



BISHOPFOX

EVOLVING

# ADVERSARY SIMULATION

PRESENTED

NOVEMBER 6, 2018

# THE REALITY OF DATA BREACHES

DATA RECORDS COMPROMISED IN FIRST HALF OF 2018

3,353,172,708

18,525,816  
records lost or stolen  
every day



771,909  
records  
every hour



12,865  
records  
every minute



214  
records  
every second

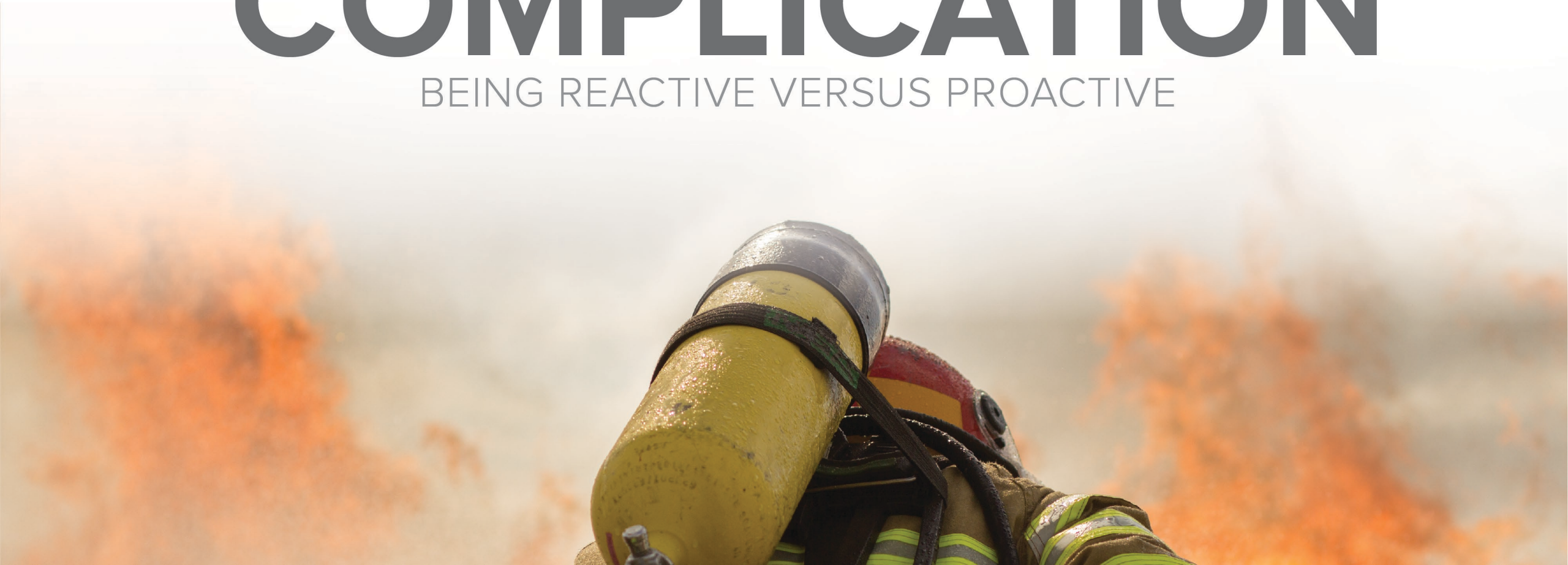




HOW DO WE FIX THIS

# COMPLICATION

BEING REACTIVE VERSUS PROACTIVE





Q

HOW CAN  
WE IMPROVE  
SECURITY  
POSTURE?



# RED TEAMING

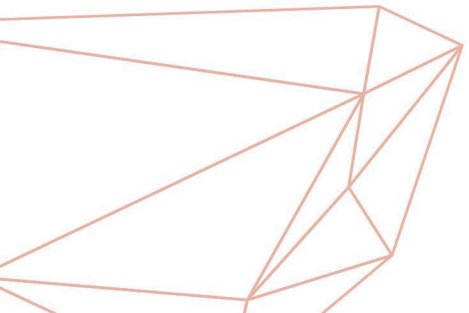
SIMULATING AN ADERSARY TO  
IMPROVE SECURITY POSTURE

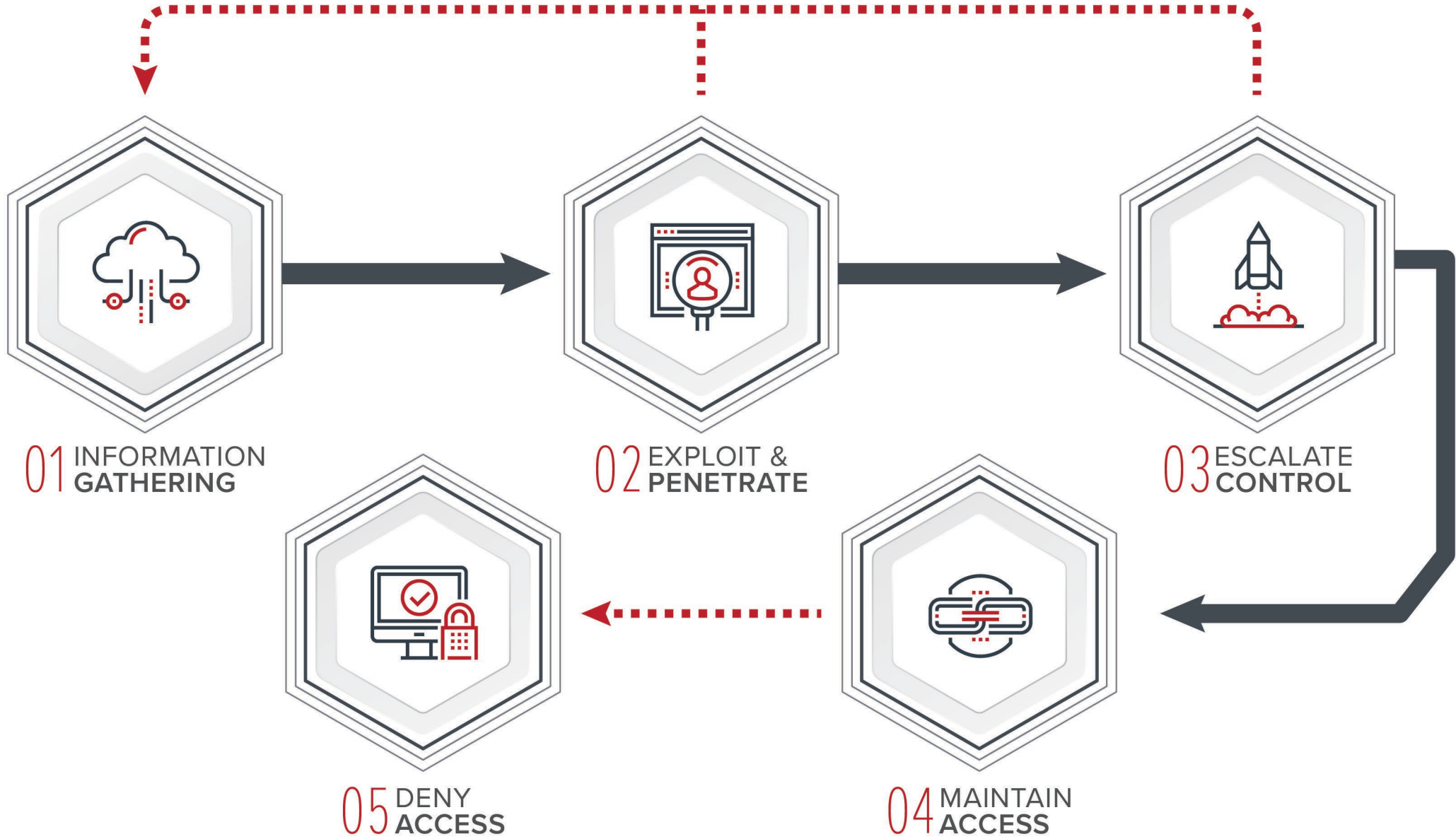


THIS IS  
HOW YOU'LL  
**BE HACKED**

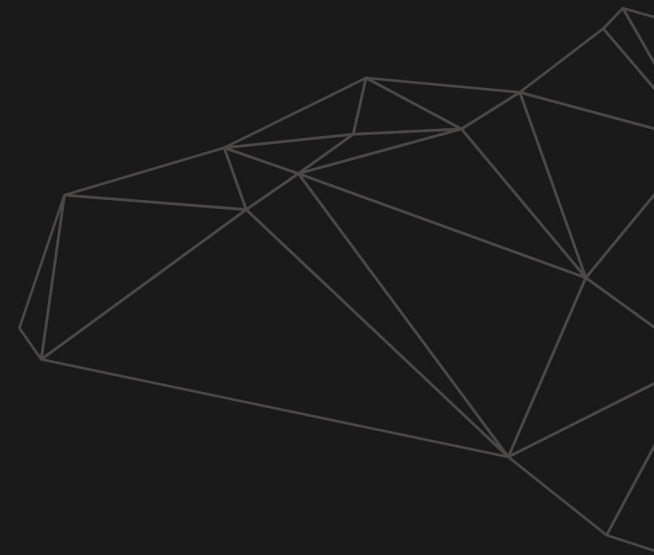


From an **offensive** perspective,  
every “security incident”  
reveals an **attack roadmap.**



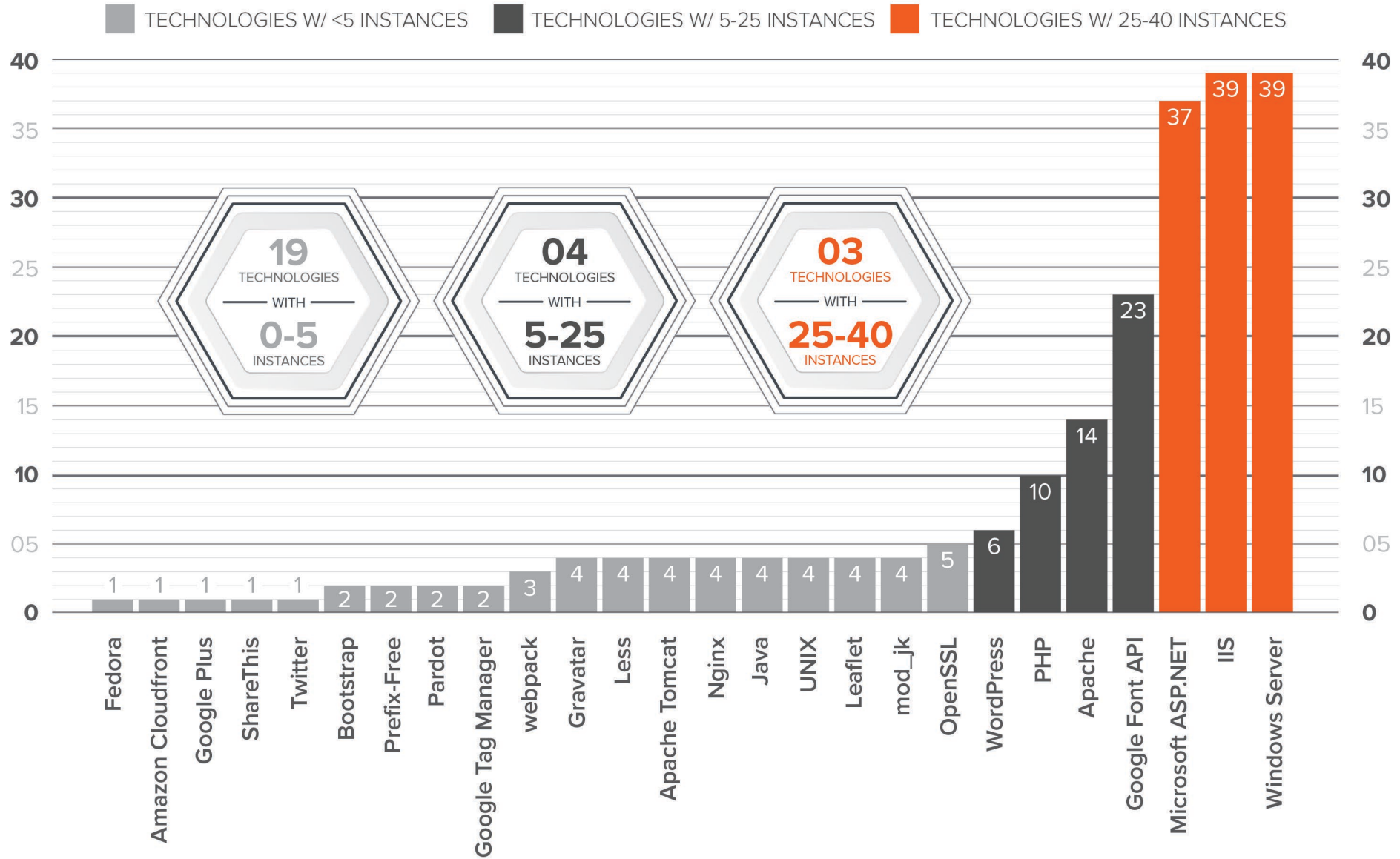







# THE 5 AVENUES OF ATTACK

# PLI TECHNOLOGIES





**'You can sit in your seat or you can be left behind'**  
A man who says his seat was caked with feces alleges that a Delta flight attendant responded by giving him paper towels and a bottle of gin. 'Dehumanizing' »  
4225 people reacting

**10 female candidates to watch on Election Day**  
**It's Election Day: Will your vote count?**  
**Viewer's guide to the 2018 election**  
**USOC deals nuclear blow to USA Gymnastics**  
**Pamela Anderson trashes #MeToo movement**

**Sinead O'Connor: "Truly I never wanna spend time with white people again"**  
The Irish singer-songwriter tweets about Donald Trump, non-Muslims, and society's perceptions on Islam.  
1570

**Khloe Kardashian Rocks String Thong in Sexy Shoot After Tristan Thompson Cheating Episode of 'KUWTK'**  
Khloe showed off her fit post-baby body in the sexy photos.  
269

- Trending Now**
1. Steve Kazee
  2. Bill Schuette
  3. Chris Hemsworth
  4. Hailee Steinfeld
  5. Dentist Near Me
  6. Home Security Ala...
  7. Camila Cabello
  8. Conor McGregor
  9. Honda Pilot
  10. Sophie Turner

**Tempe, AZ**

Today	Wed	Thu	Fri
83° 53°	81° 55°	80° 55°	77° 55°

**Scoreboard** NFL

Last Week	Current Week	Next Week
Tennessee	28	Final Nov 05
Dallas	14	
Oakland	3	Final Nov 01
San Francisco	34	
Chicago	41	Final Nov 04
Buffalo	9	
Kansas City	37	Final Nov 04
Cleveland	21	
NY Jets	6	

# IMPACT // ATTACK

# YAHOO!

## SPEAR PHISHING & CYBER KILL CHAIN

### ATTACK

- Spear Phishing
- Poor Network Security

### IMPACT

- 3 Billion Records (PII)
- Verizon Acquisition = (\$350 Million)



# THE CIA'S COMMUNICATIONS SUFFERED A CATASTROPHIC COMPROMISE

## AND IT ALL STARTED WITH A **MISCONFIGURATION**

---

IN FACT, THE IRANIANS USED GOOGLE  
TO IDENTIFY THE WEBSITE  
THE CIA WAS USING TO  
COMMUNICATE WITH AGENTS.

---

---

“IT WAS NEVER MEANT TO BE USED LONG  
TERM FOR PEOPLE TO TALK TO SOURCES.  
THE ISSUE WAS THAT IT WAS WORKING  
WELL FOR TOO LONG, WITH TOO  
MANY PEOPLE. BUT IT WAS  
AN ELEMENTARY SYSTEM.”

- Former U.S. official

---

---

“YOU START THINKING TWICE ABOUT  
PEOPLE, FROM CHINA TO RUSSIA TO  
IRAN TO NORTH KOREA,” SAID  
THE FORMER SENIOR OFFICIAL. THE CIA  
WAS WORRIED ABOUT ITS NETWORK  
“TOTALLY UNWINDING WORLDWIDE.”

---

INSECURE APPLICATION

# FACEBOOK

IMAGEMAGICK // IMAGETRAJIK

FAILED TO PATCH  
KNOWN IMAGEMAGICK  
FLAW FOR MONTHS



DISLIKE





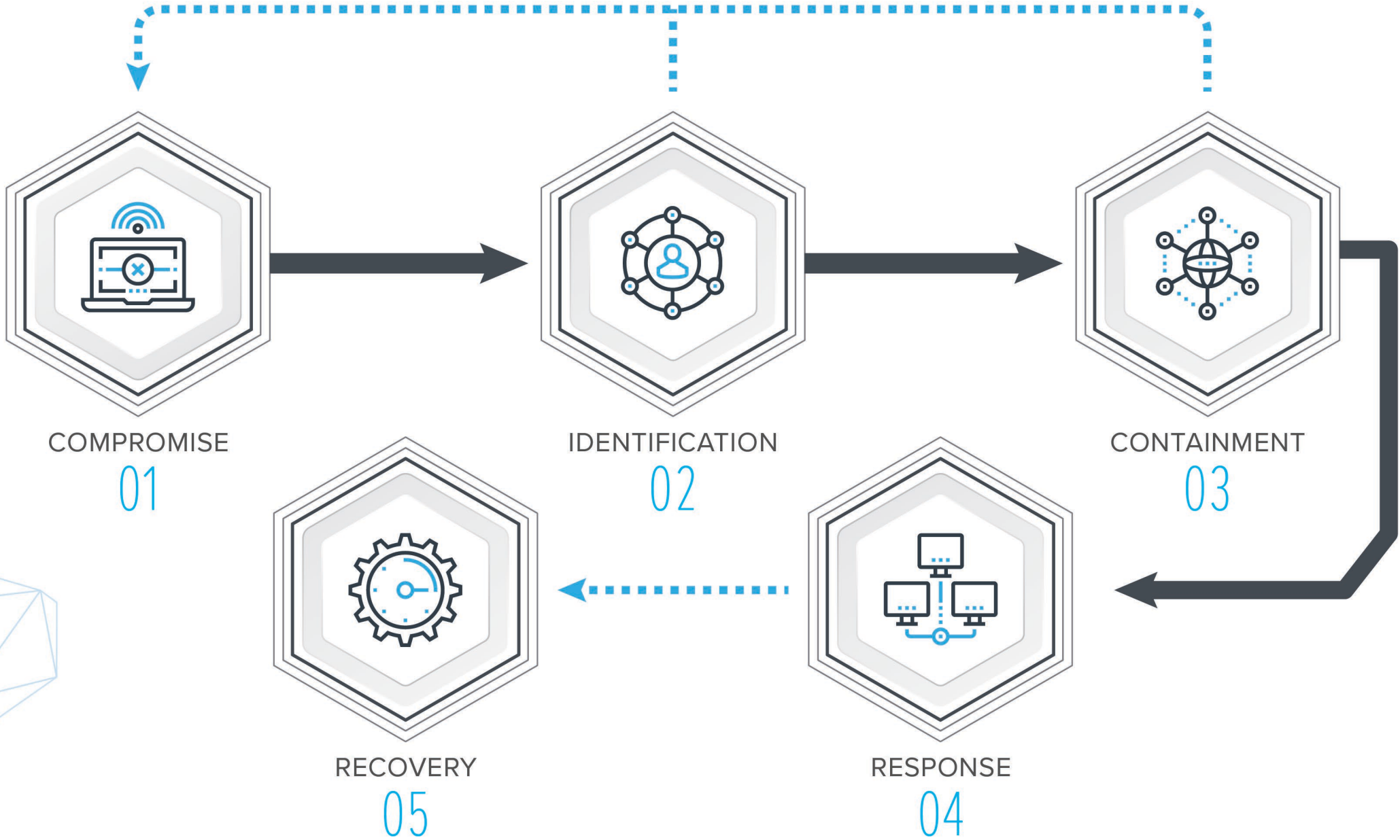
# HOW TO DEFEND YOUR DEFENSES





From a **defender's** perspective,  
every “security incident” reveals  
an **opportunity to improve.**



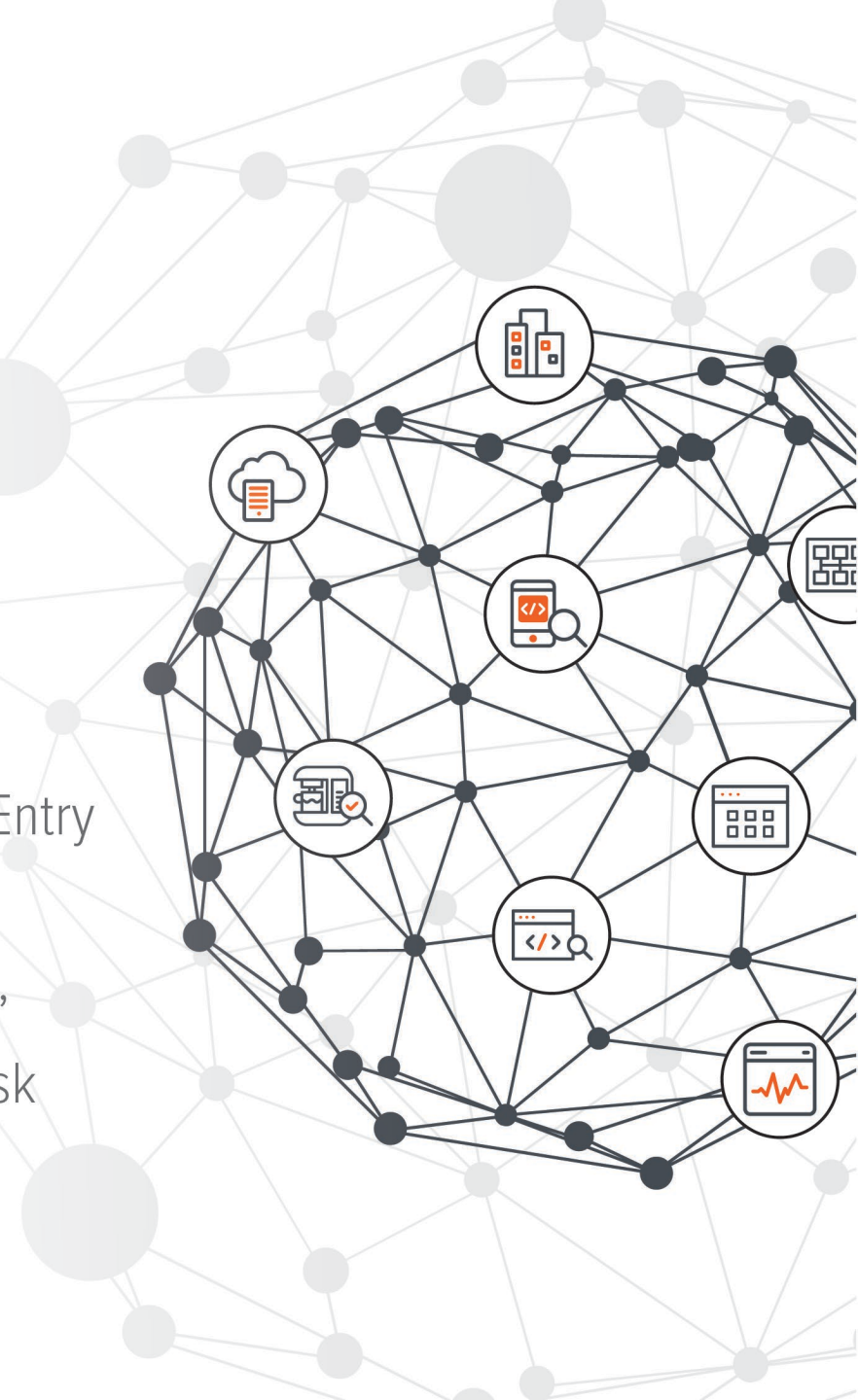




THINGS HACKERS  
**DON'T CARE**  
**ABOUT**

COMMON EXCUSES FOR LACK OF SECURITY

- The **project scope**
- It's managed by a third party
- It's a **legacy system**
- It's too "critical to patch"
- About your budget
- Non-Disclosure Agreements
- It's an **internal system**
- It's handled **in the cloud**
- About your Risk Register Entry
- It's an interim solution
- Other **priorities**
- No "return on investment"
- You contracted out that risk
- It's **encrypted** on disk



EXTERNAL THREAT //  
**NATION STATE**

EXTERNAL THREAT //  
**ORGANIZED CRIME**

EXTERNAL THREAT //  
**HACKTIVIST MOTIVATED**

INTERNAL THREAT //  
**INSIDER DRIVEN**

Economic, Political,  
Military, Espionage,  
and Influence

Financial

Reputation  
or Social

Financial, Professional  
Revenge, Political

MOTIVES

Trade Secrets, Sensitive  
Business Information,  
Critical Infrastructure

Financial Systems, Personal  
Identifiable Information (Pii),  
Payment Card Information and  
Protected Healthcare Info (Phi)

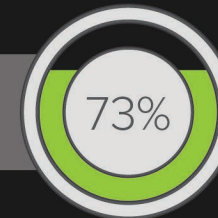
Corporations, Government,  
High Profile Individuals

Intellectual Property,  
Corporations, Government

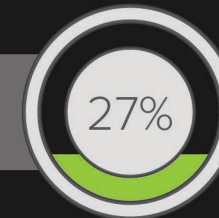
TARGETS

## DATA BREACH

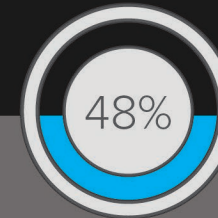
VERIZON RESPONSE REPORT



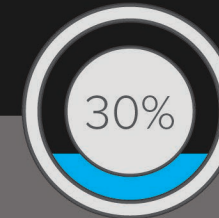
EXTERNAL



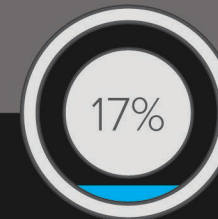
INTERNAL



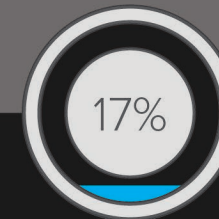
HACKING



MALWARE



ERROR



SOCIAL

WHO

TACTICS

IMPACT // ATTACK

# EQUIFAX

MISSING PATCH

## ATTACK

- Application Security

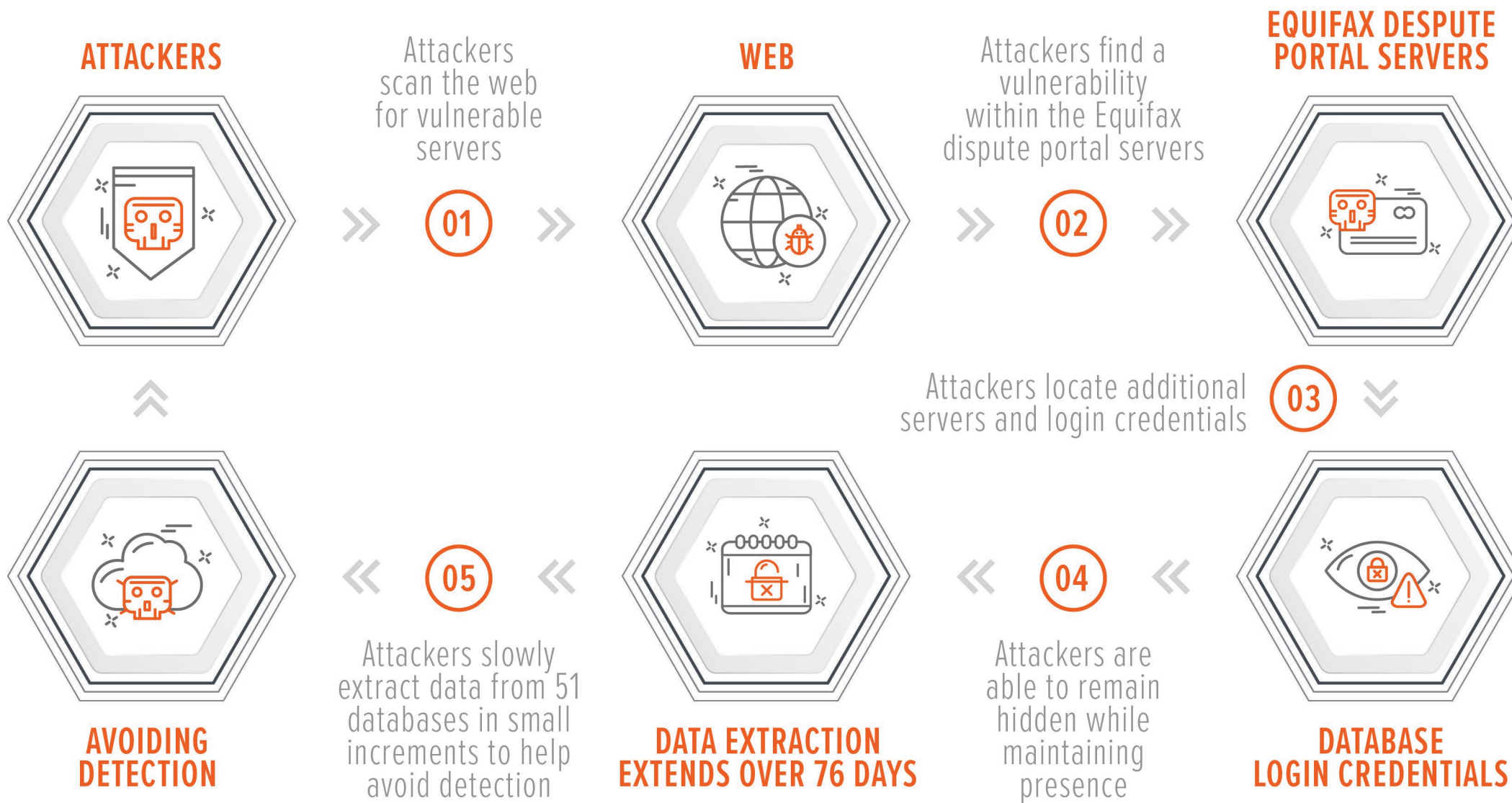
## IMPACT

- 145.5 Million (PII)
- \$439 Million Total Cost of Breach



# HOW ATTACKERS EXPLOITED VULNERABILITIES IN THE 2017 BREACH

BASED ON EQUIFAX INFORMATION





# SOLUTION

**THREE NOTIONS SHOULD GUIDE THE POSITIONING  
AND IDENTITY OF A SUCCESSFUL RED TEAM**

WHERE



The structure of the red team relative to the targeted institution

WHY




The scope of activities that it pursues

HOW



The sensitivity with which it operates and provides its findings and recommendations





# QUESTIONS TO ASK A RED TEAM

BEFORE YOU START

- What is the red team intended to do?
  - Do we have executive buy in?
  - What is the scope of activities we should pursue?
  - Who or what is to be red teamed?
  - For how long?
  - What degree of flexibility?
  - To what end?
  - Are there any sensitive aspects of the red team targets?
  - Define all the “What if?” scenarios.
- 