RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

How Shared Security Intelligence Can Better Stop Targeted Attacks

SESSION ID: SPO3-T07

Piero DePaoli

Senior Director
Global Product Marketing
Symantec Corporation

Targeted Attacks are an Increasing Issue

66%

Breaches went undetected for 30 days or more

4

Months to remediate

42%

Increase in Targeted Attacks Last Year

Targeted Attacks Defined

Broad term used to characterize threats targeted to a specific entity or set of entities

Often crafted and executed to purposely be covert and evasive, especially to *traditional* security controls

End goal is most commonly to capture and extract high value information, to damage brand, or to disrupt critical systems

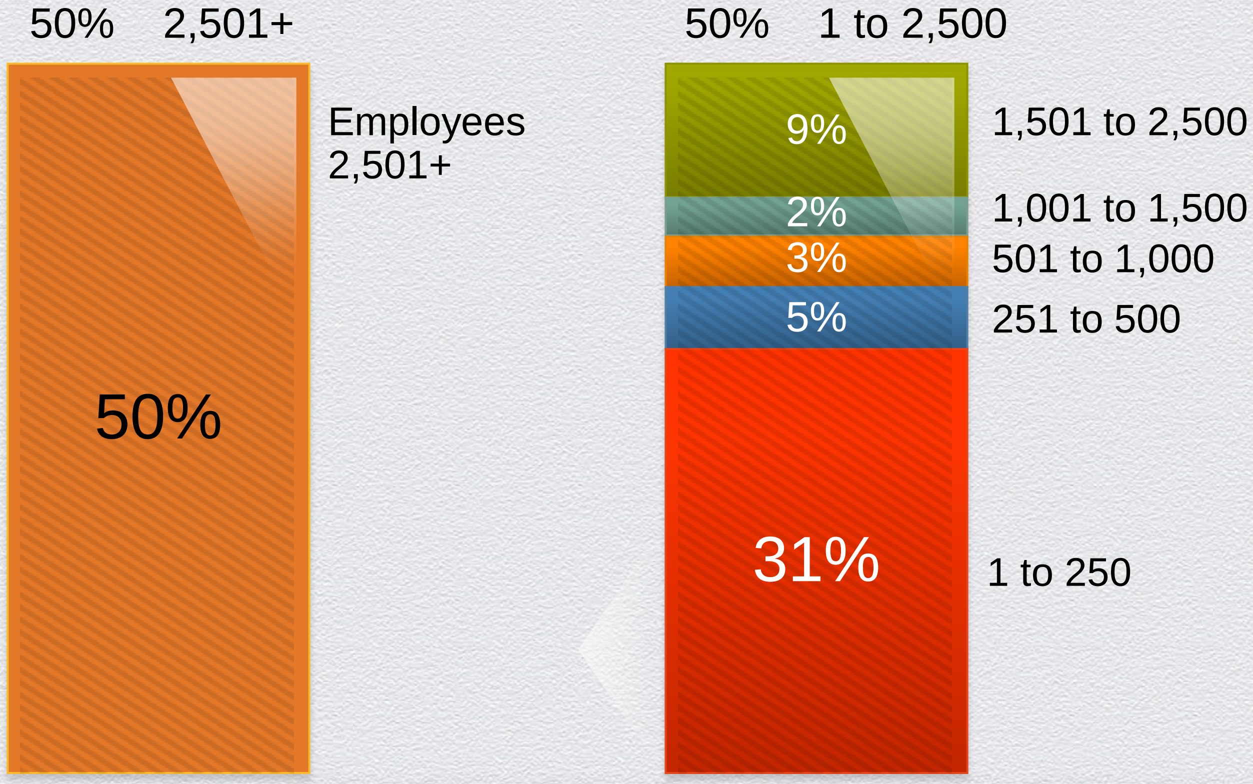
Targeted Attacks: How they Happen

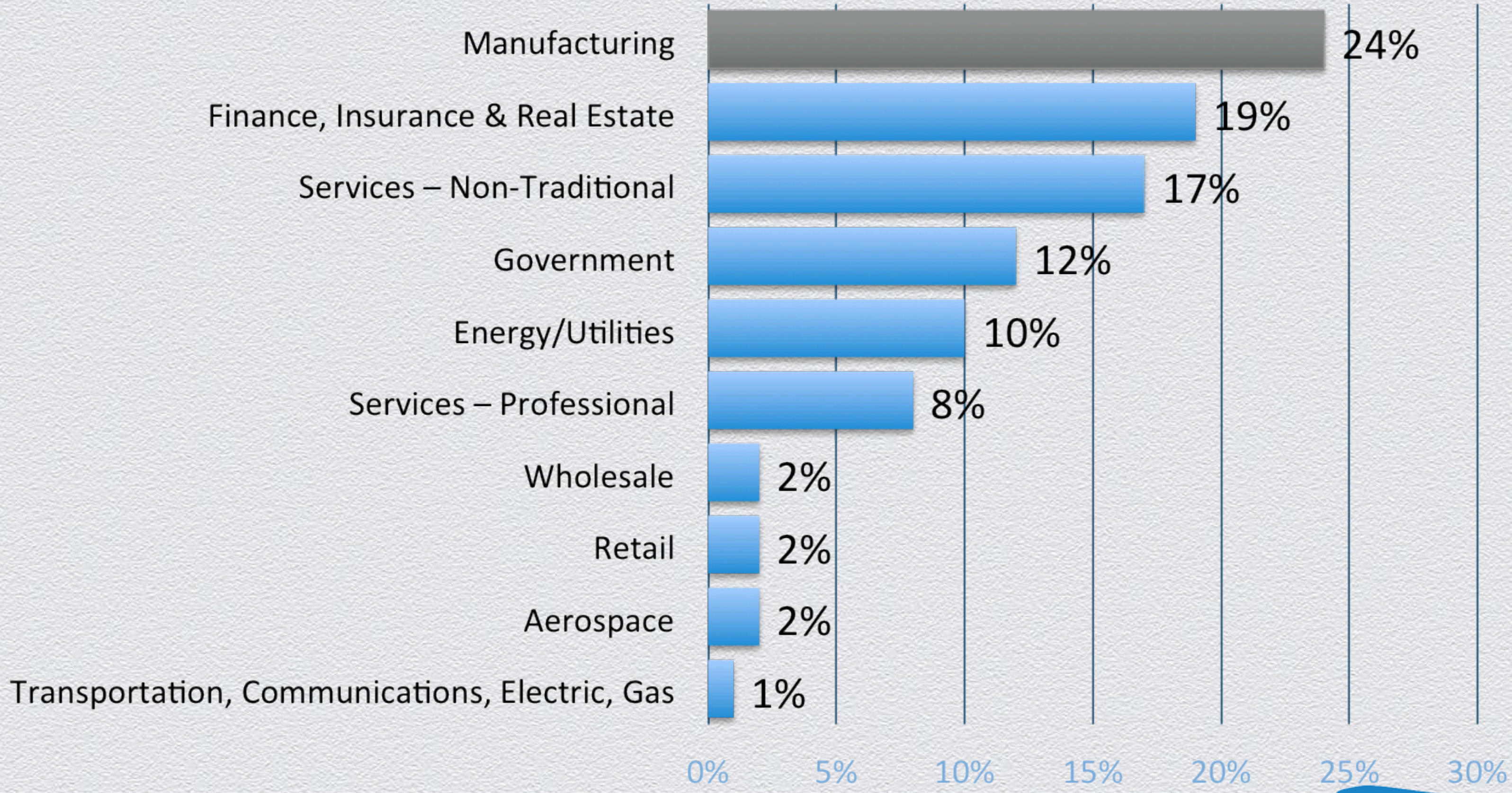
Spear Phishing

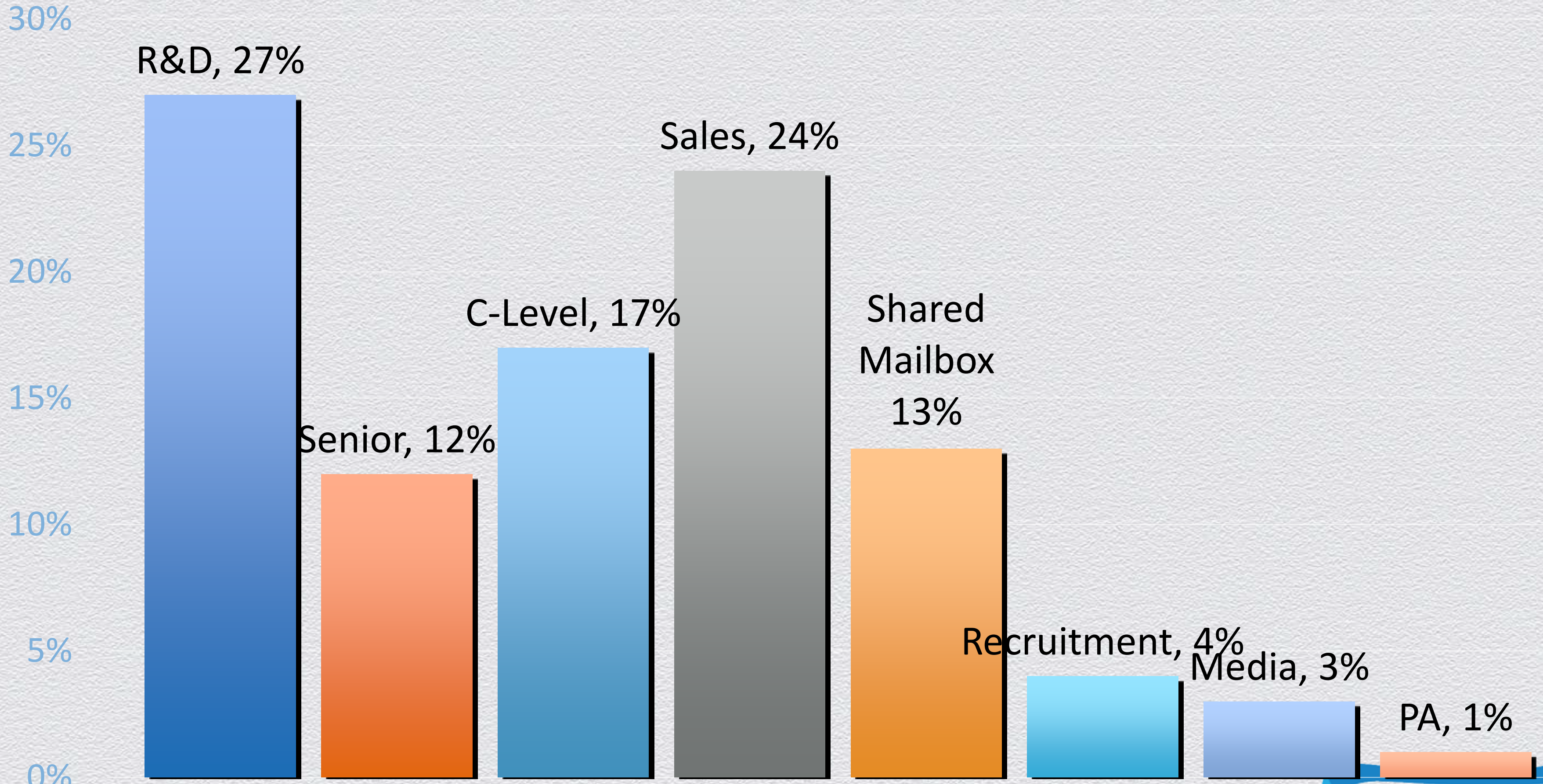
Send an email to a person of interest

Watering Hole Attack

Infect a website and lie in wait for them


50%
2,501+
50%
Employees
2,501+
50%
1 to 2,500
9%
1,501 to 2,500
2%
1,001 to 1,500
3%
501 to 1,000
5%
251 to 500
31%
1 to 250


Manufacturing
24%
Finance, Insurance & Real Estate
19%
Services – Non-Traditional
17%
Government
12%
Energy/Utilities
10%
Services – Professional
8%
Wholesale
2%
Retail
2%
Aerospace
2%
Transportation, Communications, Electric, Gas
1%
0%
5%
10%
15%
20%
25%
30%


30%
25%
20%
15%
10%
5%
0%
R&D, 27%
Senior, 12%
C-Level, 17%
Sales, 24%
Shared Mailbox 13%
Recruitment, 4%
Media, 3%
PA, 1%

Symantec.

Organizations Are Struggling to Keep Up

Reliance on Silver Bullet Technologies

- A single point product won’t identify all threats
- Most frequent Silver Bullet monitoring technologies:
  - IDP / IPS
  - Anomaly detection (on the rise)
- Individual technologies lack a comprehensive vantage point to detect today’s threats.

32%

Average % of incidents detected by IDP / IPS technologies

Incomplete Enterprise Coverage

- Companies fail to effectively assess (and update) the scope of their Enterprise
- Enterprise technology trends further challenge scope
  - Mobile
  - Cloud
  - BYOD

Underestimate SIEM Complexity

- Companies frequently underestimate effort and cost to implement
  - Technical architecture frequently under scoped
  - Time to implement can take year+
- Struggle to sustain capability
  - Turnover of “the SIEM expert”
  - Focus / Expertise Required

72%

Collect 1TB of security data or more on a monthly basis

35%

Too many false positive responses

Symantec.

Lack of Sufficient Staff / Expertise

"CISOs have become accustomed to taking on more responsibilities without corresponding growth to their resource levels." – Forrester

"Recruitment specialists report increasing difficulty sourcing [information security] candidates." – Forrester

"We're at 100% employment in IT security"
– Chief Security Officer Health Care Organization

"CISOs will not be able to hire their way out of security analytics problems"
– Enterprise Security Group, March 2013

83%

of enterprise organizations say it's extremely difficult or somewhat difficult to recruit/hire security professionals

Can’t Keep up with Global Threats

- Detection program must be evolve as threats evolves
  - Analyst training / awareness
  - SIEM tuning
  - Detection methods
  - Response tactics
- Varied tactics to keep up with threats:
  - Open source
  - Commercial

28%

Sophisticated security events have become too hard to detect for us

35%

Do not use external threat intelligence for security analytics

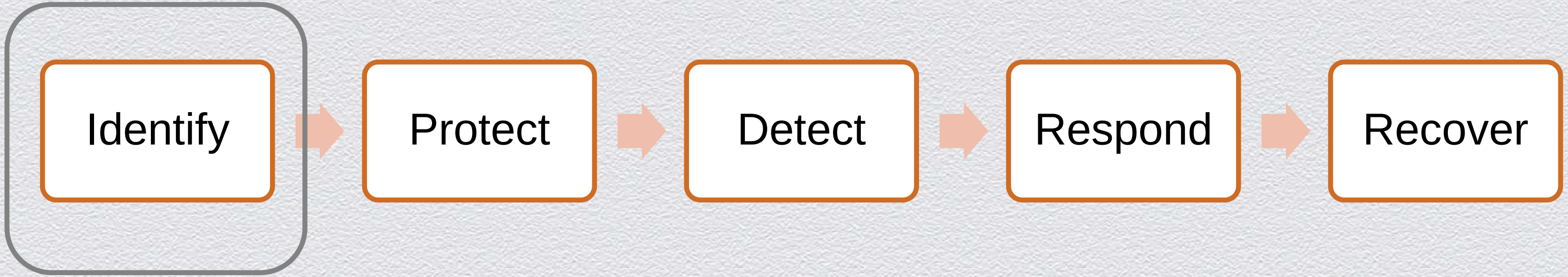
RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Stopping Targeted Attacks

THE WHITE HOUSE
WASHINGTON

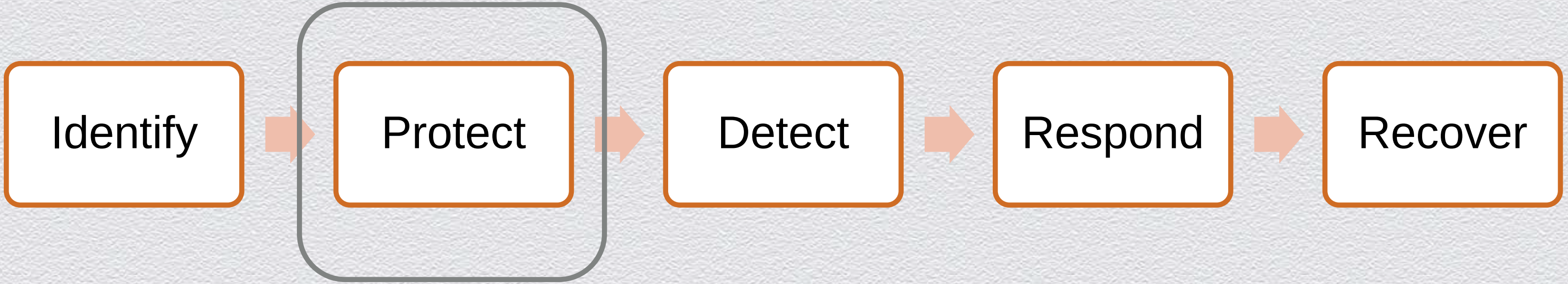
NIST



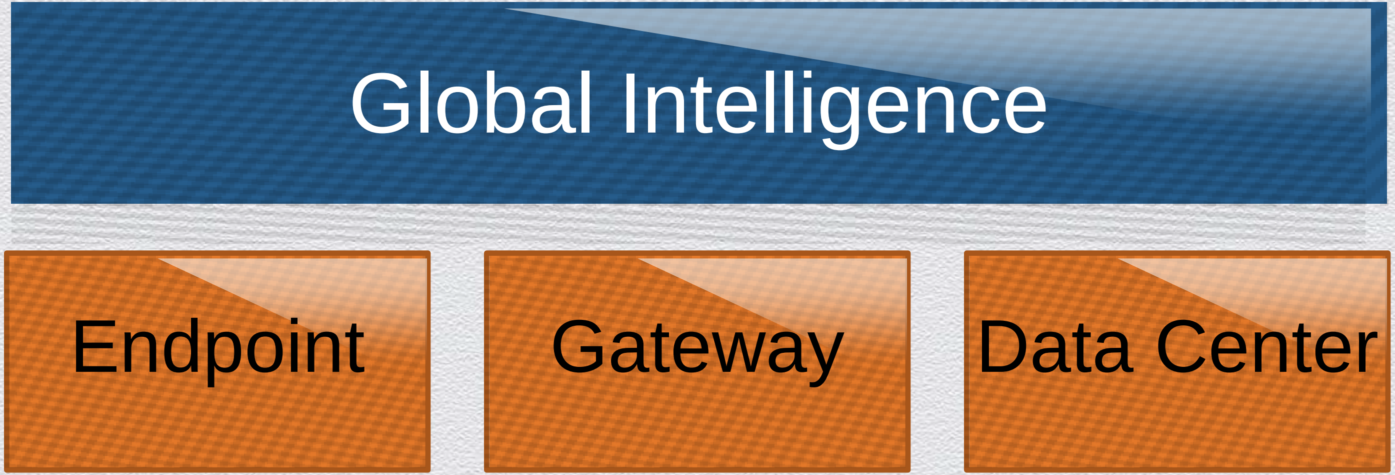
Identify → Protect → Detect → Respond → Recover

THE WHITE HOUSE
WASHINGTON

NIST



Protect Against Targeted Attacks Today



Global Intelligence

Endpoint

Gateway

Data Center

An Example of Global Intelligence

7 Billion

File, URL & IP Classifications

1 Billion+

Devices Protected

2.5 Trillion

Rows of Security Telemetry

550

Threat Researchers

240 Million+

Contributing Users & Sensors

14

Operations & Response Centers

All Security Telemetry in One Place

File/user/site associations

- Hygiene
- Parent program
- File name/path

File hash
IP/URL
Machine ID

File heuristics

- Instruction use
- File structure
- Digital signature

File hash
□
Machine ID

Behavior heuristics

- Has a GUI
- Settings changes
- In program menu

File hash
IP/URL
Machine ID

Industry feeds

- Vendor A sent us this file

File hash
□
□

Spam/phishing traffic

- IP address Y sends spam

□
IP/URL
□

Network traffic

- IP source
- IP destination
- Vulnerability ID

File hash
IP/URL
Machine ID

SSL certification

- Domain
- Level of VeriSign SSL certification

□
IP/URL
□

Honeypot sensors

- Suspicious traffic from IP address X

File hash
IP/URL
Machine ID

Web site details

- Popularity
- PII fields
- Site age

□
IP/URL
Machine ID

Endpoint

NETWORK

Block attacks before they arrive on the computer

REPUTATION

Automatically determine safety of files and web sites using the "wisdom of crowds"

BEHAVIORS

Watch programs as they run and blocks suspicious behaviors

Gateway

Identify Anomalies

Determine the True Destination of a URL

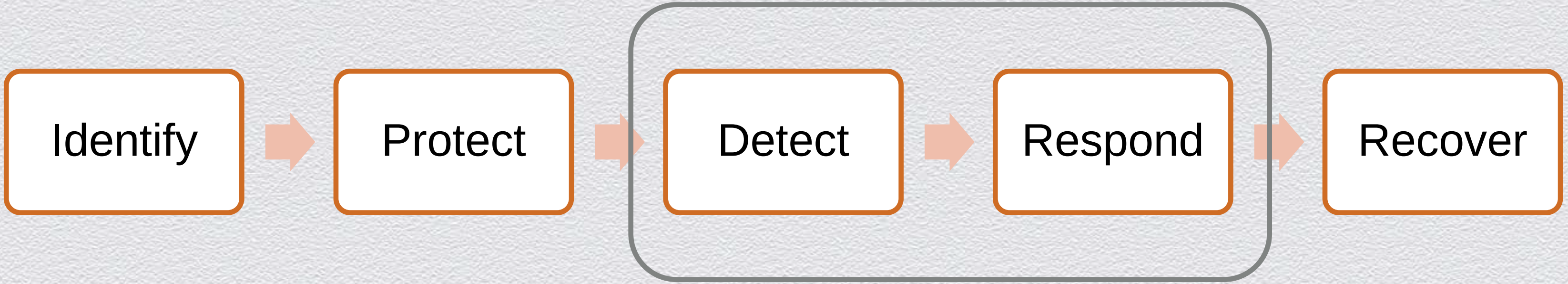
Strip Active Content from Attachments

Data Center

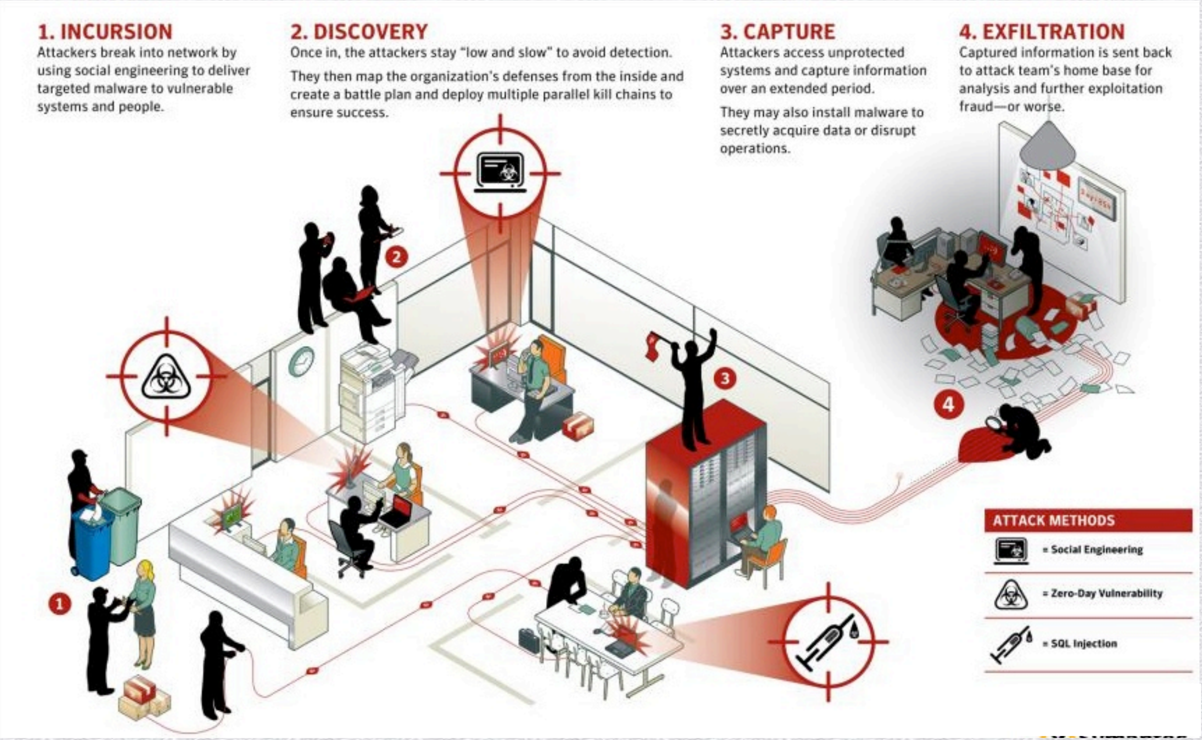
- Least Privilege Access Control
- File Integrity Monitoring
- Server Hardening

THE WHITE HOUSE
WASHINGTON

NIST



Targeted Attacks: How they Work



1. INCURSION
Attackers break into network by using social engineering to deliver targeted malware to vulnerable systems and people.

2. DISCOVERY
Once in, the attackers stay "low and slow" to avoid detection.

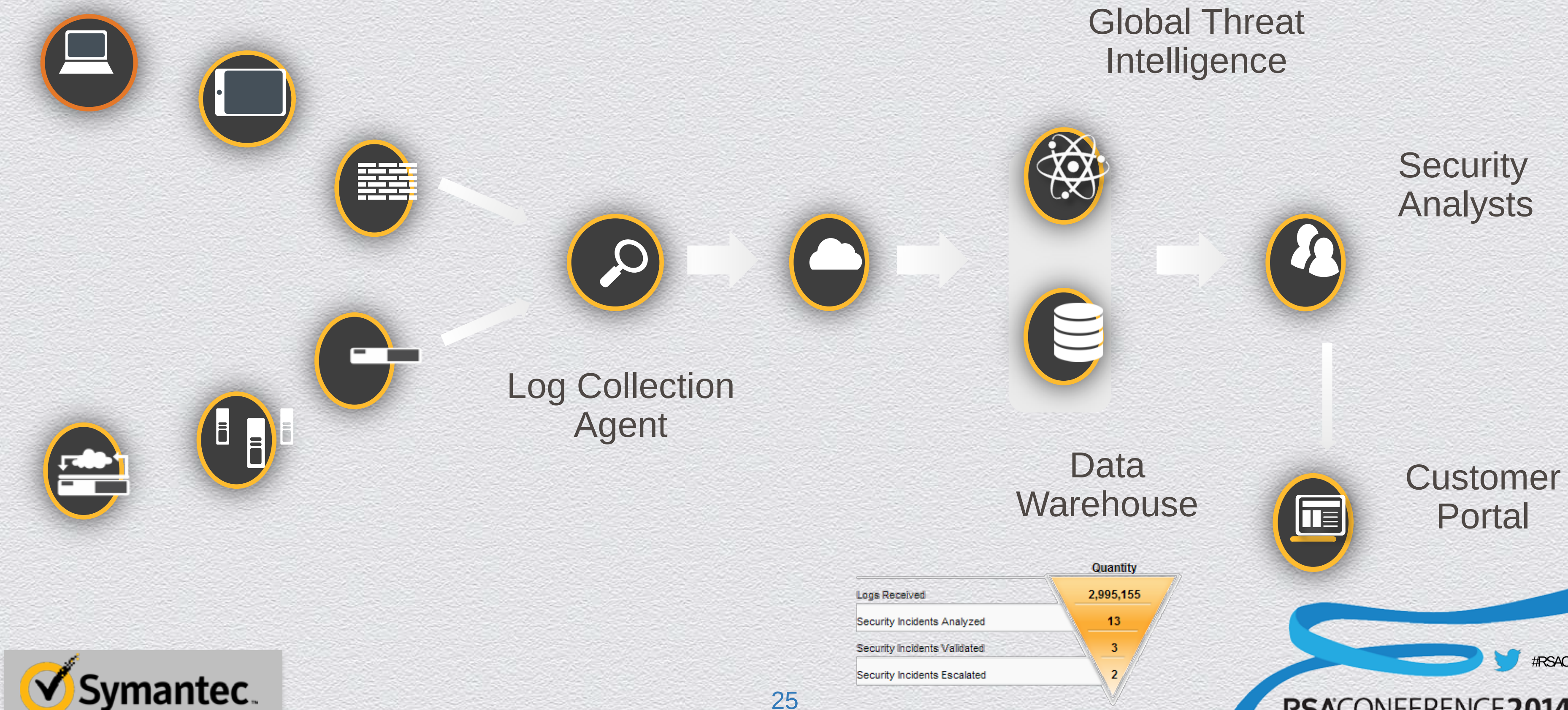
They then map the organization's defenses from the inside and create a battle plan and deploy multiple parallel kill chains to ensure success.

3. CAPTURE
Attackers access unprotected systems and capture information over an extended period.

They may also install malware to secretly acquire data or disrupt operations.

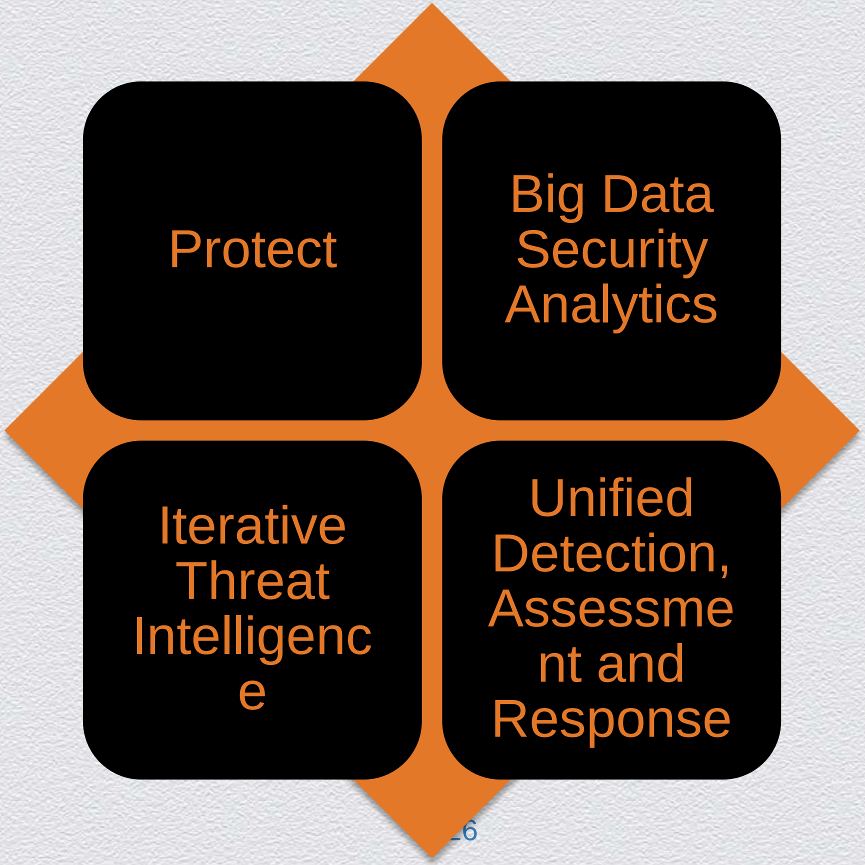
4. EXFILTRATION
Captured information is sent back to attack team's home base for analysis and further exploitation fraud—or worse.

How Managed Security Services Works



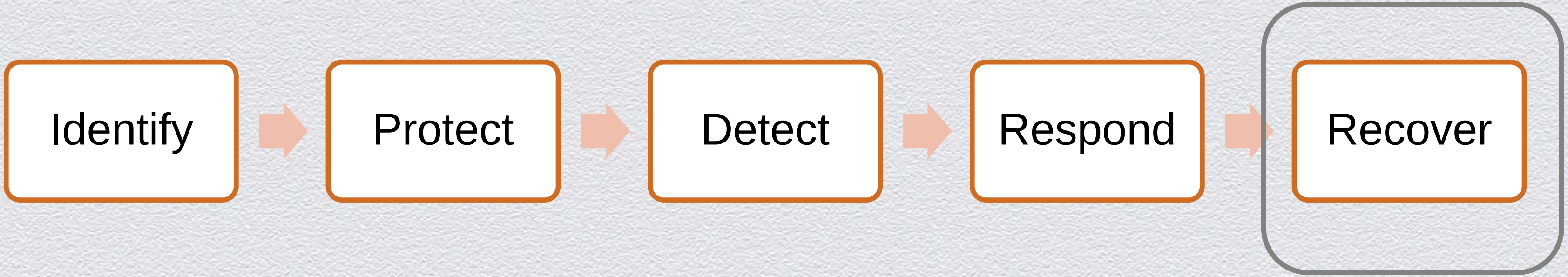
	Quantity
Logs Received	2,995,155
Security Incidents Analyzed	13
Security Incidents Validated	3
Security Incidents Escalated	2

The Future of Detect & Respond

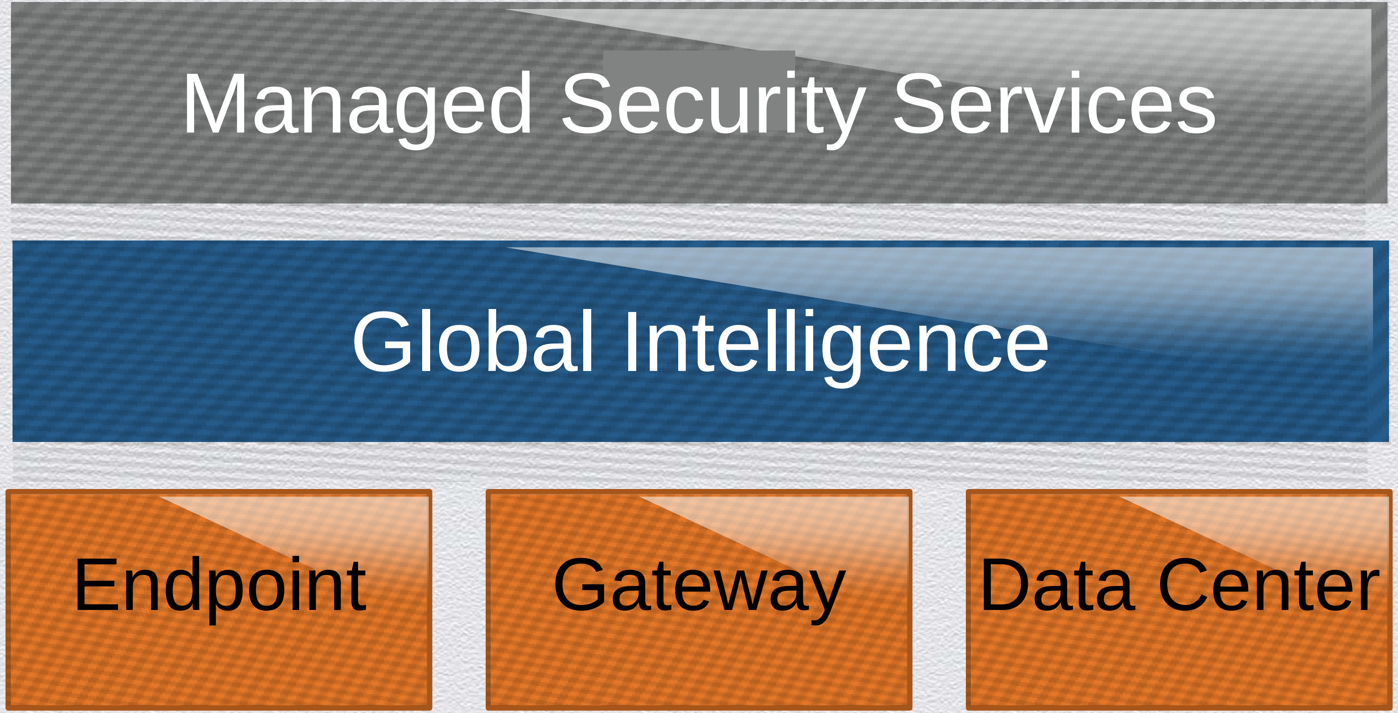

Protect
Big Data Security Analytics
Iterative Threat Intelligence
Unified Detection, Assessment and Response

THE WHITE HOUSE
WASHINGTON

NIST



How Symantec Can Help



Managed Security Services

Global Intelligence

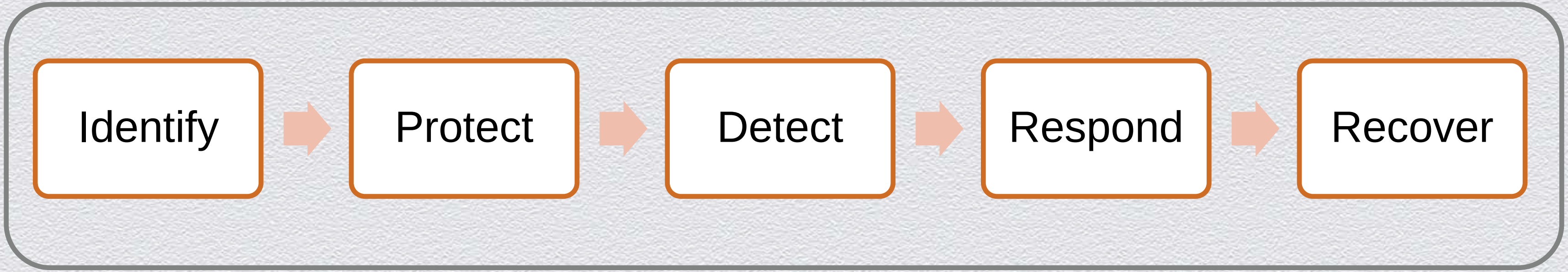
Endpoint

Gateway

Data Center

THE WHITE HOUSE
WASHINGTON

NIST


Identify → Protect → Detect → Respond → Recover

Thank You!

Come Visit Symantec in North Hall Booth #2803