UTILIZE MULTIPLE VECTORS
AND MULTIPLE FLOWS TO COMPLETE THEIR MISSION


MALWARE & CALLBACK
MAINTAIN PRESENCE
DATA EXFILTRATION
EXTERNAL RECON
IDENTIFY PEOPLE, PLACES & THINGS
INITIAL COMPROMISE
GAIN INITIAL ACCESS INTO TARGET
ESTABLISH FOOTHOLD
STRENGTHEN POSITION WITHIN TARGET
INTERNAL RECON
MOVE LATERALLY, IDENTIFY TARGET DATA
COMPLETE MISSION
PACKAGE & STEAL TARGET DATA

DETECTING THE EXPLOIT IS KEY SINCE EVERY PHASE AFTER THAT CAN BE ENCRYPTED BY THE ATTACKER

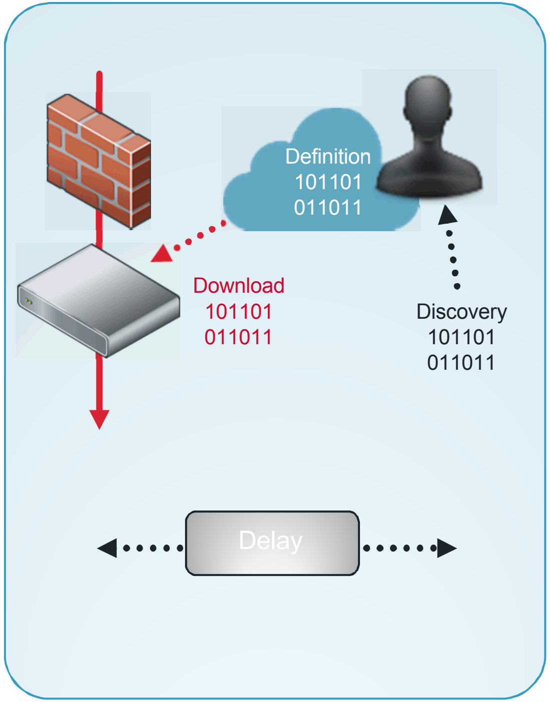
Ave. 74% attacks are custom designed & unique

(% of number instances of each attack per company by month first seen)

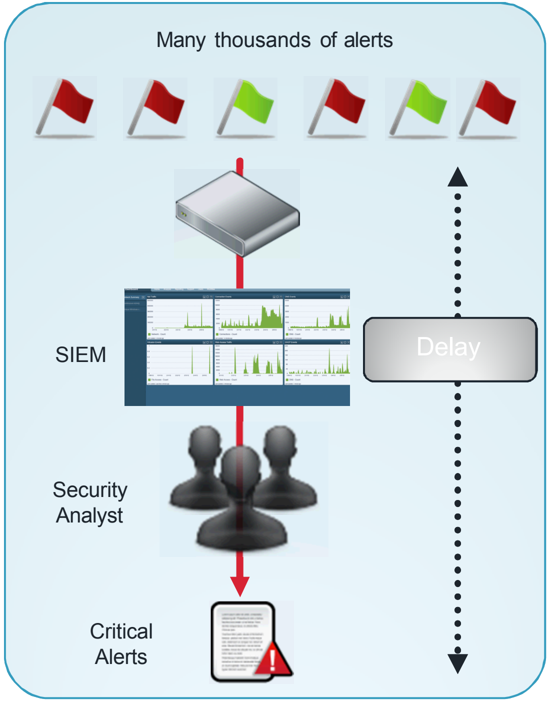


Ave. 99,000 unique samples per month

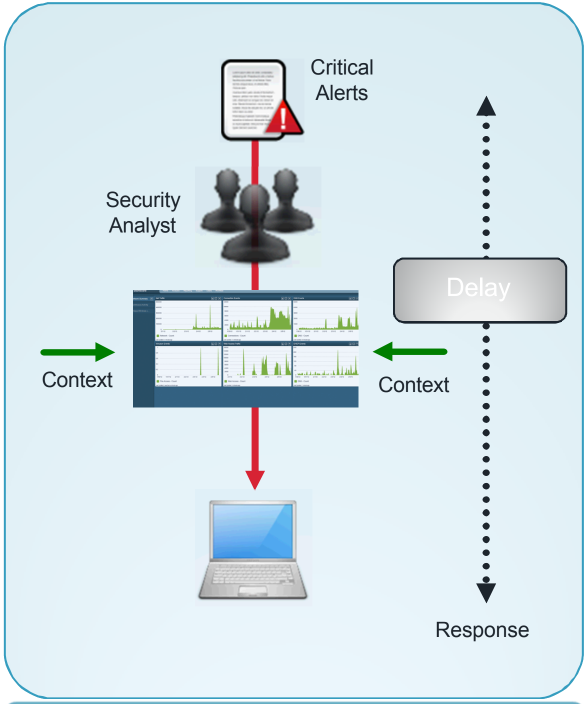
Traditional Defense-in-Depth – The Reality



1. Reactive Security



2. Needle in the Haystack



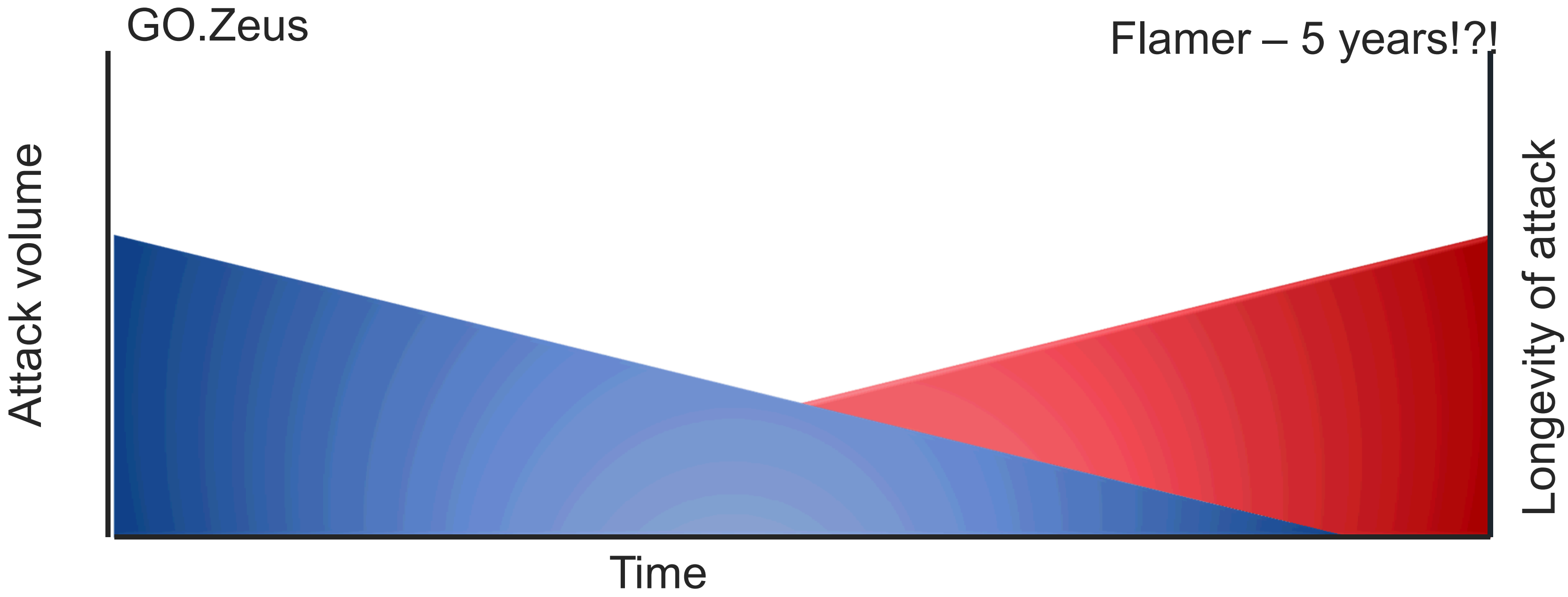
3. Missing Context

Missed or Delayed Detection

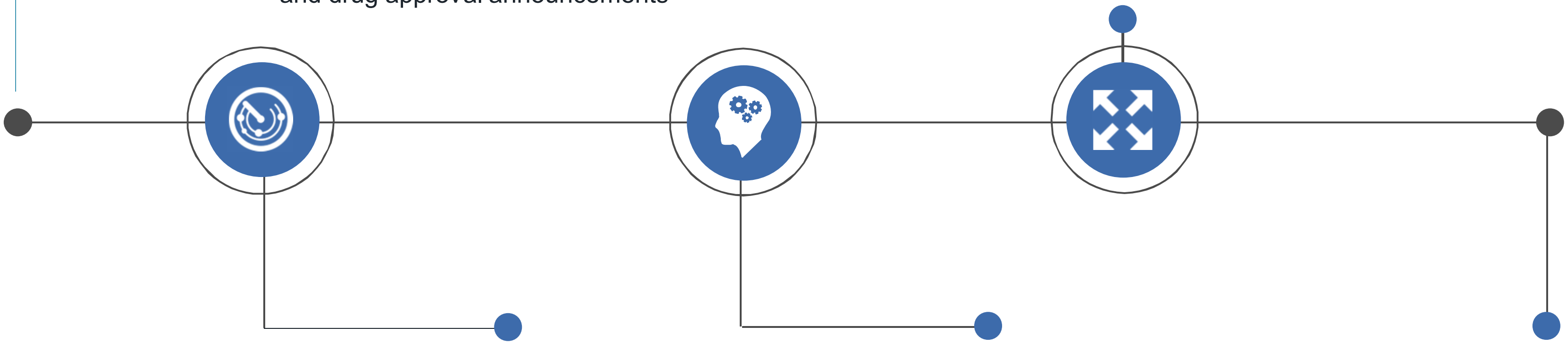
Manual Processing (More spend)

Limited Context (Delayed Response)

Impact: Less is more!



INCIDENT RESPONSE AND INTELLIGENCE IN ACTION: FIN4



WHO ARE THEY?

Financially Motivated Group 4

- **Tactics:** Compromise email accounts; spear phishing
- **Targets:** Healthcare and pharmaceuticals; advisory firms
- **Impact:** Insider trading advantage from early access to R&D and drug approval announcements

HOW DID WE FIND IT?

Summer 2014

- Incident response at major financial firms
- Similar activity, methodology, and targets

INCIDENT RESPONSE INFORMS PRODUCT DETECTION

Summer 2014

- Deployed across FireEye products

FIN4 REPORT PUBLISHED

Dec 2014

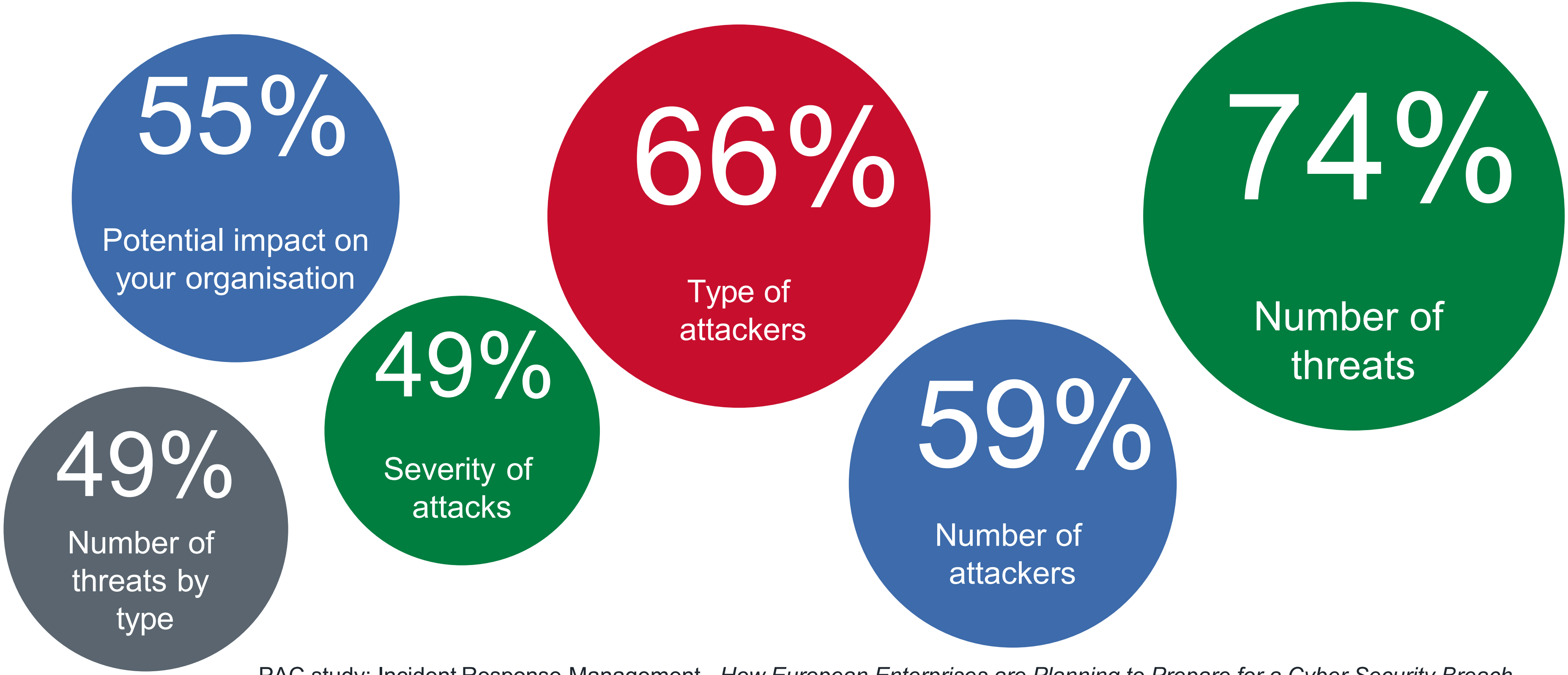
- Victim compromises were wide and broad
- Daily indicators of breached customers
- Signatures & recommendations used for widespread detection and prevention

IR INTELLIGENCE

- IOCs created
- Gathered intelligence informs log analysis (e.g. terms, IPs)
- Additional intelligence cycled back into products

FireEye

How do you measure the cyber landscape?



55%

Potential impact on your organisation

49%

Number of threats by type

49%

Severity of attacks

66%

Type of attackers

59%

Number of attackers

74%

Number of threats

PAC study: Incident Response Management - *How European Enterprises are Planning to Prepare for a Cyber Security Breach*

THANK YOU

Questions

Simon Mullis
Global Technical Lead
FireEye, Inc.
Simon.Mullis@FireEye,com