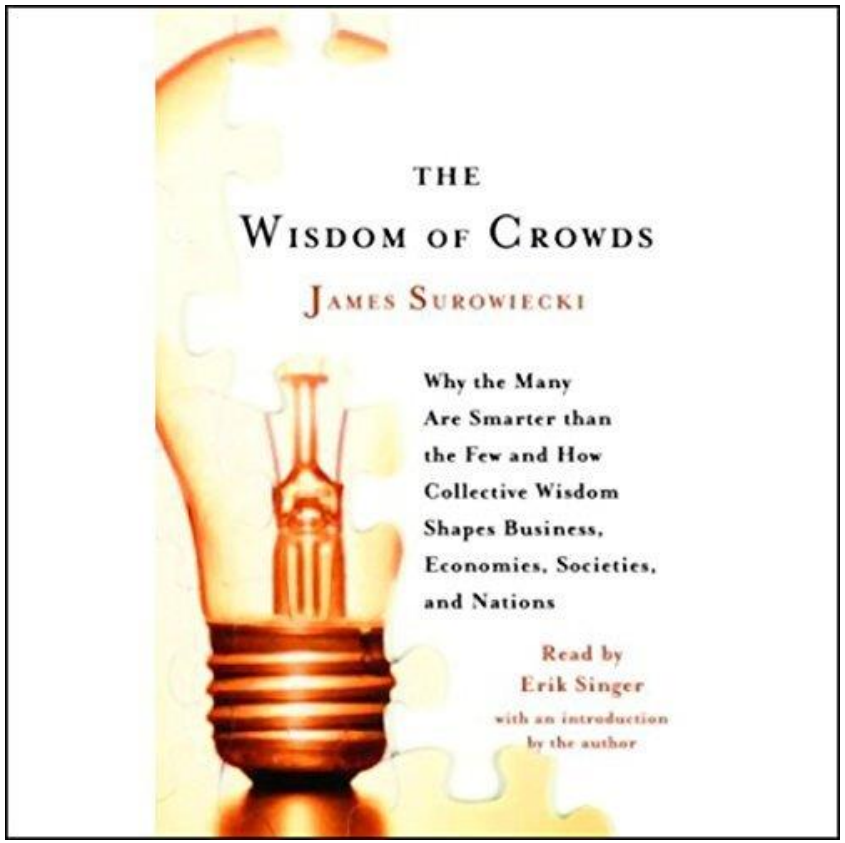
Crowd Sourced Security

Applying the Wisdom of the Crowd to Cyber Defenses

John ‘Lex’ Robinson
Anti-Phishing / Cyber Security Strategist

COFENSE.COM

The Wisdom of Crowds



A theory which proposes the answers to difficult questions are best reached by **a group of alert, intelligent individuals** rather than by single, even respected, experts alone.

The author highlights **tragedies that could have been avoided** had a greater number of persons been consulted before crucial decisions were made.

COFENSE

The Intelligence Process

Actionable Intelligence consists of bits of data, that when grouped together, reveal trends and a "big picture" of a corner of the world. **The requested data are delivered by a field agent to the case officer.**

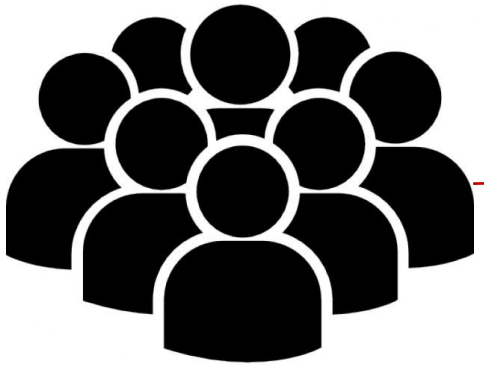
A case officer sometimes has a network of field agents who do his legwork, giving him small bits of information from various sources. An example might be production numbers for several units of a business that's owned by U.S. interests, but operated by the native population in different locations throughout the country.

The case officer assembles these bits of information and either performs his own analysis or sends them to the U.S., **where other analysts collate them with more data from other case officers and field agents**.

COFENSE

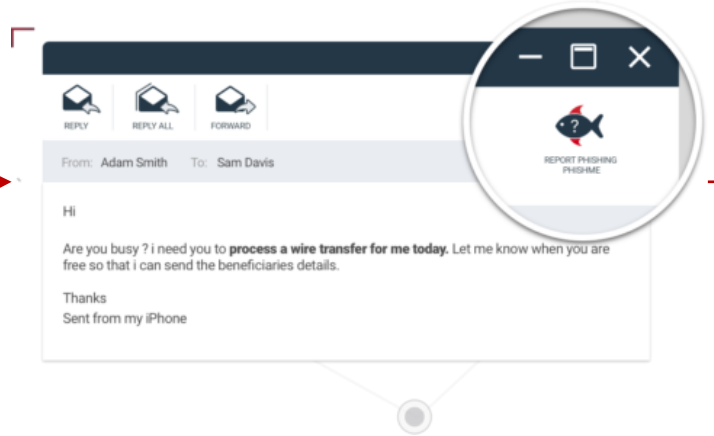
Application to Cyber Security

User Recognition



A group of alert, intelligent individuals…

Reporting Capability



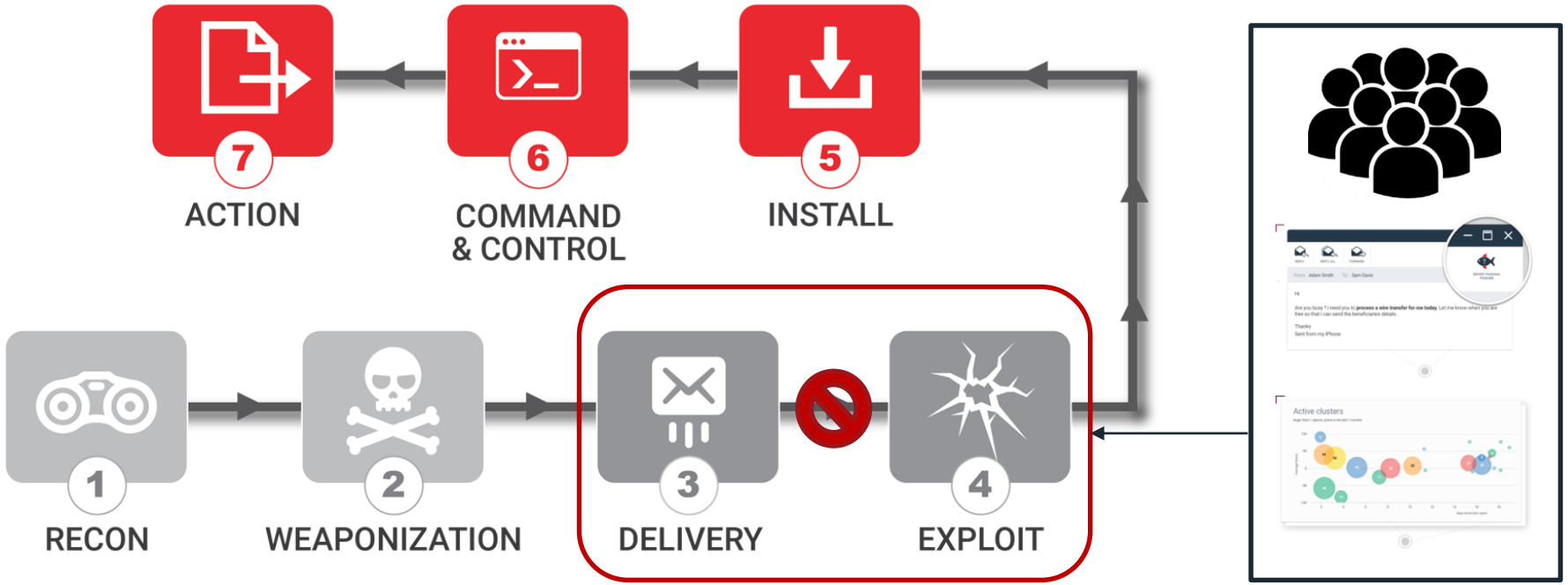
The requested data are delivered to experienced incident responders…

Advanced Analysis and Resolution

Collated data is analyzed and acted upon to avoid breaches.

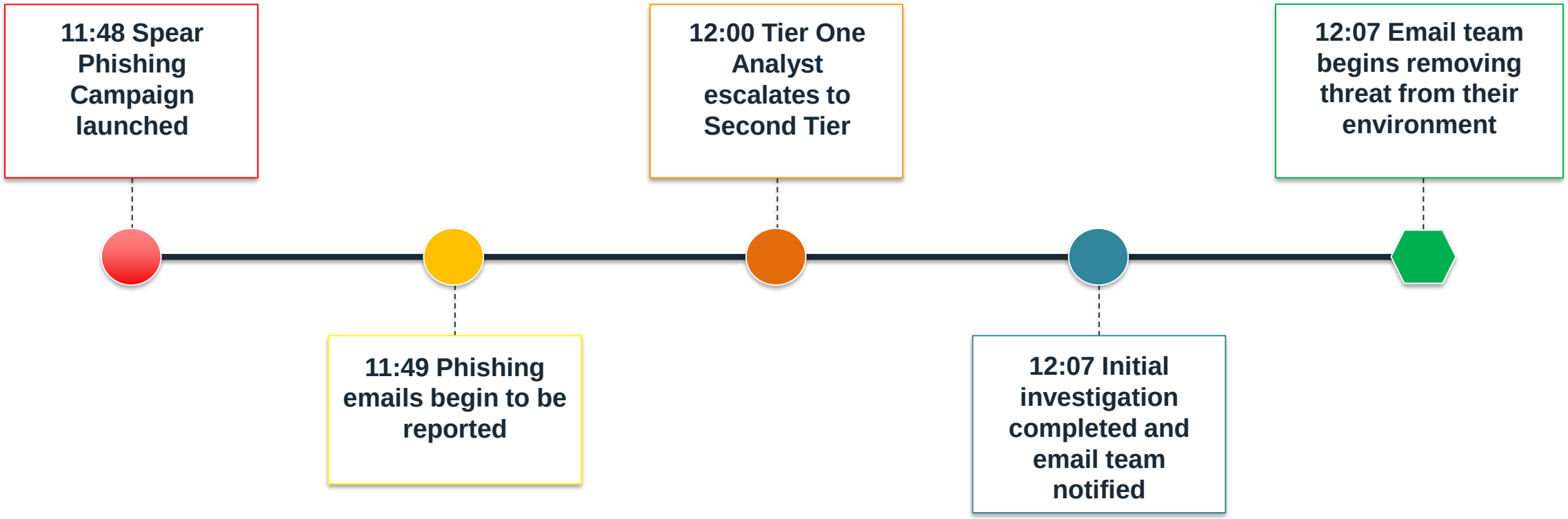
COFENSE

The Cyber Kill Chain



NOTE: With development of crowd sourced intelligence capabilities, it's possible to get 'Left of Breach'

Use Case - Minutes, Not Months



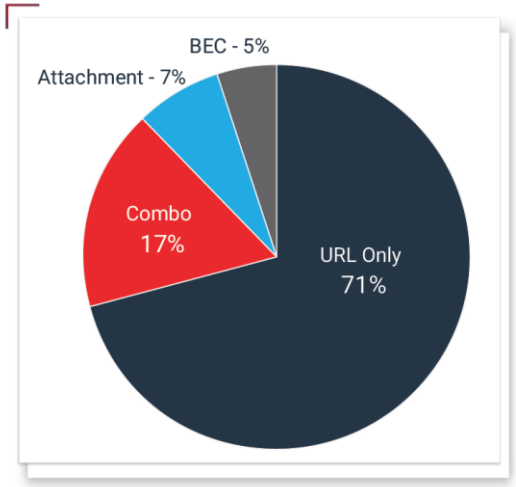
NOTE: Median time for internal discovery of breach is 80 days and external discovery is 107 days

COFENSE

DOES YOUR ORGANIZATION HAVE THE CAPABILITY TO RESIST AN ACTIVE PHISHING THREAT?

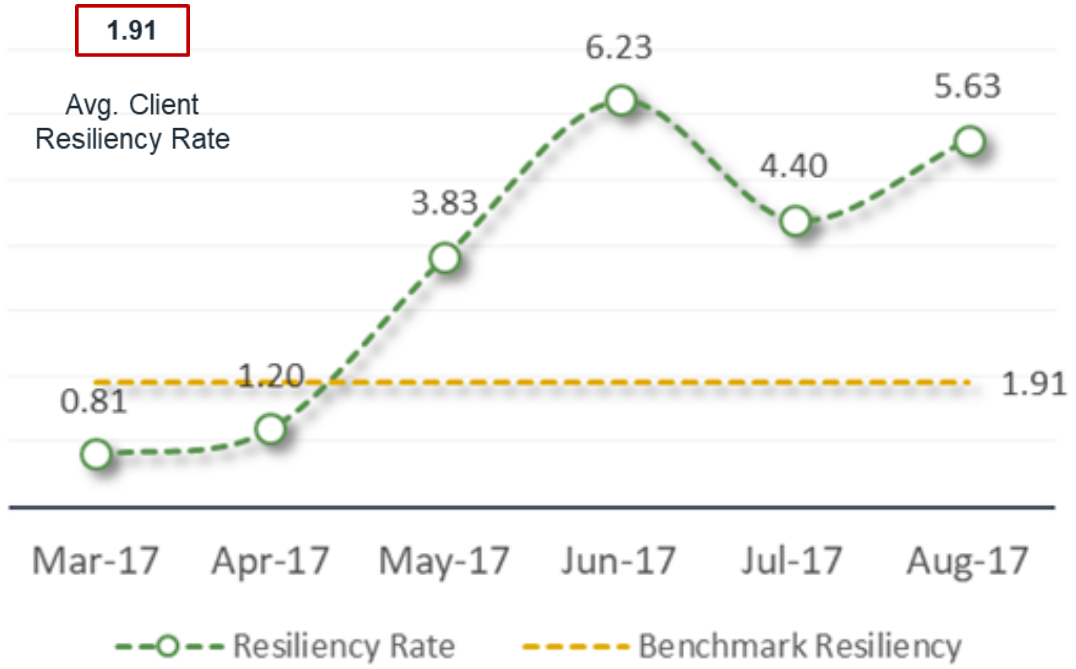
WHAT YOU NEED TO KNOW

Active Threats



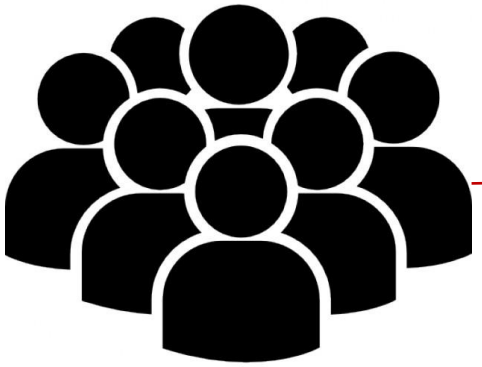
Understand how your organization is being attacked and model as simulations in your anti-phishing program

Recognition and Reporting Capability



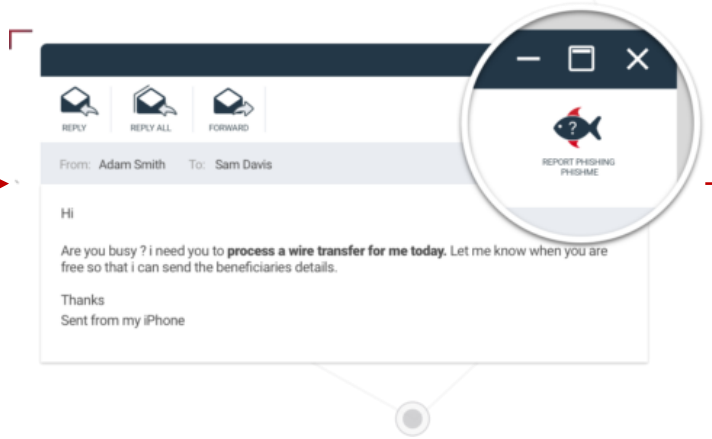
Developing Crowed Sourced Capabilities

User Recognition



Help your users recognize active threats through immersive simulations.

Reporting Capability



Provide users an automated reporting process to ensure appropriate collection of data.

Advanced Analysis and Resolution

Enable incident responders with solutions that prioritize data for analysis and assist the mitigation process.

COFENSE

Program Best Practices

1) Be transparent with your users – encourage self reporting
2) Focus measures on recognition and reporting – NOT susceptibility
3) Be consistent with presentation of active threat simulations
4) Enable in-line analysis and mitigation capabilities

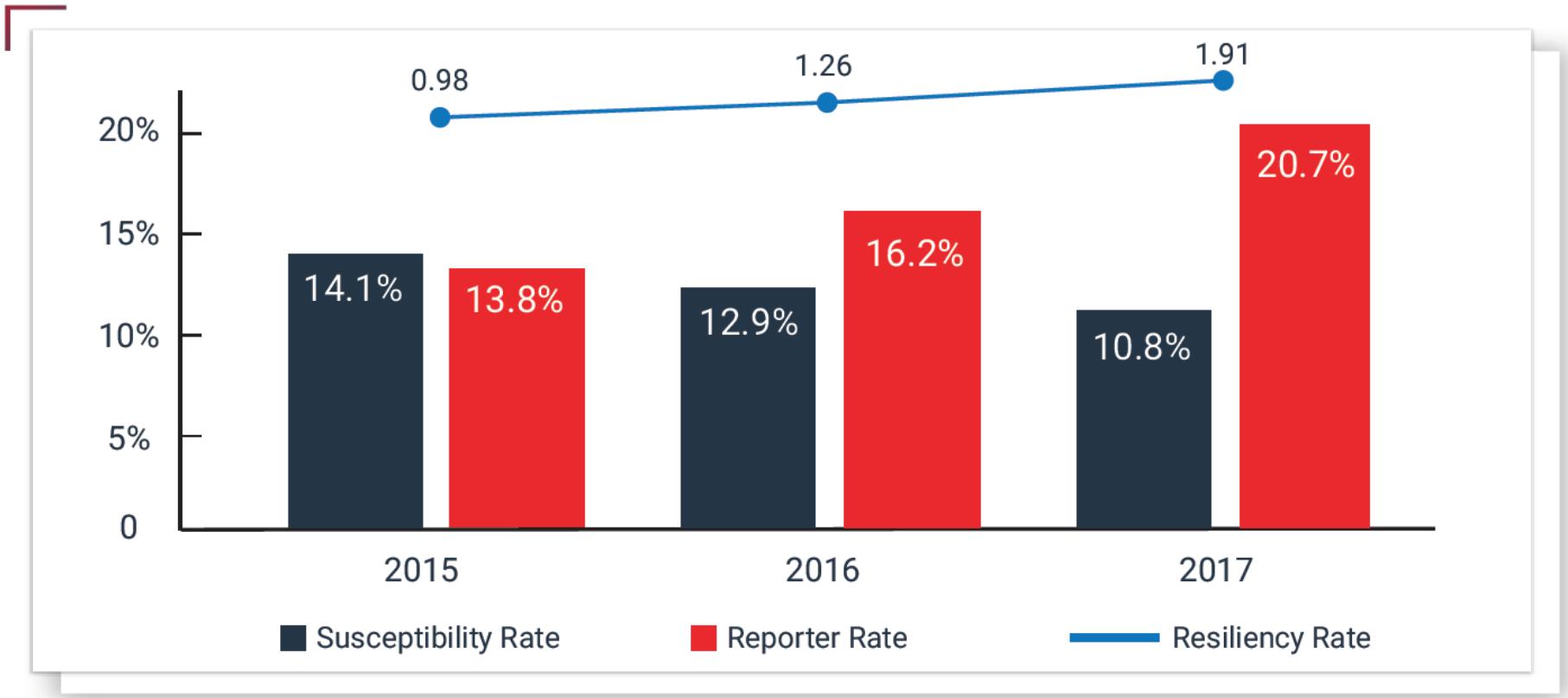
Encourage Self Reporting

Behavior Analysis

Reported	Response	Behavior	Count	%	Description
Did Not Report	Opened the Attachment (Did not Report)	Undesirable	76	14.23%	User viewed the phishing email then clicked the scenario link
	Viewed Email (Did not Report)	Neutral	0	0.00%	User viewed the phishing email but did not report the email
No Action	No Response	Neutral	213	39.89%	Due to technical restrictions, we were unable to track these users.
Reported	Responded and Reported	Desirable	12	2.25%	User fell susceptible for the phishing email but did report it
	Reported Only	Very Desirable	233	43.63%	User viewed the phishing email and reported it
		Total	534		

Note: Because reporting is the behavior you want to increase, focus on those that fall susceptible and don't report.

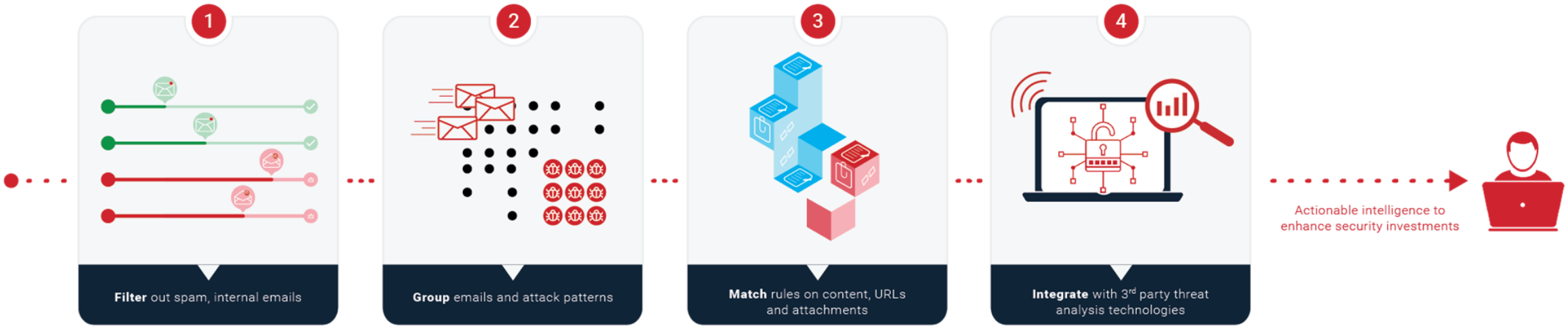
Consistency Drives Capability



Note: Trend recognition and reporting capabilities over time.

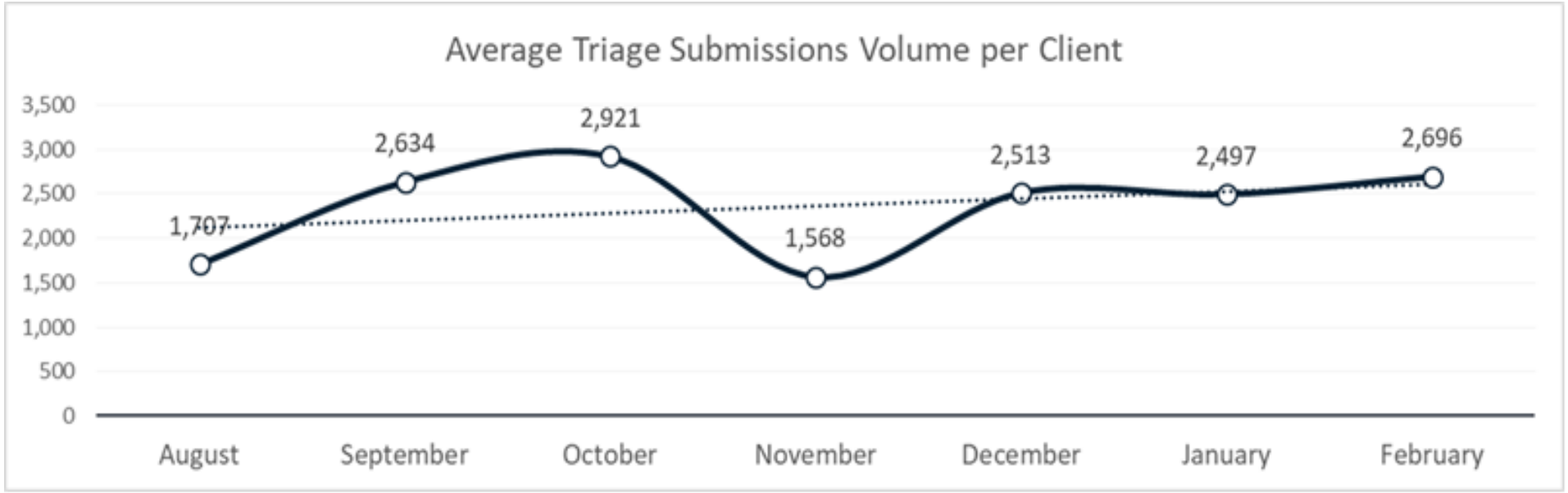
COFENSE

Enable In-Line Incident Response



DEVELOPING RECOGNITION, REPORTING AND RESOLUTION CAPABILITIES LEADS TO MITIGATION OF ACTIVE THREATS

The Value of the Crowd



NOTE: As of February 2018, users across 30 organizations were reporting ~ 2,500 potential threats. Of these the percentage of malicious emails ranged from 10-12%. That is roughly 250 malicious (mitigated) emails making it past perimeter defenses (per month / per company).

RELATED RESOURCES

- Check out our weekly blog @ phishme.com/blog
- Threat alerts – sign up for them @ phishme.com/threat-alerts
- Phishing Defense & Resiliency Report @ phishme.com/whitepaper/enterprise-phishing-resiliency-and-defense-report/

COFENSE