

The logo features a stylized red graphic on the left, consisting of two curved, overlapping lines that resemble a flame or a wing. To the right of this graphic, the word "CROWDSTRIKE" is written in a bold, white, sans-serif font.

CROWDSTRIKE



Innovation Never Rests

A New SOC Blueprint for
Tomorrow's Threats

A LITTLE ABOUT ME:

ARIS KOIOS

As a Technology Strategist for CrowdStrike, Aris is part of the CTO office and responsible for creating and communicating the company's technical vision and strategy.

Aris is a trusted leader with over 16 years of experience in the cybersecurity industry working in various management positions and technical consulting roles across 3 continents with a focus on helping customers to prevent breaches and manage risks.



aris.koios@crowdstrike.com



Key SOC Challenges:

- Business Alignment
- Measurement
- Talent gap / skill shortage
- Day to day tasks

Today's analysts must...



Triage faster

79 minutes

Average breakout time



Defend new attack vectors

3x

Increase in cloud-conscious adversaries



Onboard and uplevel new analysts

+80%

Say skills shortage has impacted operations



Do more with less – workforce does not scale

7 in 10

Organizations struggle to keep up with alerts

Stop the breach.

Progressive Attack Surface

Digital Transformation: Apps everywhere, work anywhere

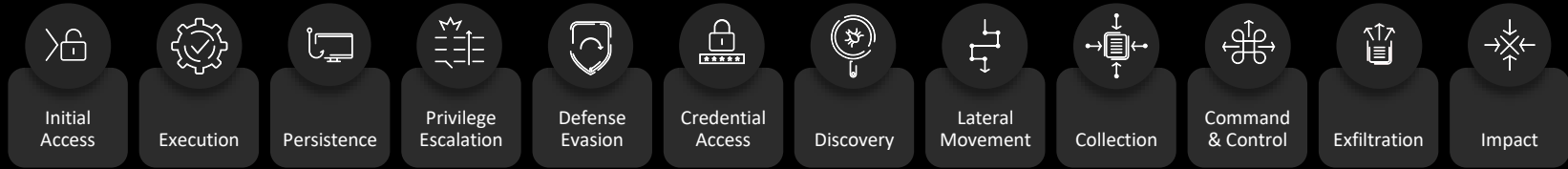
Cloud Adoption – Hybrid and Multi-Clouds

Ransomware, Malware-free attacks and Identity

Vulnerabilities and complex Supply Chains

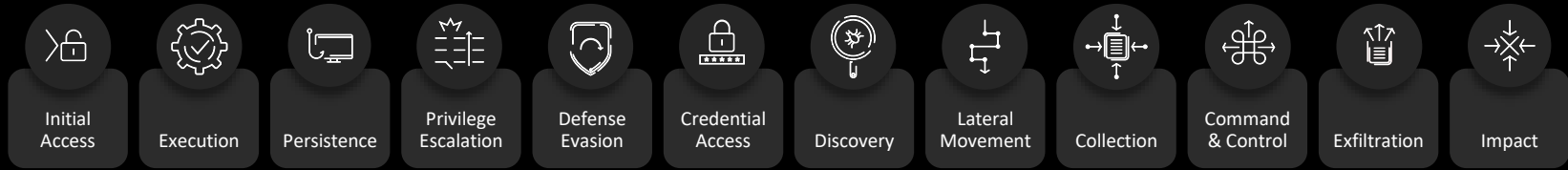


Evolving Adversarial Tactics



Linear?

Evolving Adversarial Tactics



Business email compromise

Infected BYOD

Supply chain vulnerability

Legacy system vulnerability

Malware

Drive-by downloads

Credential scanning

Deprecated protocol usage

Phishing

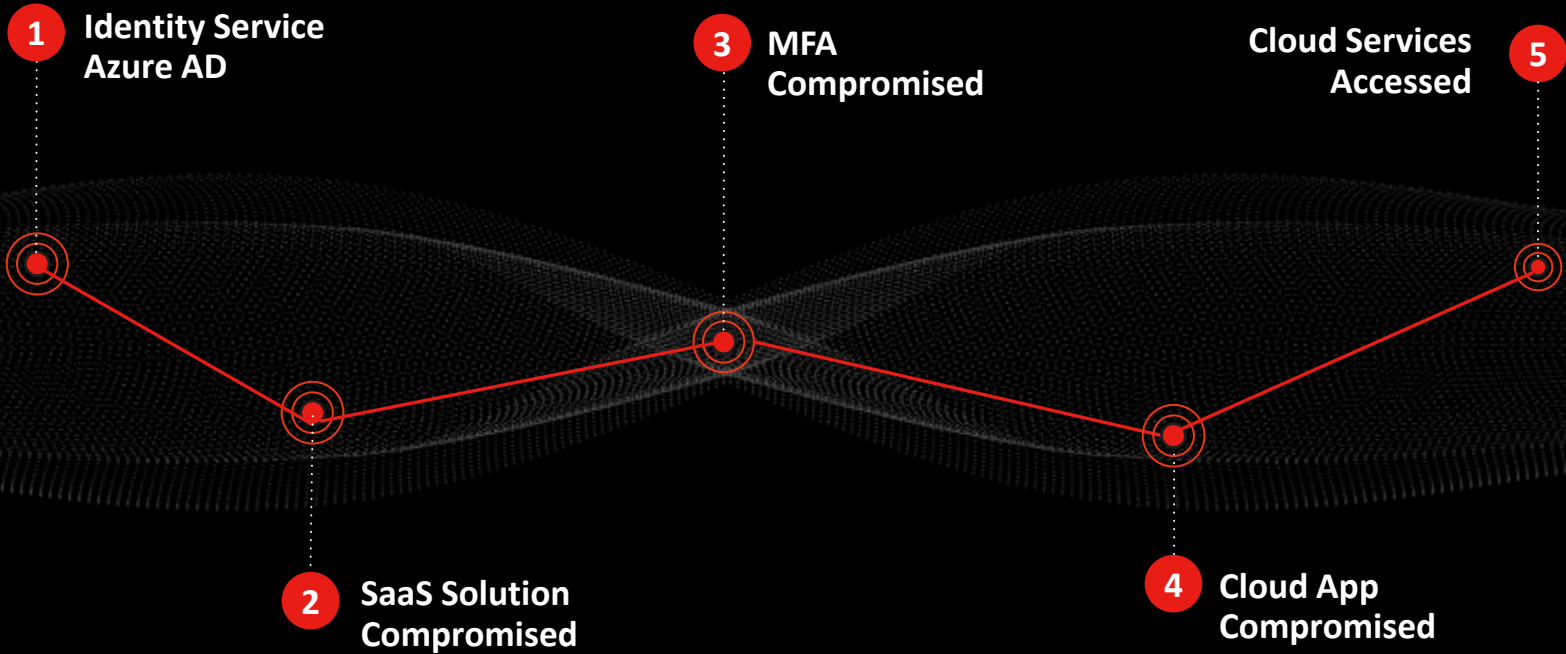
Privilege escalation

Compromised USB

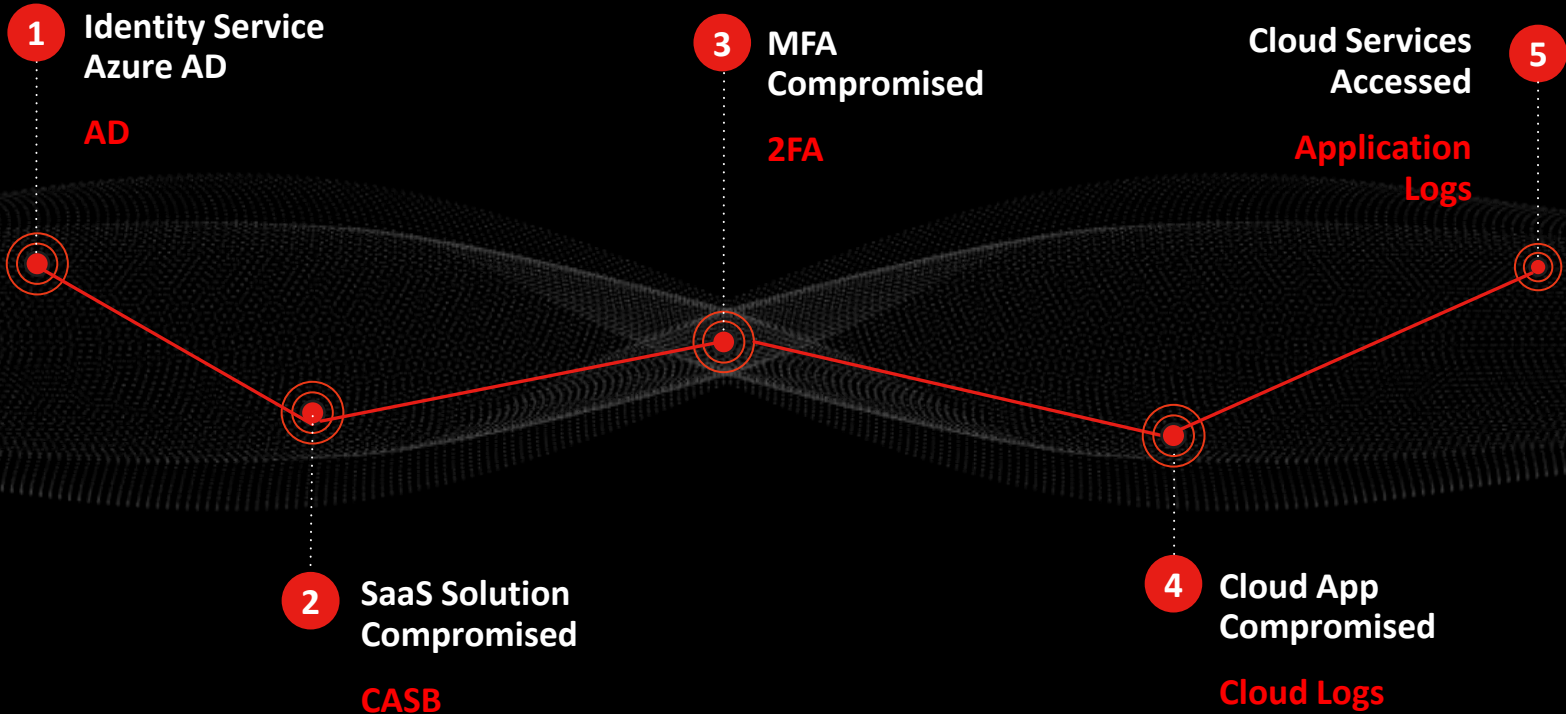


The path of least resistance!

The reality of an attacker



The reality of an attacker



Every Second Counts

Effective SOCs Requires Efficient Response



Protect all vectors

A 288% increase in attacks against cloud workloads and environments



Adversaries are getting faster

Breakout time declined from 98 minutes in 2021 to 79 minutes in 2023



Valid Accounts Facilitate Lateral Movement

Adversaries often operate in possession of multiple sets of credentials, increasing opportunities for lateral movement.

79
MINUTES

average eCrime breakout time

FASTEST TIME RECORDED: 7 MINUTES

The Components of a SOC



Technology



People & Processes



Data

SOC = SIEM

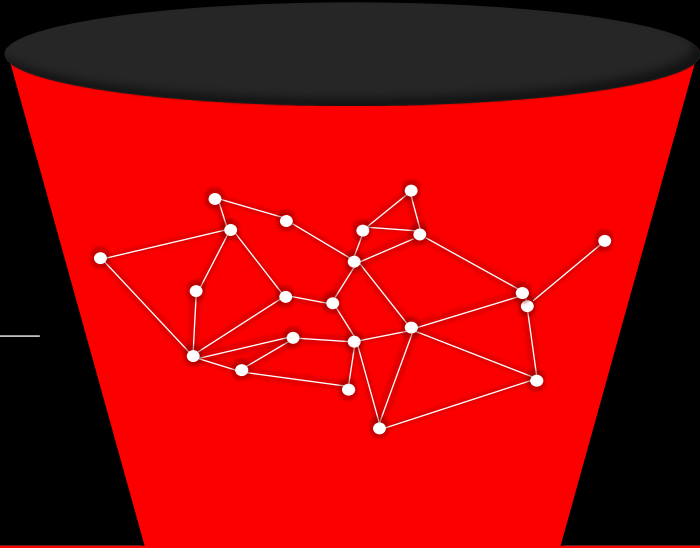
SOC  SIEM

The Data Engineering Panacea

Data

Analytics & AI

Outcomes



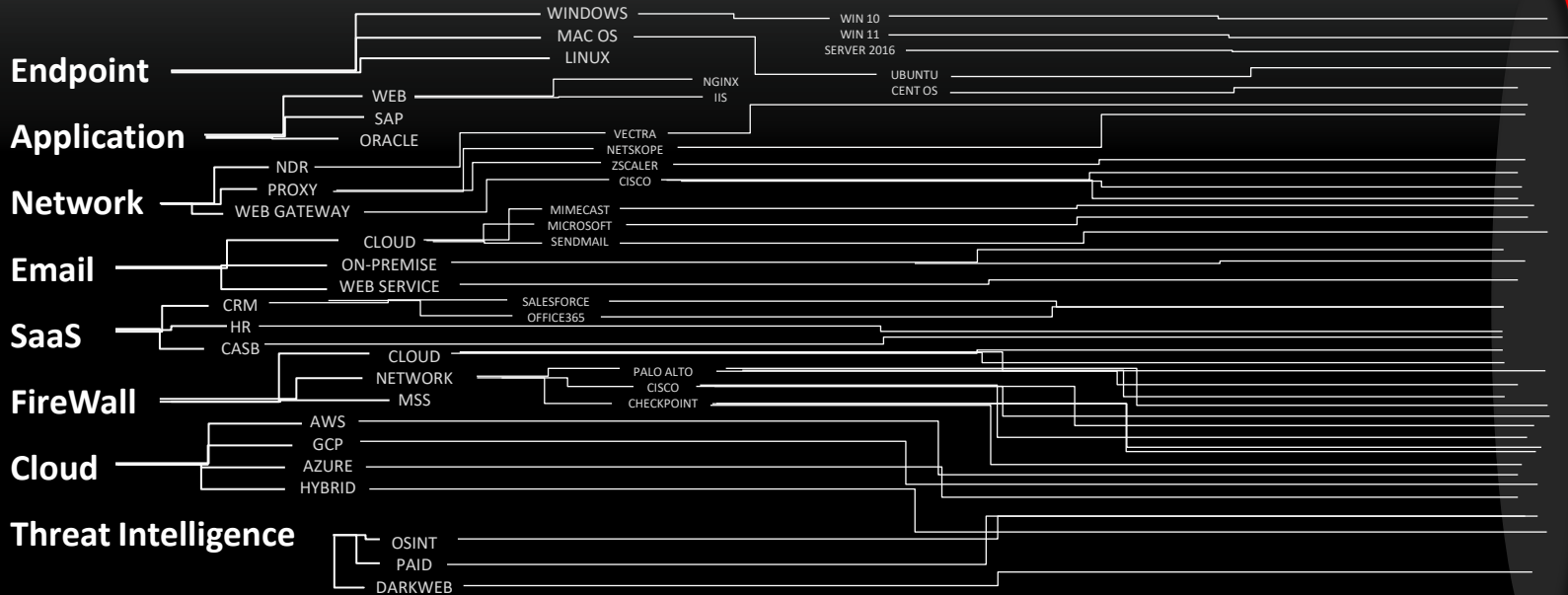
- _____
- _____
- _____
- _____
- _____

The Problem with Data Collection

Data source

Vendors

Versions

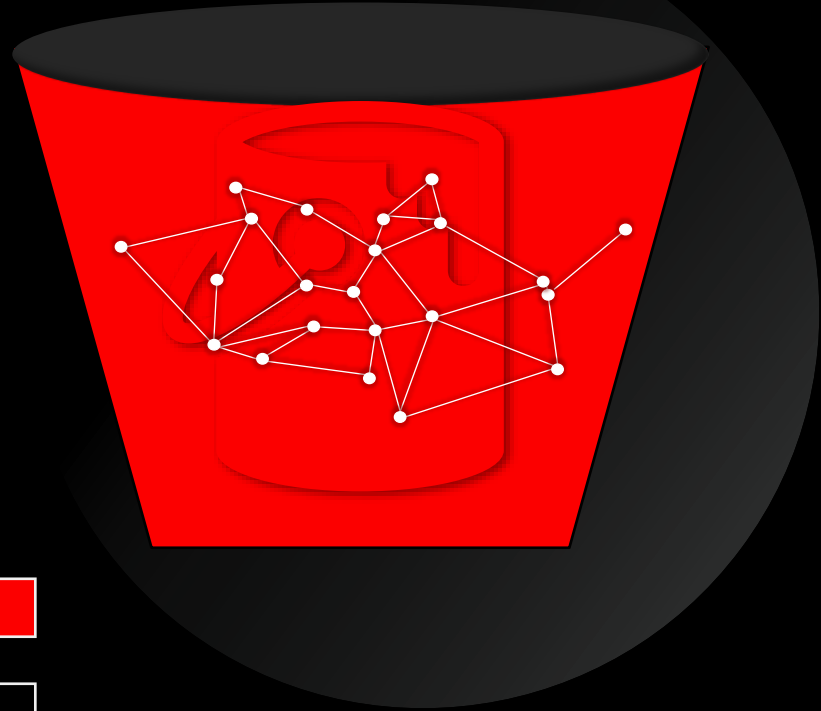
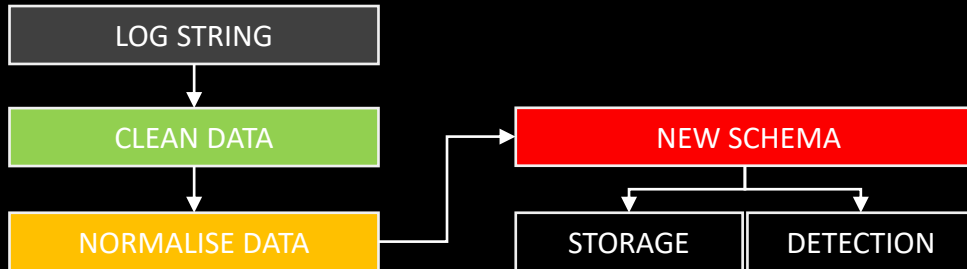


Analytics & AI

The Analytics Problem

IP4
IPVersion4
NetworkEventIP4
NetAddress
IP
NetworkConnect4

= IP4

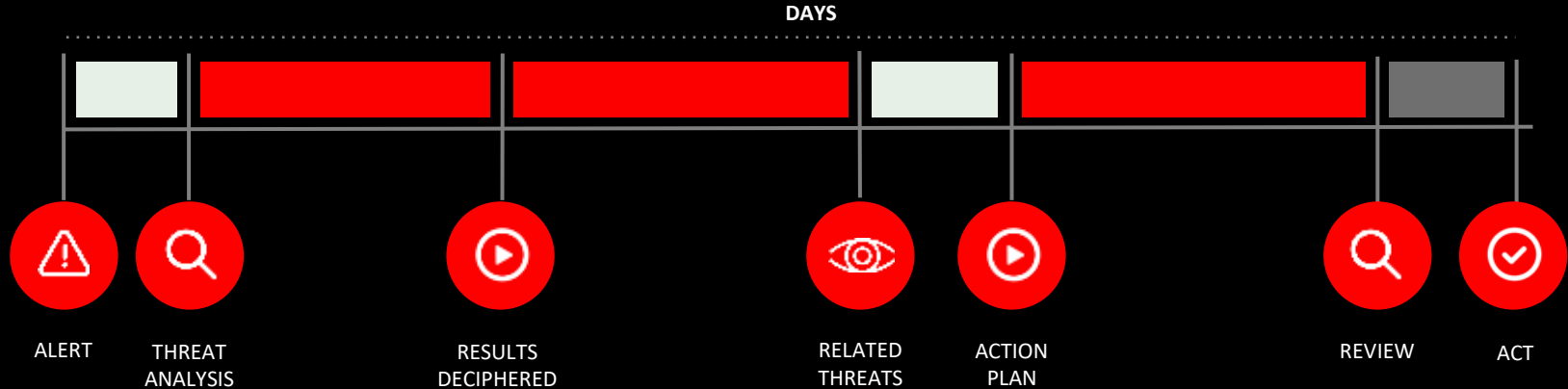


A large, vibrant red abstract graphic on the left side of the slide, resembling a stylized flame or a flowing ribbon that curves upwards and then downwards.

Learning from mistakes.
The total cost of data engineering.

The problem:

For sophisticated adversaries, investigation and response takes too long



CHALLENGES

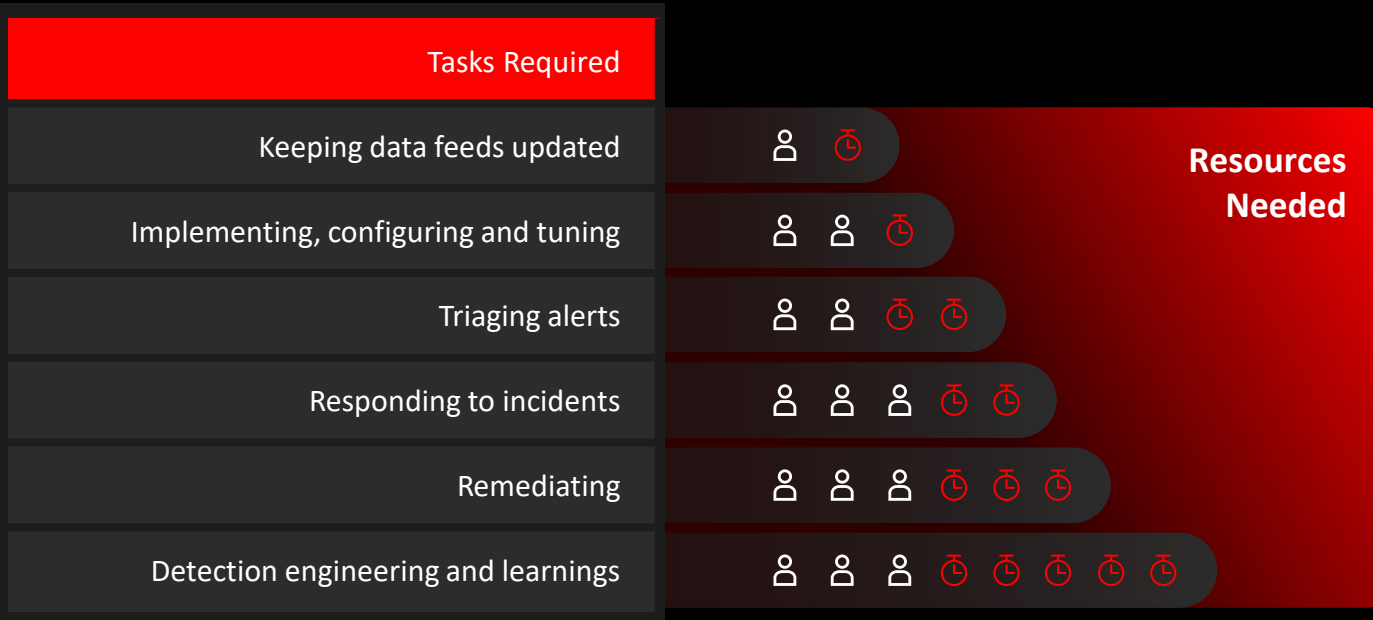
Requires advanced skills

Time consuming analysis

Multiple analysis tools

Error prone, manual effort

Skills, skills and more skills!



Vision for Generative AI in a SOC

Tier 1 Analyst

- Answers Question, Shows Work
- Saves Time by bringing All relevant Data into View
- Primary Goal of Accuracy

Tier 2 Analyst

- Containment Actions & Policy Change Suggestions
- Investigation Suggestions & Remediation Generation

Tier 3+ Analyst

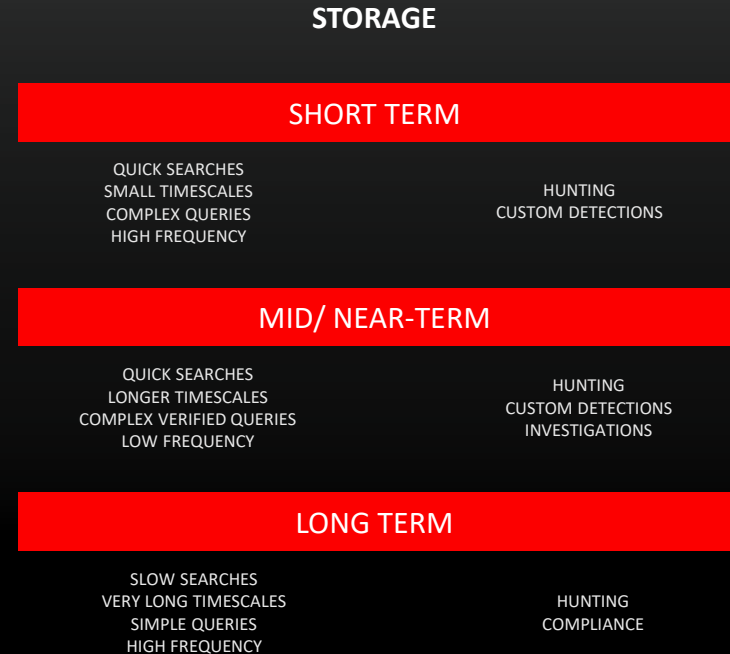
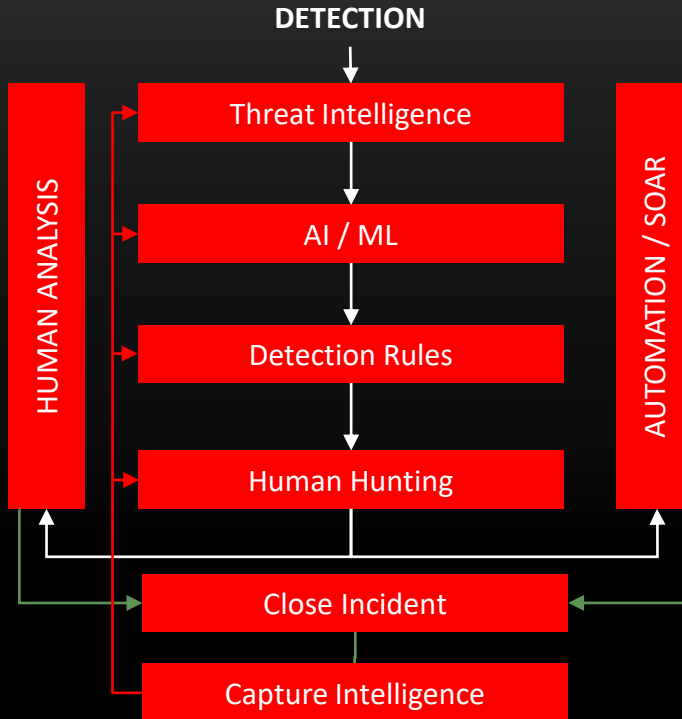
- SOAR Workflow Generation
- Hunting Automation
- Containment Automation

AI Models and API - Automate Interactions

Automated Analysis & Triage
Automated Response
Automated Hunting

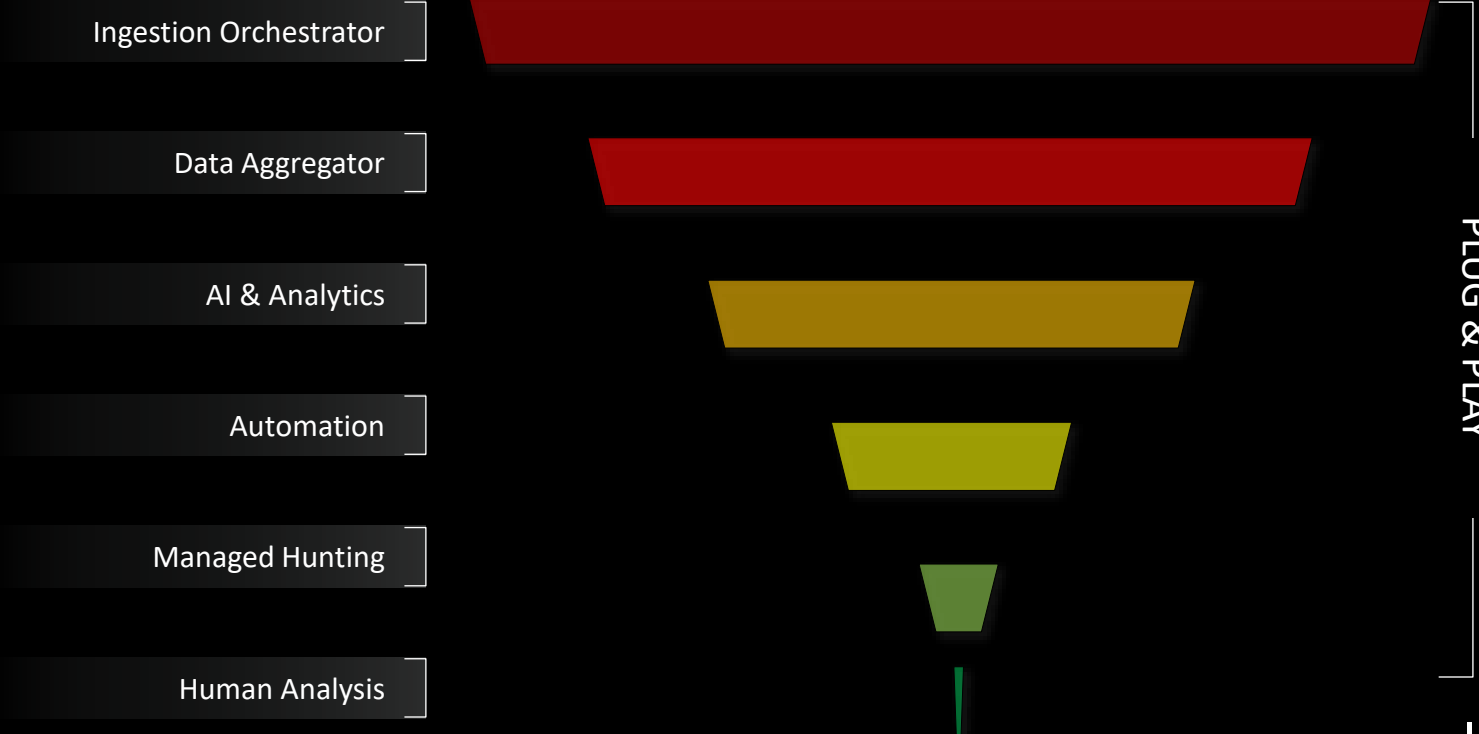
The Future Blueprint

The Architecture



The Future Blueprint

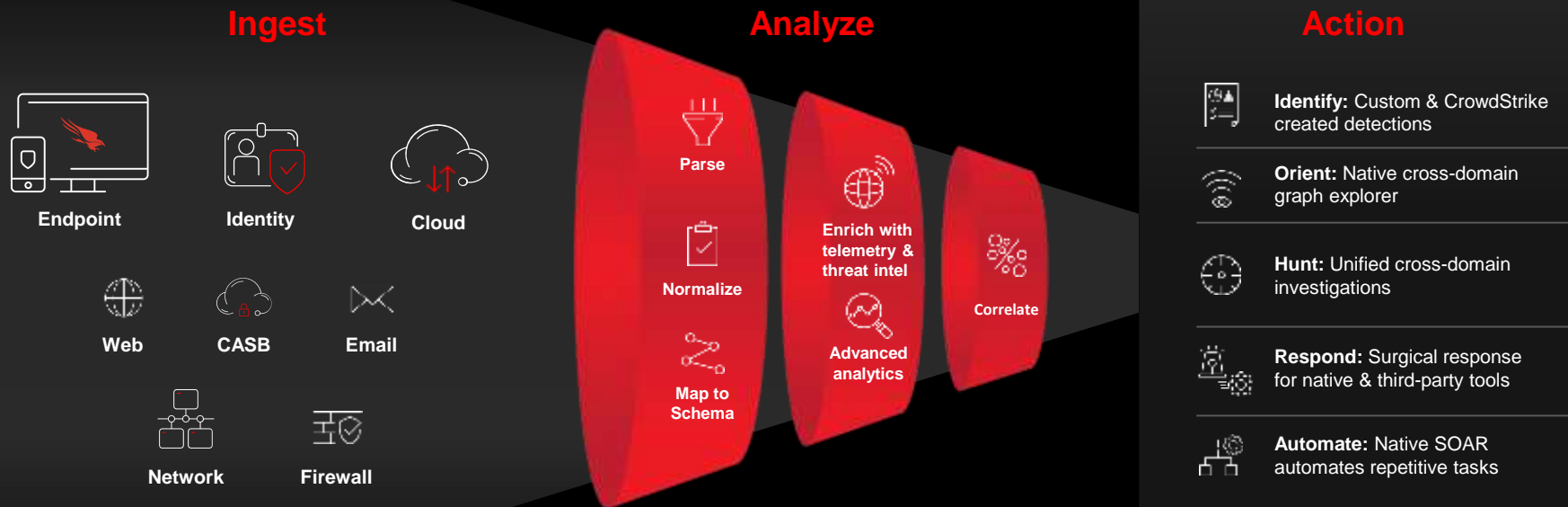
The Data Funnel



PLUG & PLAY

The CrowdStrike Journey

CrowdStrike Insight XDR, the future Blueprint



Conclusion

Did we learn anything?

1

The pain is real, the journey is possible

2

Cover all avenues and telemetry

3

Don't forget about the human



Thank you