Security Operations:
Moving to a Narrative-Driven Model

Josh Goldfarb – VP, CTO - Americas

STATE OF CYBER SECURITY: THE PROBLEM

DESPITE $30B SPENT ON CYBERSECURITY EVERY YEAR, 97% OF ORGANIZATIONS ARE BREACHED.

— **67%** LEARN THEY ARE BREACHED FROM A THIRD PARTY

— **$3.5M** AVERAGE COST OF A BREACH

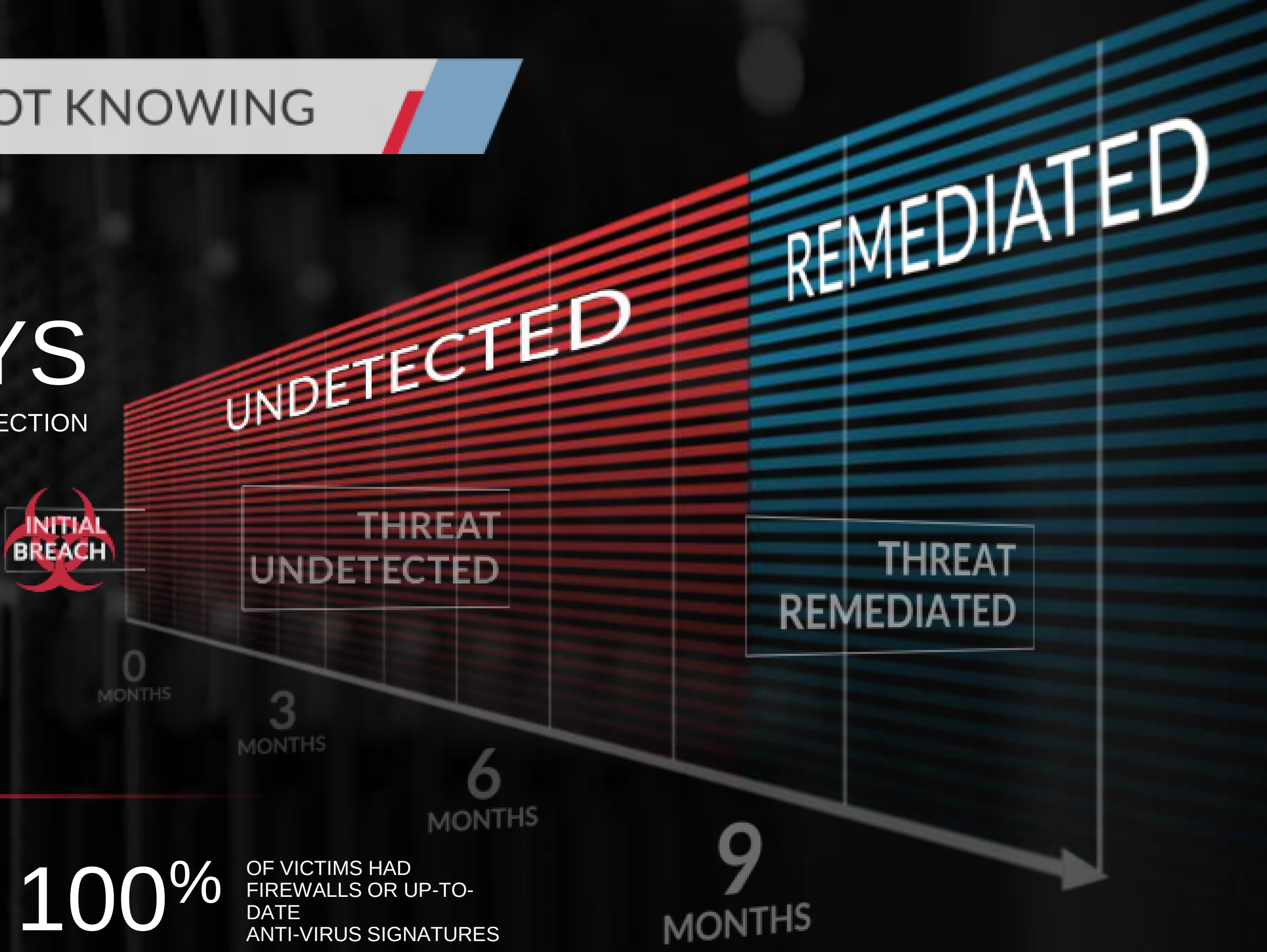
— **32** DAYS TO RESPOND TO A BREACH ON AVERAGE

— **229** TO DETECT THE BREACH

THE IMPACT OF NOT KNOWING

229 DAYS

MEDIAN NUMBER OF DAYS BEFORE DETECTION



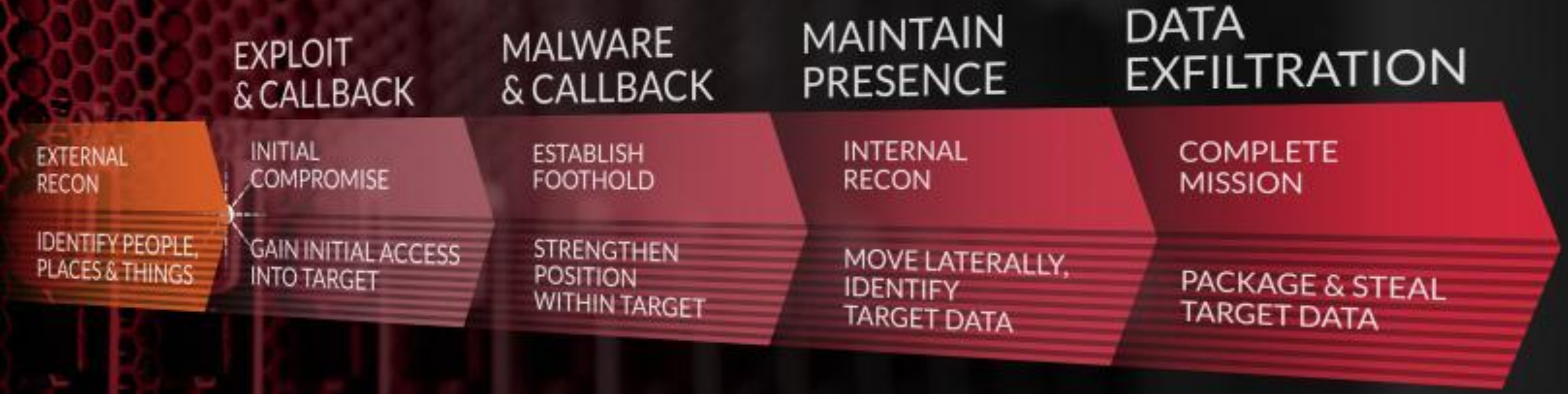
67% OF COMPANIES LEARNED THEY WERE BREACHED FROM AN EXTERNAL ENTITY

100% OF VICTIMS HAD FIREWALLS OR UP-TO-DATE
ANTI-VIRUS SIGNATURES

SOURCE: MANDIANT M-TRENDS REPORT

UNDERSTANDING THE ATTACK

ATTACKERS UTILIZE MULTIPLE VECTORS
AND MULTIPLE FLOWS TO COMPLETE THEIR MISSION



EXTERNAL RECON

IDENTIFY PEOPLE, PLACES & THINGS

EXPLOIT & CALLBACK

INITIAL COMPROMISE

GAIN INITIAL ACCESS INTO TARGET

MALWARE & CALLBACK

ESTABLISH FOOTHOLD

STRENGTHEN POSITION WITHIN TARGET

MAINTAIN PRESENCE

INTERNAL RECON

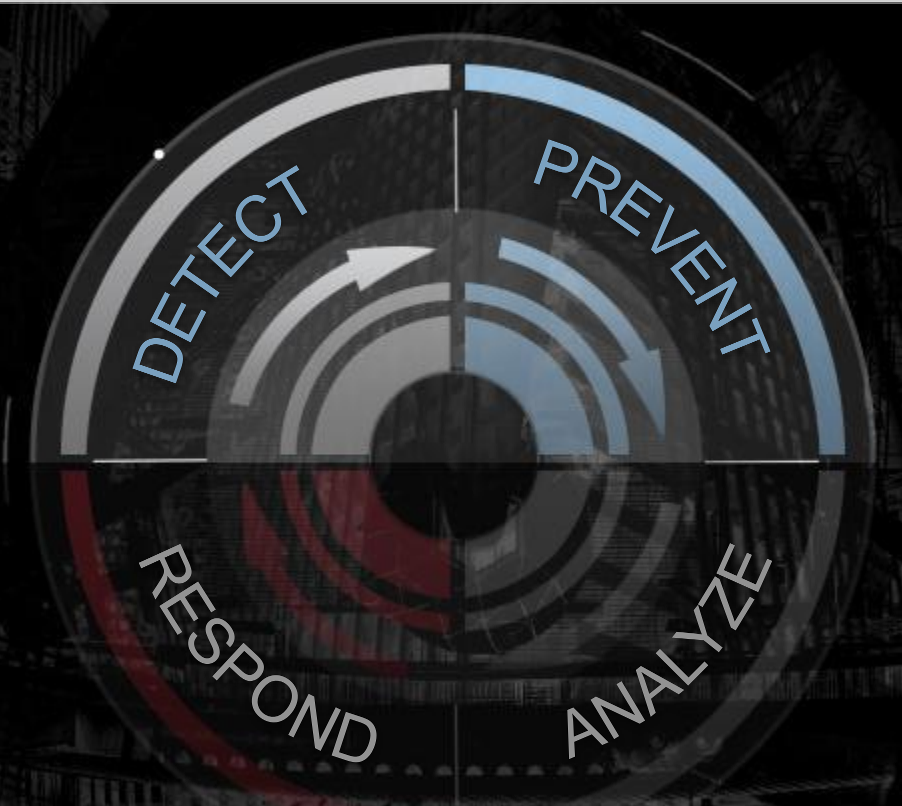
MOVE LATERALLY, IDENTIFY TARGET DATA

DATA EXFILTRATION

COMPLETE MISSION

PACKAGE & STEAL TARGET DATA

CONTINUOUS SECURITY MONITORING



So Many Important Questions

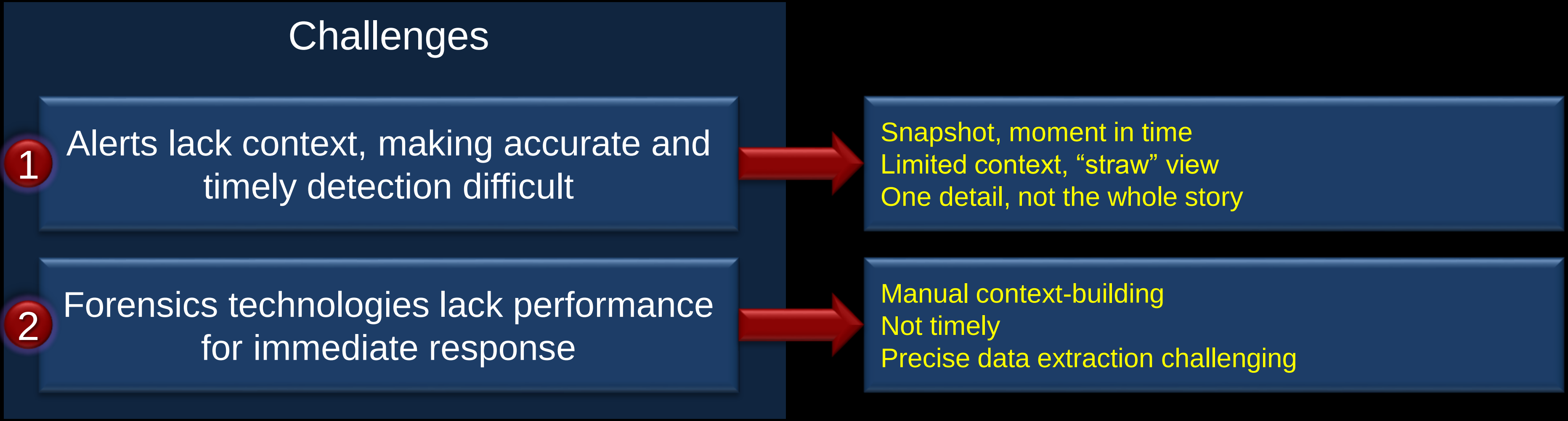
How long have I been under attack?

How many endpoints are infected?

What was the extent of the damage?

What are the Indicators of Compromise?

Challenges: Alert-Driven Detection Model



Challenges

1 Alerts lack context, making accurate and timely detection difficult

Snapshot, moment in time
Limited context, “straw” view
One detail, not the whole story

2 Forensics technologies lack performance for immediate response

Manual context-building
Not timely
Precise data extraction challenging

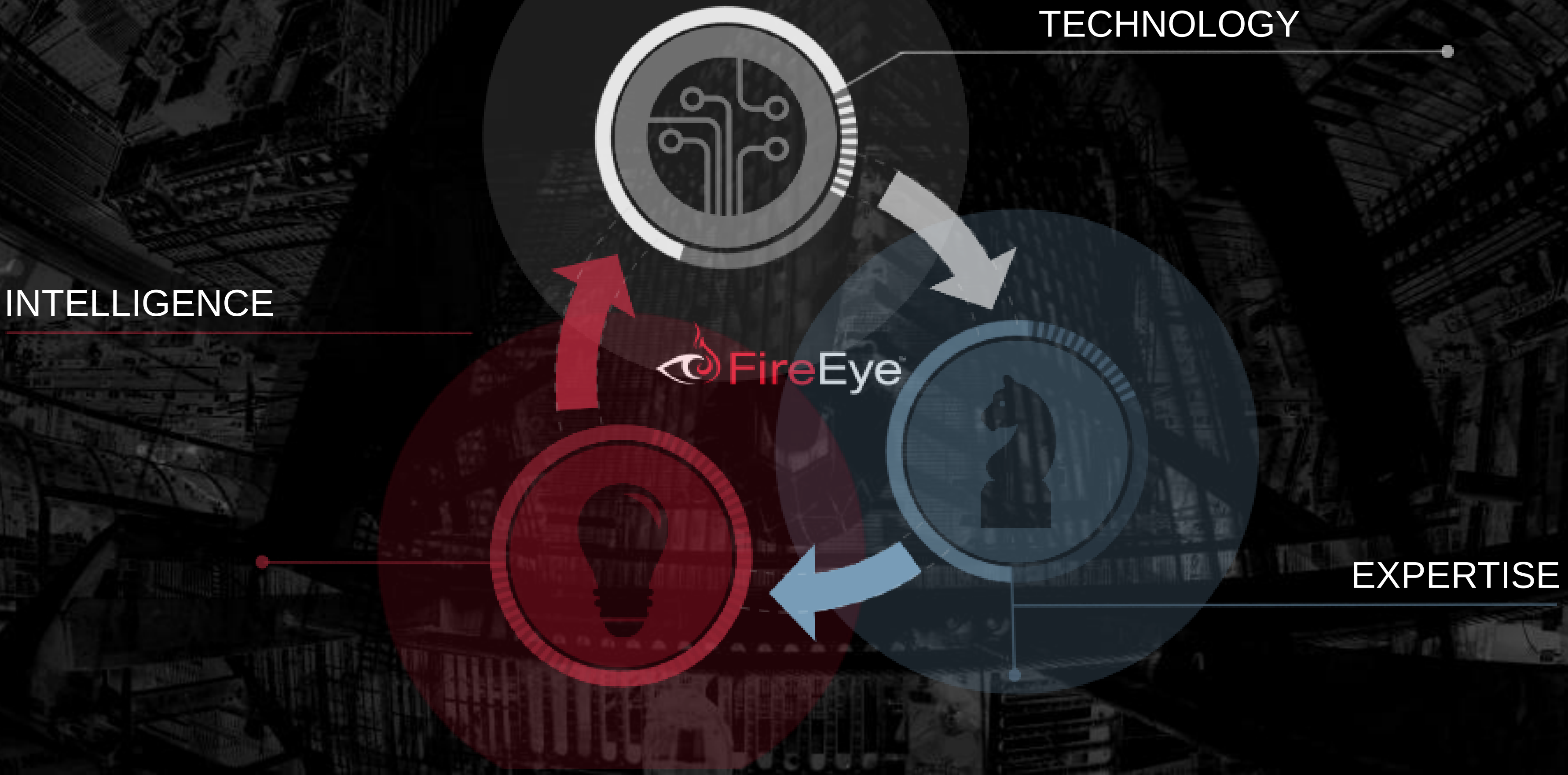
Putting Together the Story: Narrative Driven Security

Did the attack succeed?
What else can I learn about the attack?
Endpoint

Where is the attack destined?
Do I see artifacts of intrusion?
Network

What does the complete picture look like?
What is my exposure?
Forensics

COMPONENTS THAT BUILD THE NARRATIVE



How?

- Identify risks, goals, and priorities
- Identify gaps in telemetry
- Develop content
- Improve signal-to-noise ratio
- Concentrate into unified work queue
- Enrich with supporting evidence
- Automate common analysis steps
- Interleave intelligence
- Present the narrative

FireEye™
SECURITY REIMAGINED

THANK YOU

@ananalytical