cisco

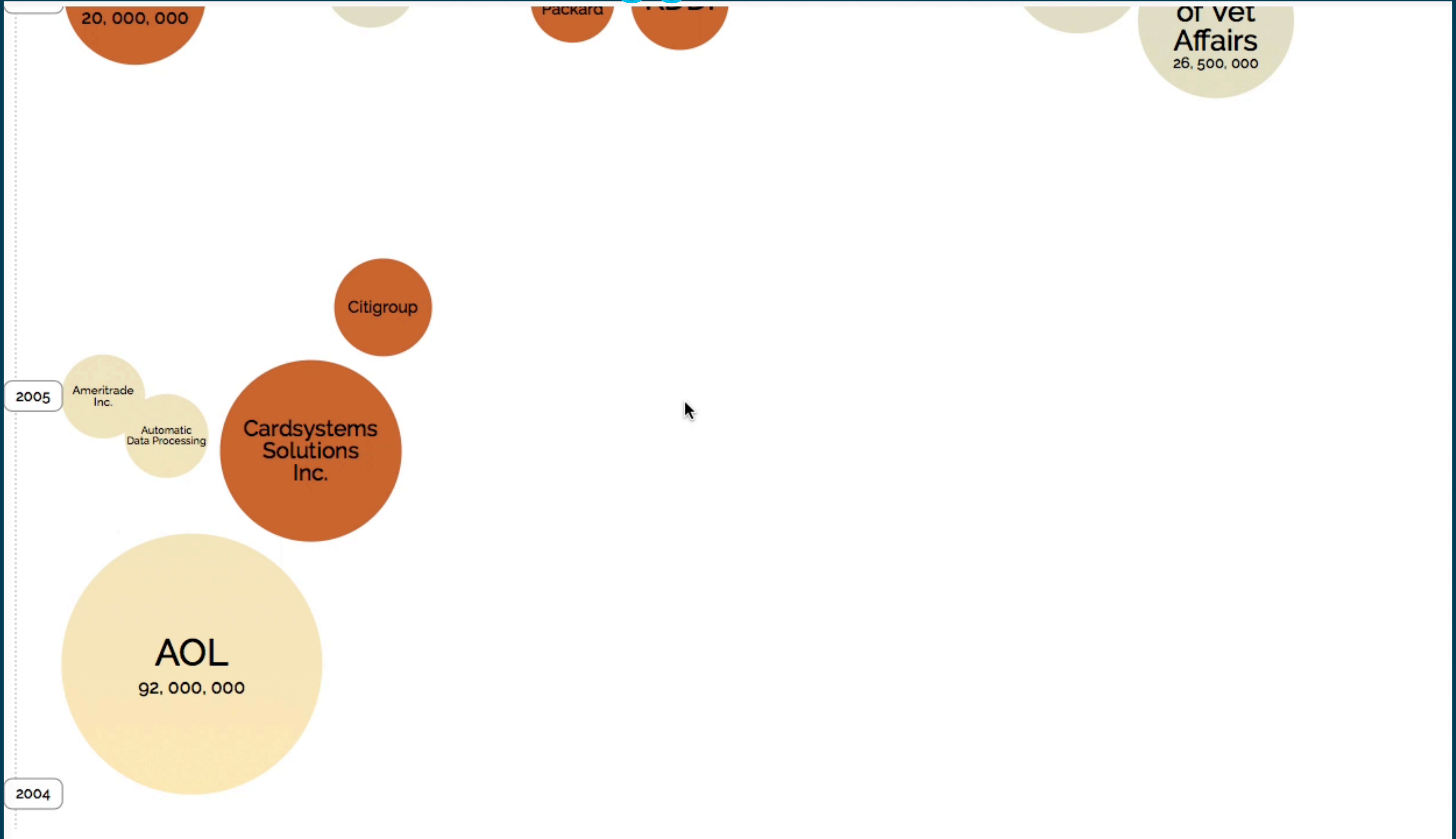
Digital Transformation

Preparing for the Unexpected

Chris Leach
Senior CISO Advisor

October 2019

A Little of Our History
World's Biggest Data Breaches



Today’s risk reality

More interconnected than ever

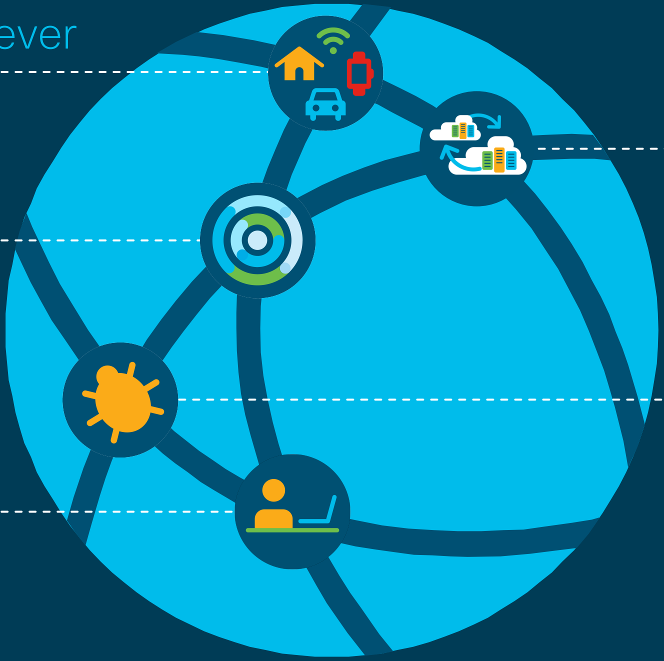
Expanded attack surface

Continuous operations

Must keep business running

Workers connecting everywhere

Loss of control



Multi-cloud reality

A software-defined world

Automated and sophisticated threats

High likelihood of a breach

Attack landscape constantly evolving

Advanced Persistent Threats

Unpatched Software

Spyware/Malware

Wiper Attacks

Phishing

Man in the Middle

DDoS

Cryptomining

Supply chain attacks

Ransomware

Data/IP Theft

Malvertising

Drive by Downloads

Rogue Software

Botnets

Credential compromise

Impossibly complex

Network & Infrastructure Security
Advanced Threat Protection
ICS + OT
NAC
SDN
DDoS Protection
DNS Security
Network Analysis & Forensics
Network Firewall
Deception
Web Security
Endpoint Security
Endpoint Prevention
Endpoint Detection & Response
Application Security
WAF & Application Security
Application Security Testing
MSSP
Traditional MSSP
Advanced MSS & MDR
Data Security
Encryption
DLP
Data Privacy
Other
Mobile Security
Risk & Compliance
Risk Assessment & Visibility
Security Ratings
Pen Testing & Breach Simulation
GRC
Security Awareness & Training
Security Ops & Incident Response
SIEM
Security Incident Response
Security Analytics
Momentum Cyber
Threat Intelligence
IoT
IoT Devices
Automotive
Connected Home
Messaging Security
Identity & Access Management
Authentication
IDaaS
Privileged Management
Identity Governance
Consumer Identity
Digital Risk Management
Security Consulting
Blockchain
Fraud & Transaction Security
Cloud Security
Infrastructure
Container
CASB

Coping with rapid change in a field with endless choices

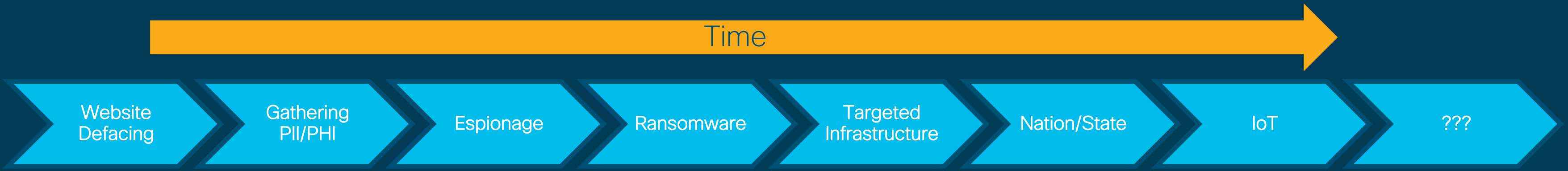
“In a chronically leaking boat, energy devoted to **changing** vessels is more productive than energy devoted to patching leaks.” –Warren Buffett

Coping with rapid change in a field with endless choices

“Change before you have to.” —Jack Welch

ellen

The Attacker’s Playground



Time

Website Defacing

Gathering PII/PHI

Espionage

Ransomware

Targeted Infrastructure

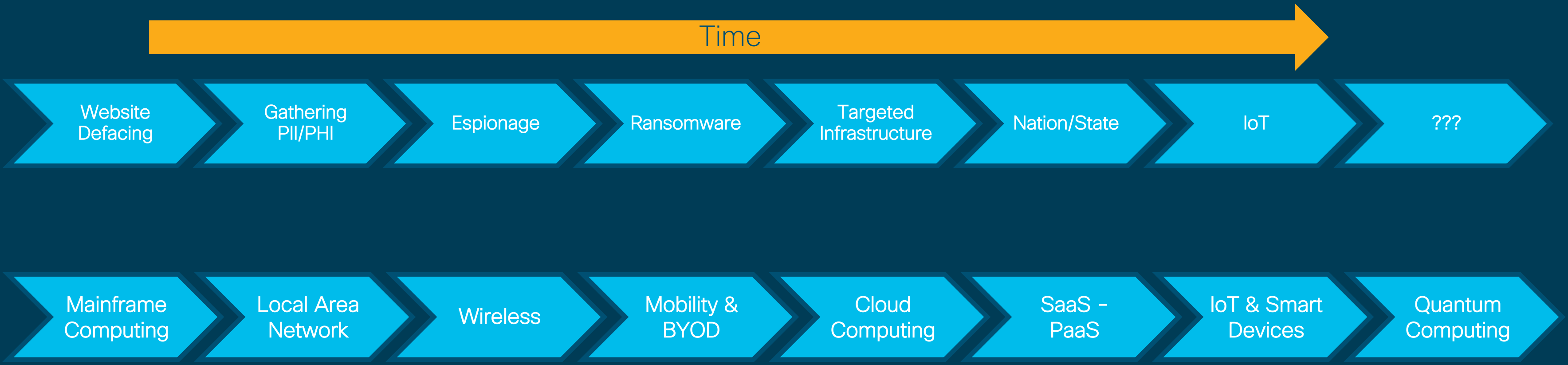
Nation/State

IoT

???

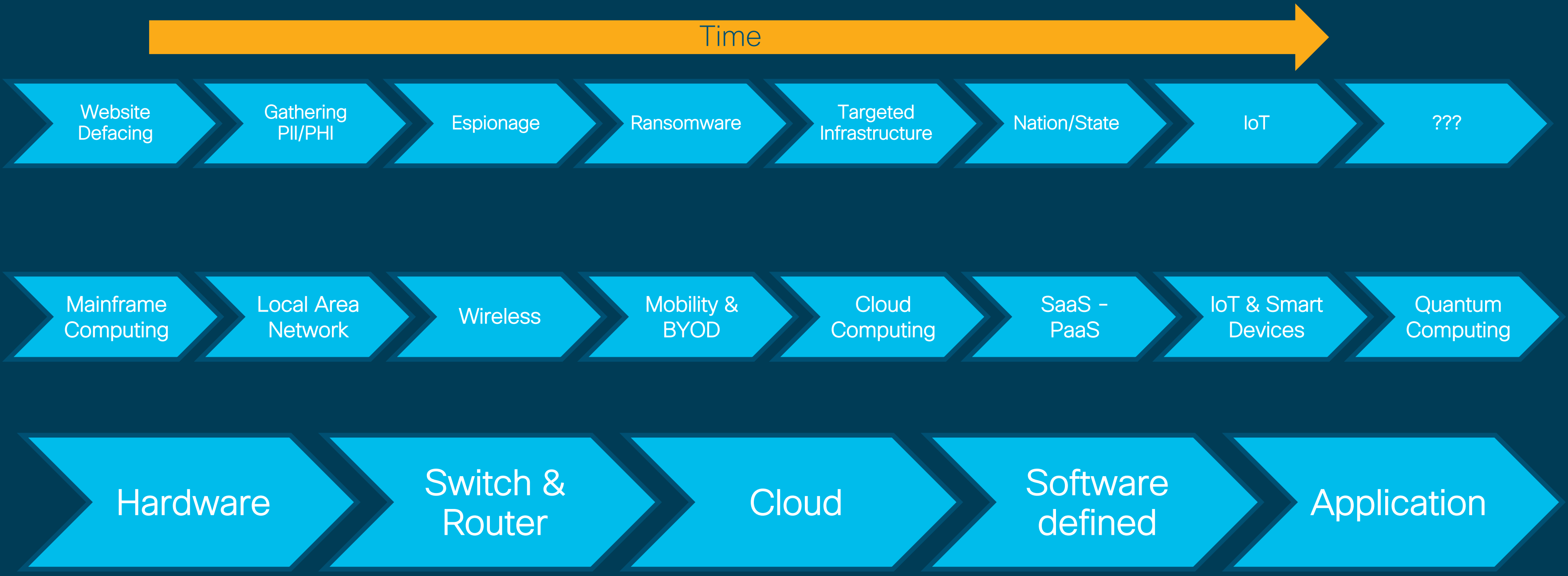
How they play

The Attacker's Playground



Where they play

The Attacker’s Playground



Time

Website Defacing

Gathering PII/PHI

Espionage

Ransomware

Targeted Infrastructure

Nation/State

IoT

???

Mainframe Computing

Local Area Network

Wireless

Mobility & BYOD

Cloud Computing

SaaS - PaaS

IoT & Smart Devices

Quantum Computing

Hardware

Switch & Router

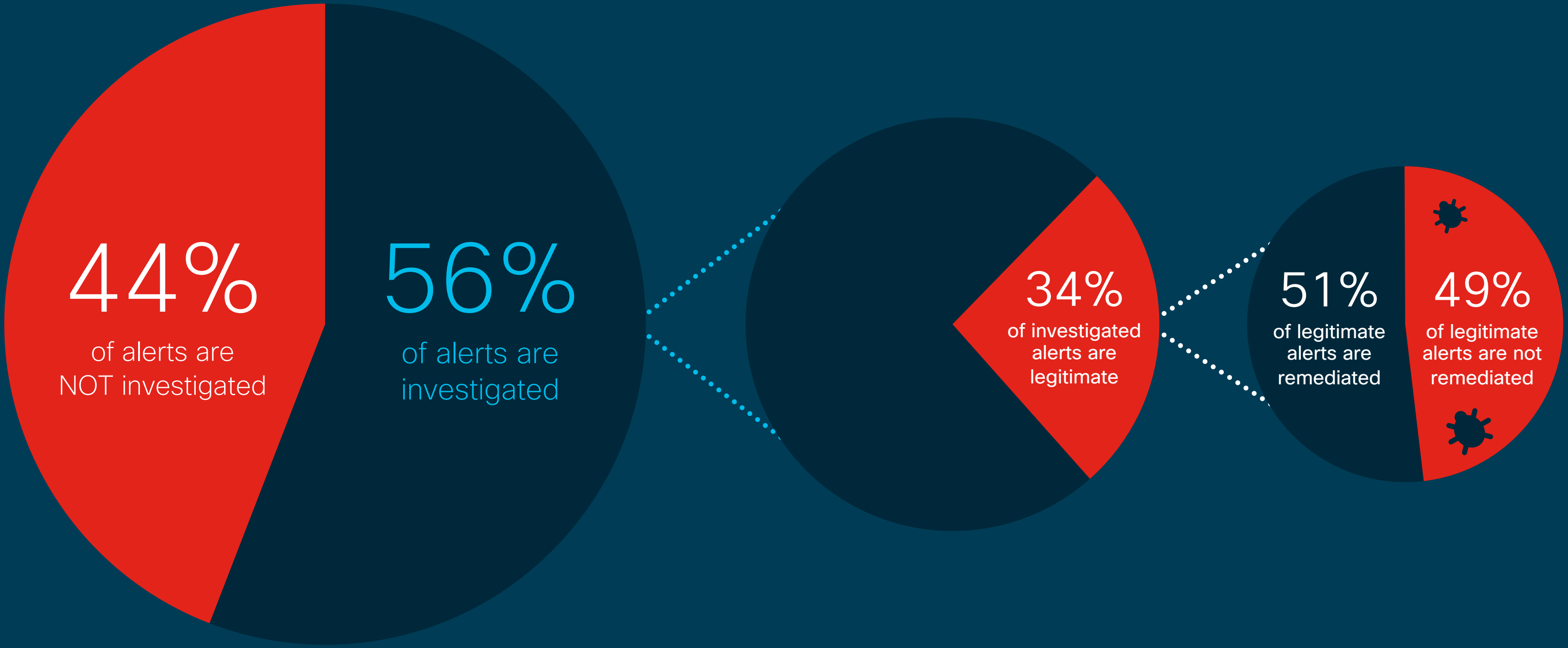
Cloud

Software defined

Application

Where their play toys reside

So many alerts



44%
of alerts are NOT investigated

56%
of alerts are investigated

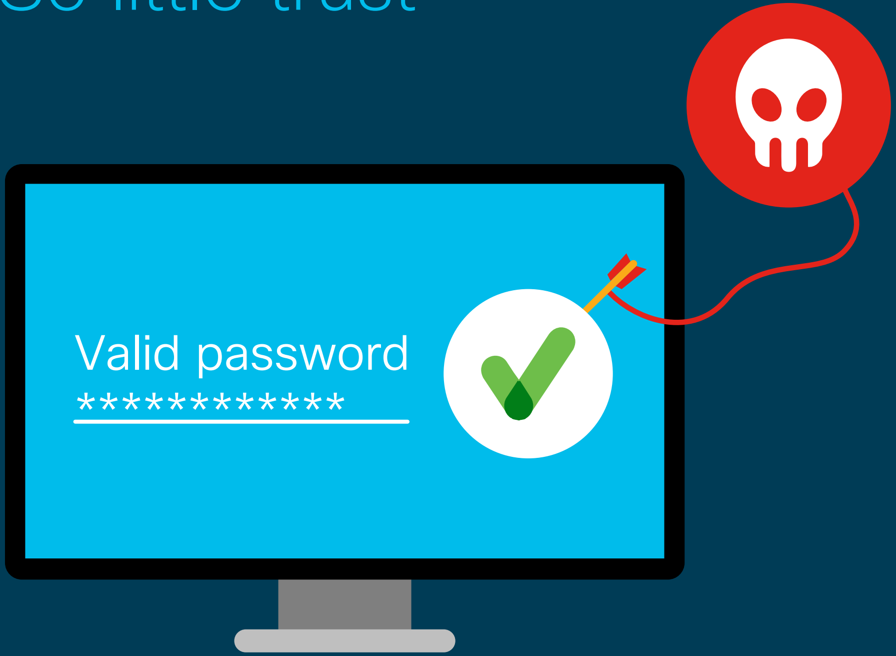
34%
of investigated alerts are legitimate

51%
of legitimate alerts are remediated

49%
of legitimate alerts are not remediated

Source: Cisco Annual CyberSecurity Report 2018

So little trust

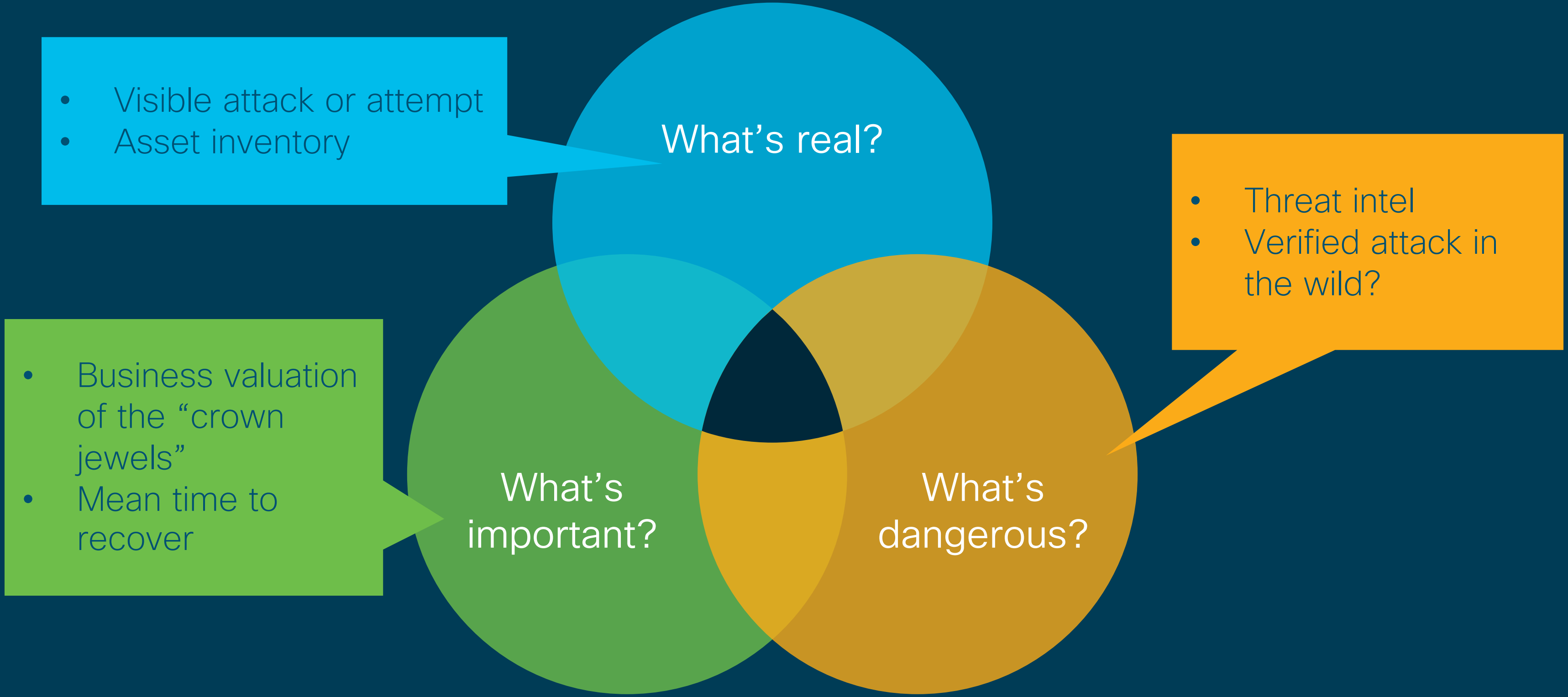


81%

of breaches leverage either stolen or weak passwords

Source: Verizon Data Breach report, 201X

Four questions for preparing for the unexpected



- Visible attack or attempt
- Asset inventory

What's real?

- Threat intel
- Verified attack in the wild?

- Business valuation of the "crown jewels"
- Mean time to recover

What's important?

What's dangerous?

Source: Gartner (September 2018)

Four questions for unexpected

- Visible attack or at
- Asset inventory

Why would I be breached/attacked?

Threat intel
erified attack in
e wild?

- Business valuation of the “crown jewels”
- Mean time to recover

Source: Gartner (September 2018)

What does all of this mean to the CISO

- Change your strategy
- Identify and protect what's important first (what are your crown jewels?)
- Have a migration plan
- Stop shopping for the best of breed tools
- Avoid the paralysis by analysis syndrome
- Consider your team
- Let go of failed ideas