Inside Intelligence 2016

A SAS CONFERENCE FOR INDUSTRY ANALYSTS

SAS® CYBERSECURITY

STU BRADLEY

THE CHALLENGE | COLLABORATIVE CRIME

THE CHALLENGE | MALWARE-AS-A-SERVICE

THE CHALLENGE | WORLD WITHOUT GOVERNANCE

…Conventions, Policies, Agreements, Treaties…

THE CHALLENGE | ENLARGING THREAT SURFACE

$170B Annual Spend

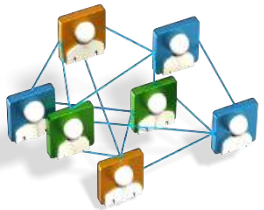
80.5 Days

10B Events

$154 per Record

59% Detected by 3rd Party

$450B Lost



$133M OPM

200% increase in cost

SOLVING THE MARKET PROBLEM

Enterprises unable to detect attackers' presence on their network due to excessive volume of security alerts and lack of visibility into network behaviors

SAS®
CYBERSECURITY

KEY CHALLENGES THAT MUST BE ADDRESSED

Detection Avoidance

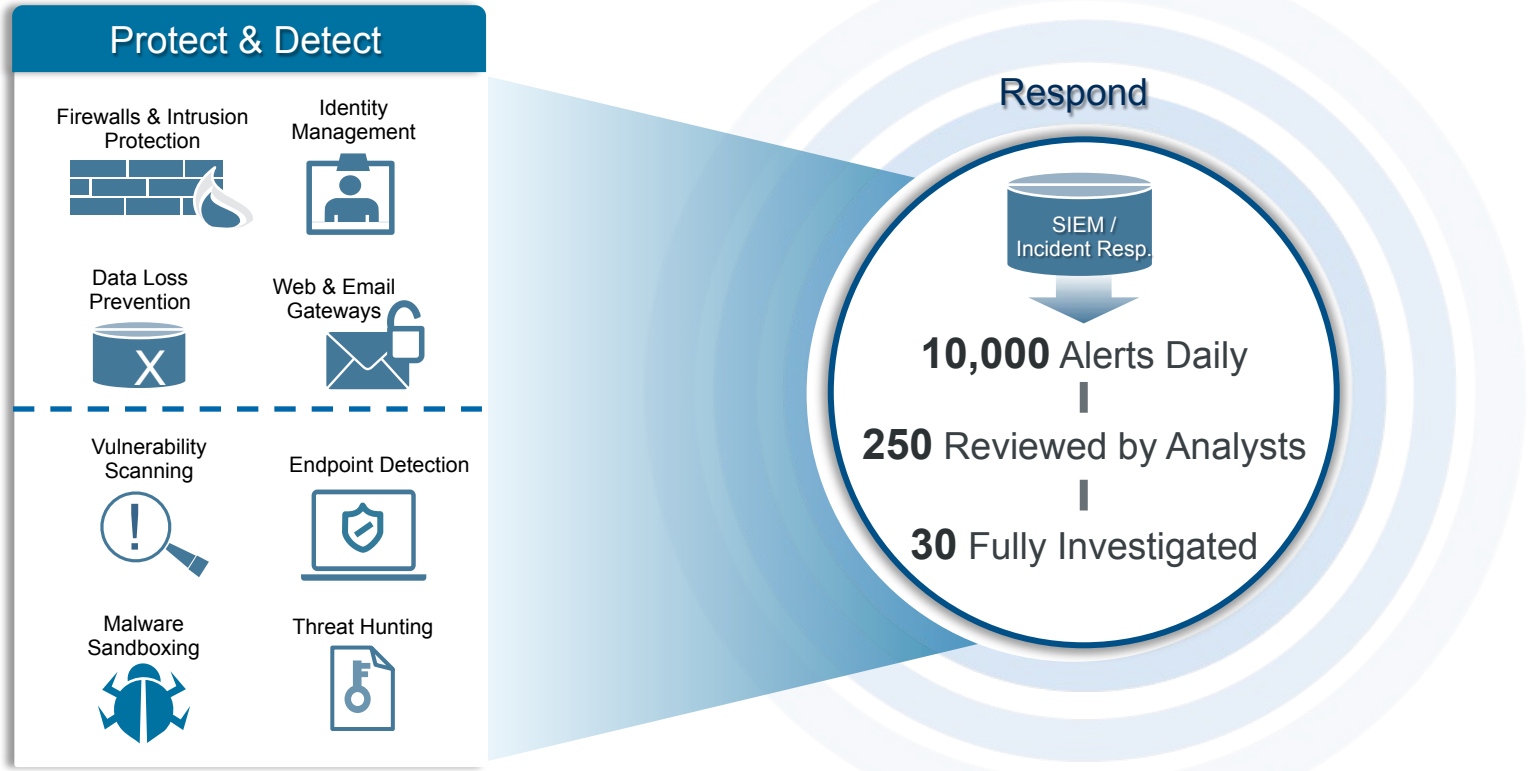
Limits of Signatures & Rules

Economics of Data Scale

Analyst Fatigue

THE CYBER ECOSYSTEM

IDENTIFY – PROTECT – DETECT – RESPOND – RECOVER

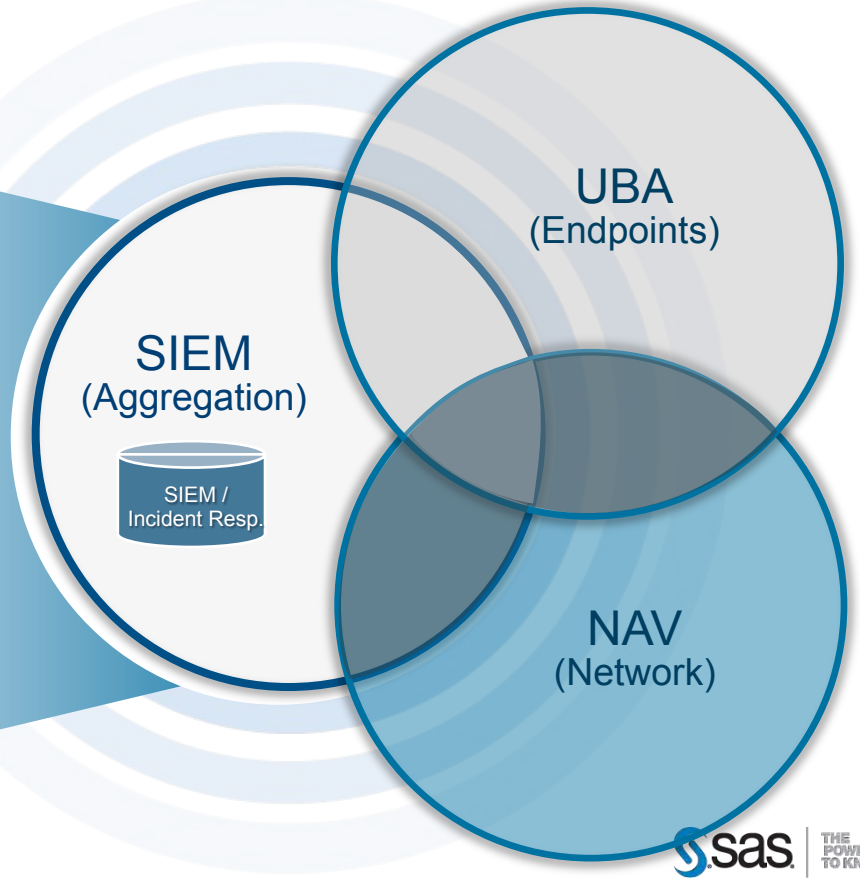


THE CYBER ECOSYSTEM

THE DETECTION MARKET IS CHANGING

Protect & Detect

- Firewalls & Intrusion Protection
- Identity Management
- Data Loss Prevention
- Web & Email Gateways
- Vulnerability Scanning
- Endpoint Detection
- Malware Sandboxing
- Threat Hunting



SECURITY ANALYTICS

THE BUZZ IS NOT ENOUGH…

sas THE POWER TO KNOW.

CYBER MARKET | ANALYTIC MATURITY CURVE

Value of Results

SECURITY ANALYTICS

THE ANALYTIC PILLARS

Analytic Driven Triage

Analytic insight and triage guidance served to security analysts to drive focus and efficiency.

Predictive Cyberanalytics

Additive machine learning layer based upon feedback loop highlighting & categorizing malicious behaviors.

Anomaly Detection

Understand normal & abnormal network activity. Leverage device peer groups to identify subtle threats.

In-stream & In-memory

sas THE POWER TO KNOW.

IN SUMMARY

What you Need to Know

THERE IS HOPE FOR SECURITY ANALYTICS…

- Can provide network visibility
- You should investigate data, timing & analytic approaches used
- You should understand impact of scale

Inside Intelligence 2016

A SAS CONFERENCE FOR INDUSTRY ANALYSTS

QUESTIONS?

THE CHALLENGE | MASSIVE MALICIOUS EXPLOITATION

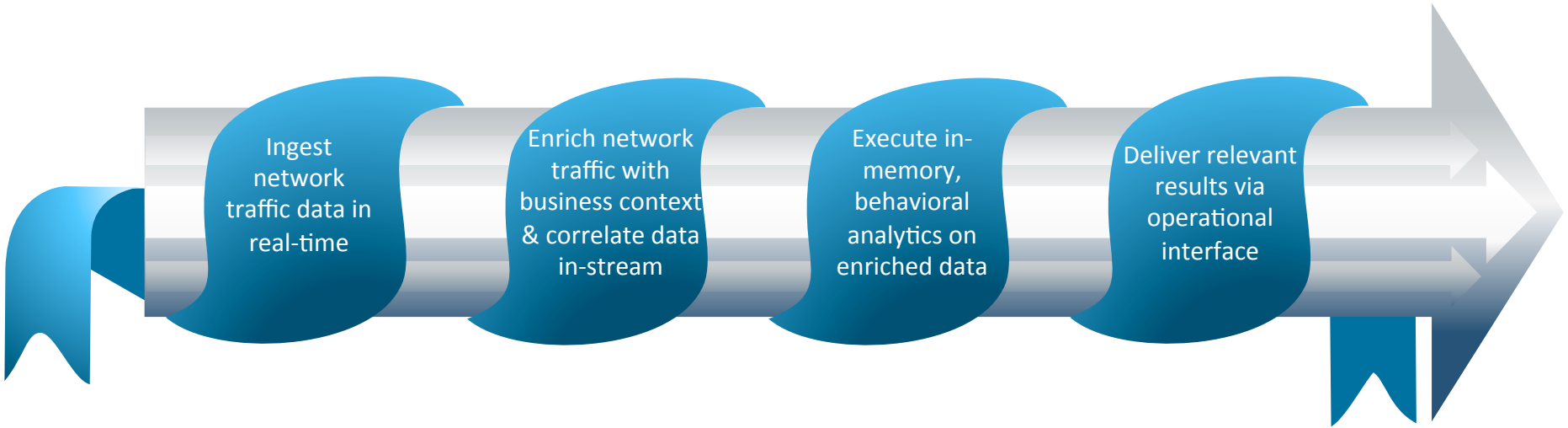
"There are two types of big companies in the U.S., those that have been hacked... and those who don't know they've been hacked." - James Comey, Director of the FBI

THE CHALLENGE | NETWORK UNKNOWN: DEPTH & SCOPE

SAS®
CYBERSECURITY

BEHAVIORAL ANALYTICS ON SMARTER DATA

How it Works…



SAS®
CYBERSECURITY

BEHAVIORAL ANALYTICS ON SMARTER DATA