

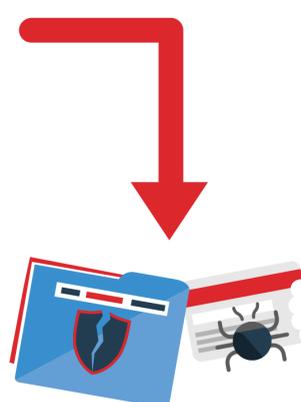
# Why Human-vetted, Phishing-specific Threat Intelligence Is Best



## The Problem

### Machine Data is Unreliable

Threat data collected and produced only by machines can be overwhelming, nonspecific and unreliable. It wastes time, resulting in negative consequences.



### Lack of Established Course of Action

Time is wasted thinking about what to do next because responders lack an established course of action.



### Longer Attacks, More Damage

The longer attackers have access to your network, the more damage they can do.

When the threat actor is already inside your defenses, they can be quite a challenge to detect—and most of the incidents are still taking months and years to discover.”

Verizon, "2017 Data Breach Investigations Report," 10th Edition, 2017.

## The Solution

Human-vetted, phishing-specific intelligence provides the most actionable data. Cofense security specialists enrich and verify threat data. Their analysis turns threat data into threat intelligence available in multiple formats, including machine-readable reports. Context/enrichment is an attribute of our intelligence that stands on its own.

Actionable intelligence is:

### Consumable

It's easy to use.

### Accurate

It's correct.

### Timely

It allows you to find malware quickly.

### Relevant

It yields detailed information about specific threats.

Having actionable data early can dramatically:

Reduce time to discover a threat

Quantify risk to the organization

Optimize a response for rapid remediation

Minimize attack damage and costs

## Phishing Stats

### 9 out of 10

Data breaches used phishing as the attack vector<sup>1</sup>

### 66 Days

Mean time to contain an attack<sup>2</sup>

### 191 Days

Mean time to identify a security breach<sup>3</sup>

### \$3.62 million

Average cost of a breach<sup>4</sup>

To learn more about why human-vetted, phishing-specific threat intelligence is best, read the white paper, **“Reducing Risk with Intelligence.”**

#### Sources

- 1 Cofense: "2016 Enterprise Phishing Susceptibility and Resiliency Report," 2016.
- 2 Ponemon Institute: "2017 Ponemon Cost of Data Breach Study," sponsored by IBM, June 2017.
- 3 Ibid.
- 4 Ibid.

