

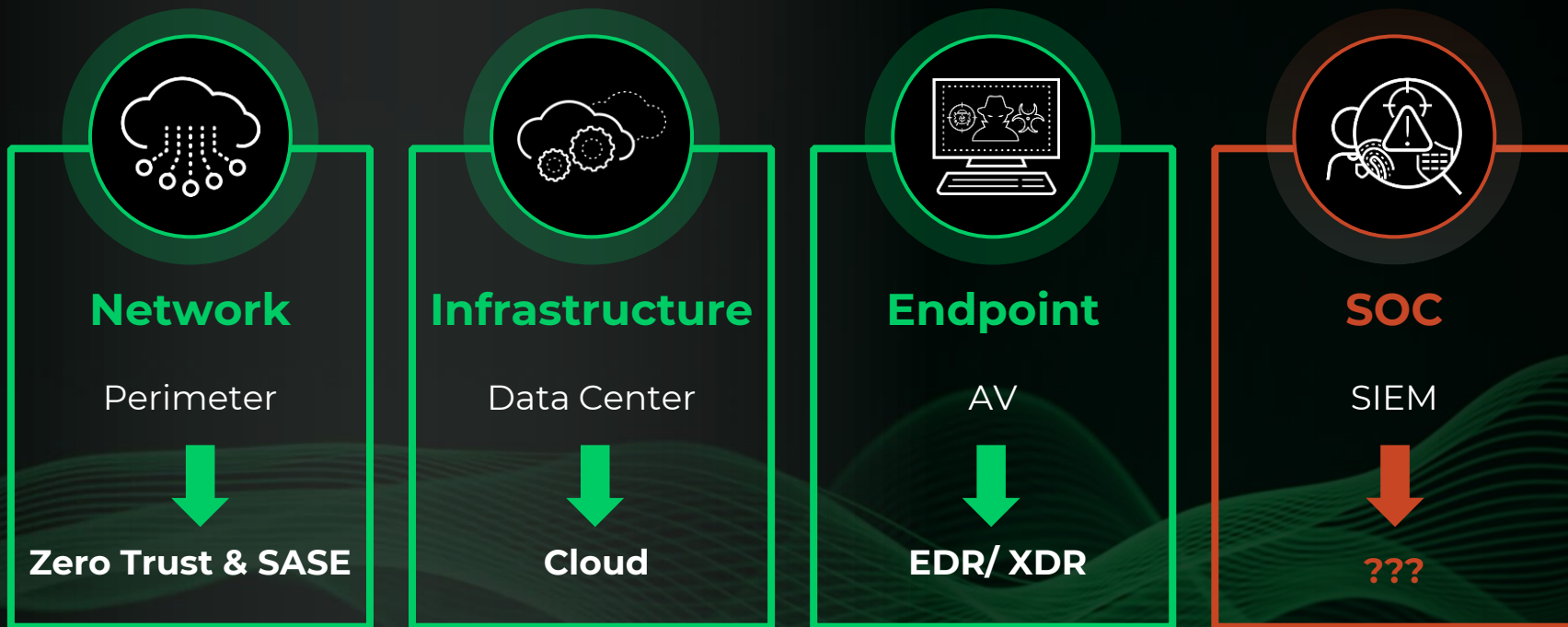
Overcoming SOC's Achilles' Heel:

The Modern SOC, Reimagined

Harri Ruuttila

Consulting Engineer - Cortex - EMEA & LATAM

Most Security Real Estate Has Been Redesigned, Except...



Attacks are happening faster than organizations can respond

Average Days from “Compromise” to “Exfil”¹



Sources:

¹ Unit 42 Cloud Threat Report - Volume 7, 2023, Unit 42 Engagement Experience;

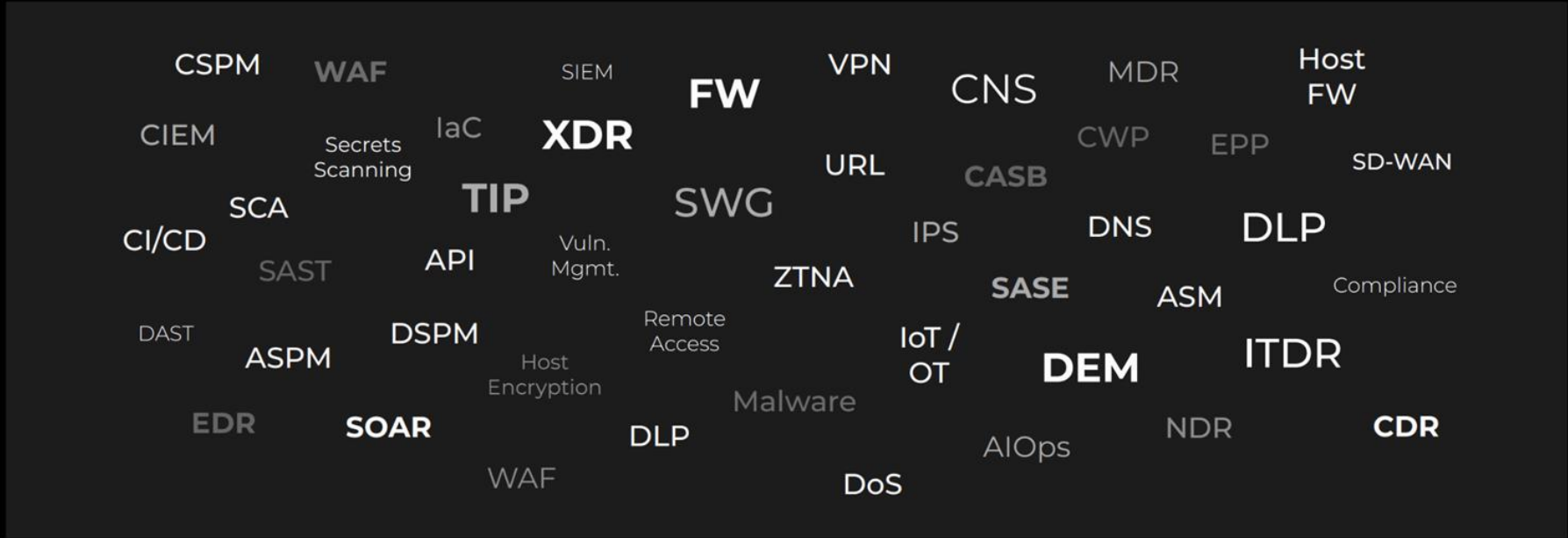
² Under the new SEC Rules, the occurrence of a cybersecurity incident must be reported within four business days of when the incident is determined to be material by the reporting company.



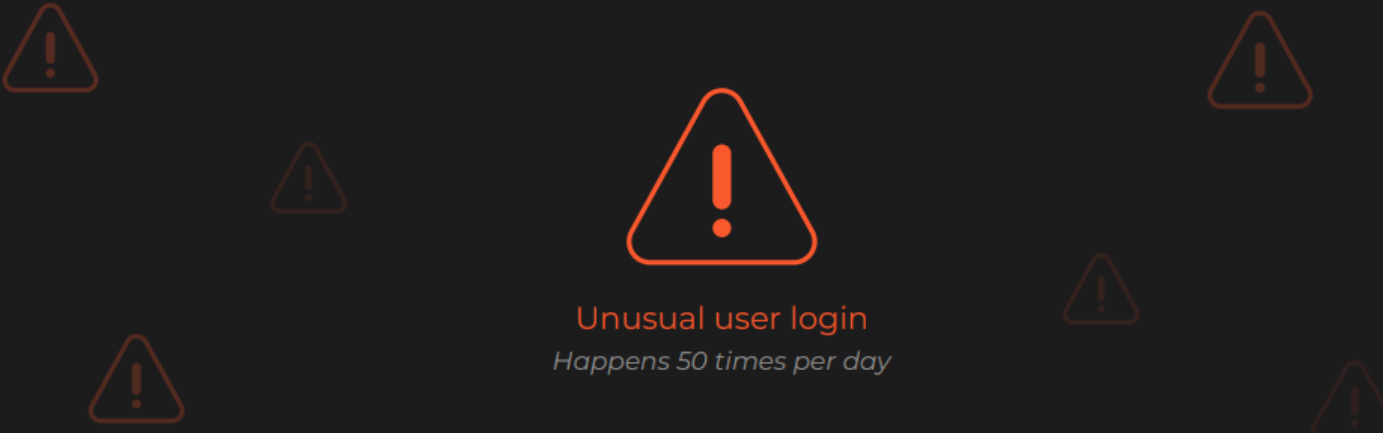
Industry average
6 DAYS
to remediate

SEC adopted rule
4 DAYS
to disclose material
cybersecurity incident²

Industry approach is trying to “solve” the problem with point products



Detecting attacks with siloed tools and data is impossible



Unusual user login
Happens 50 times per day

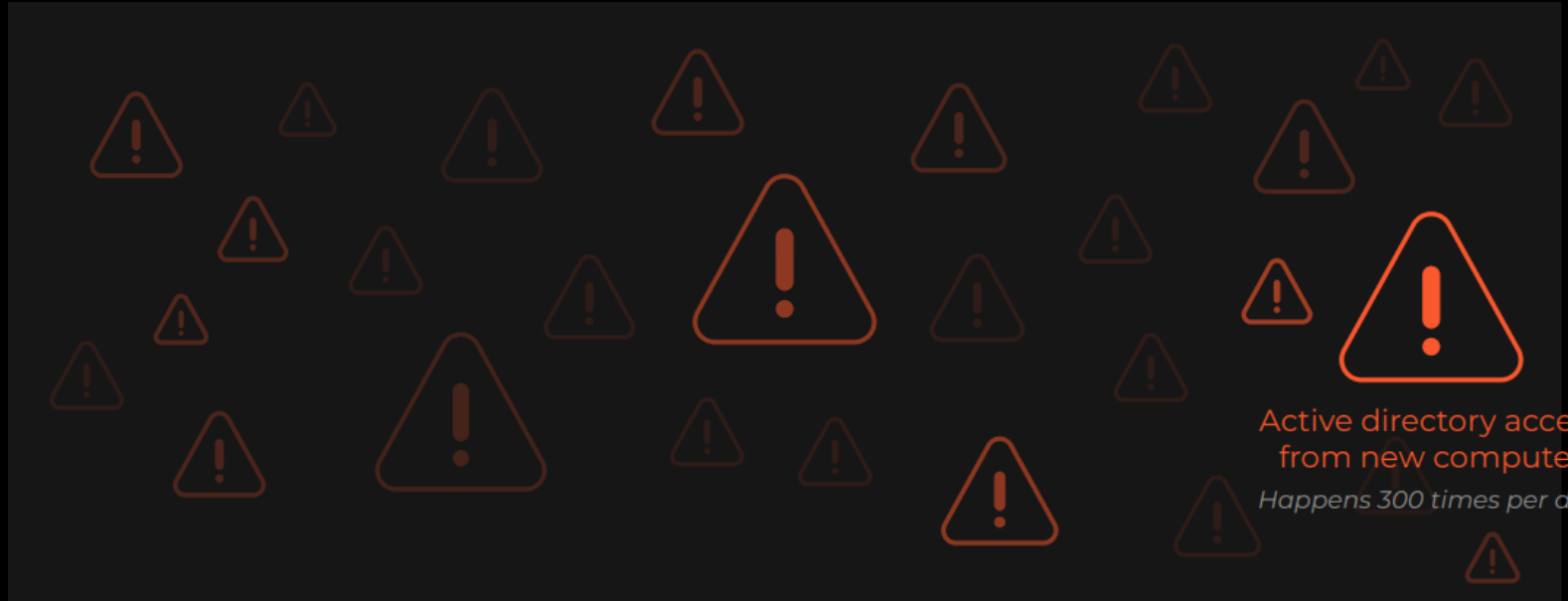
Single event type can be suspicious...

Detecting attacks with siloed tools and data is impossible



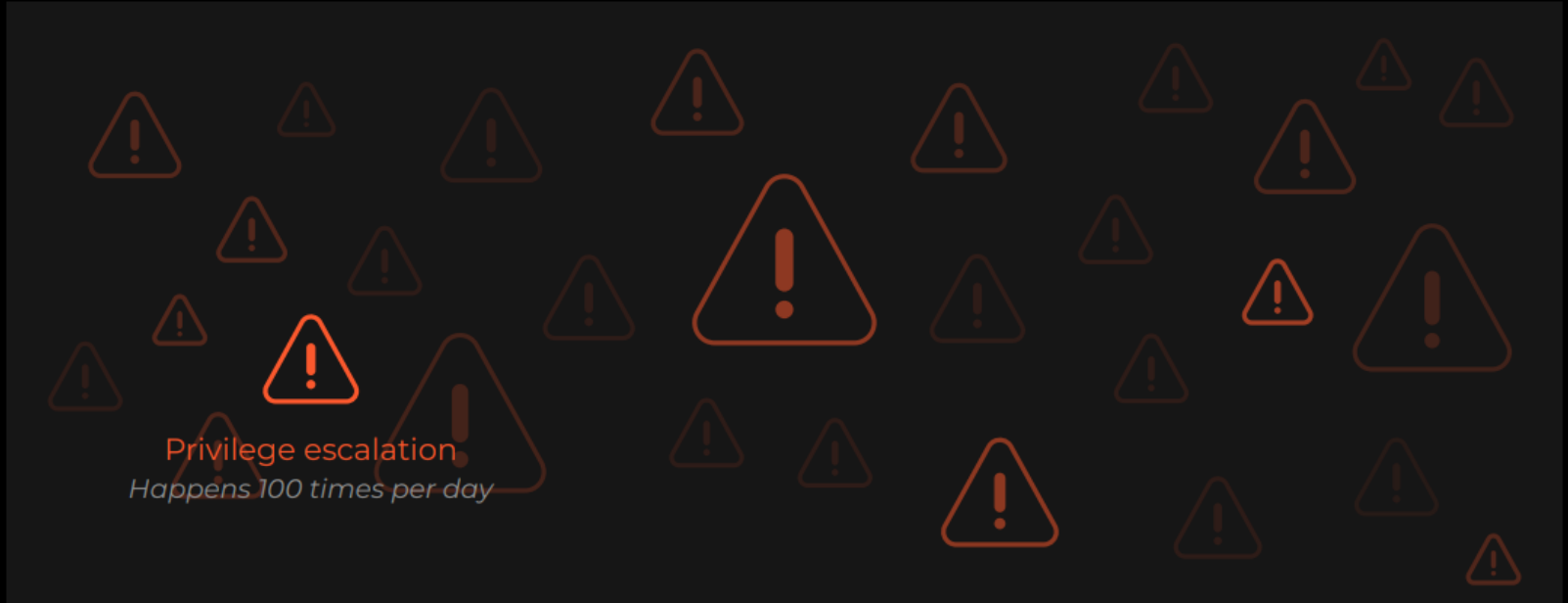
...but they are common and overwhelm the SOC

Detecting attacks with siloed tools and data is impossible



This means attacks are missed...

Detecting attacks with siloed tools and data is impossible



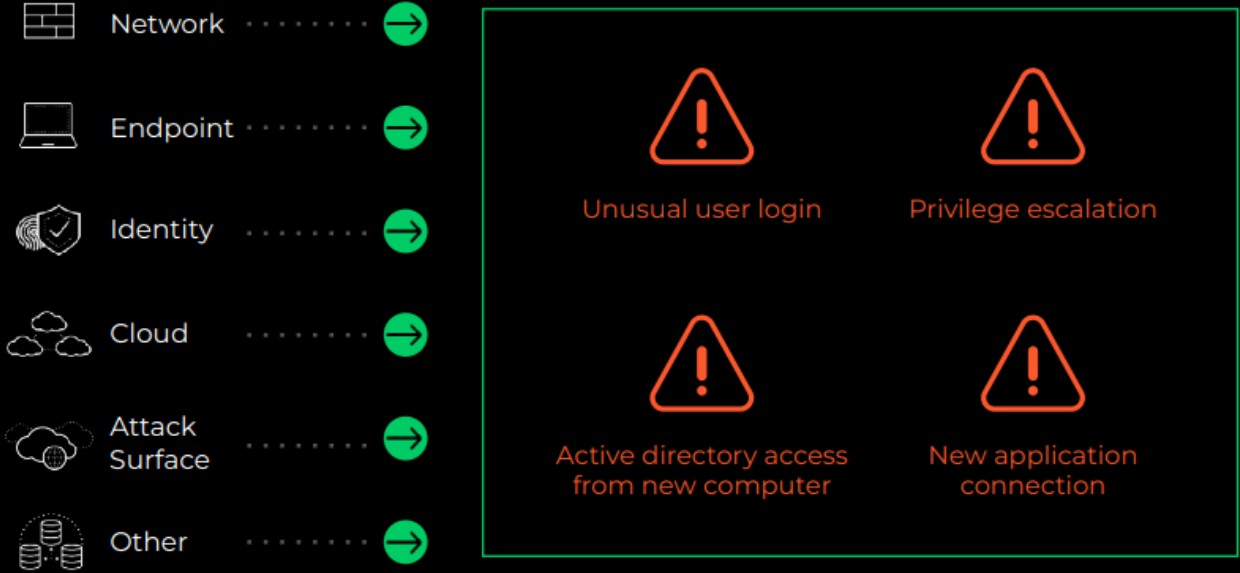
...because of a low confidence to act on any one alert.

Cortex XSIAM

The Autonomous Security
Platform Transforming the SOC

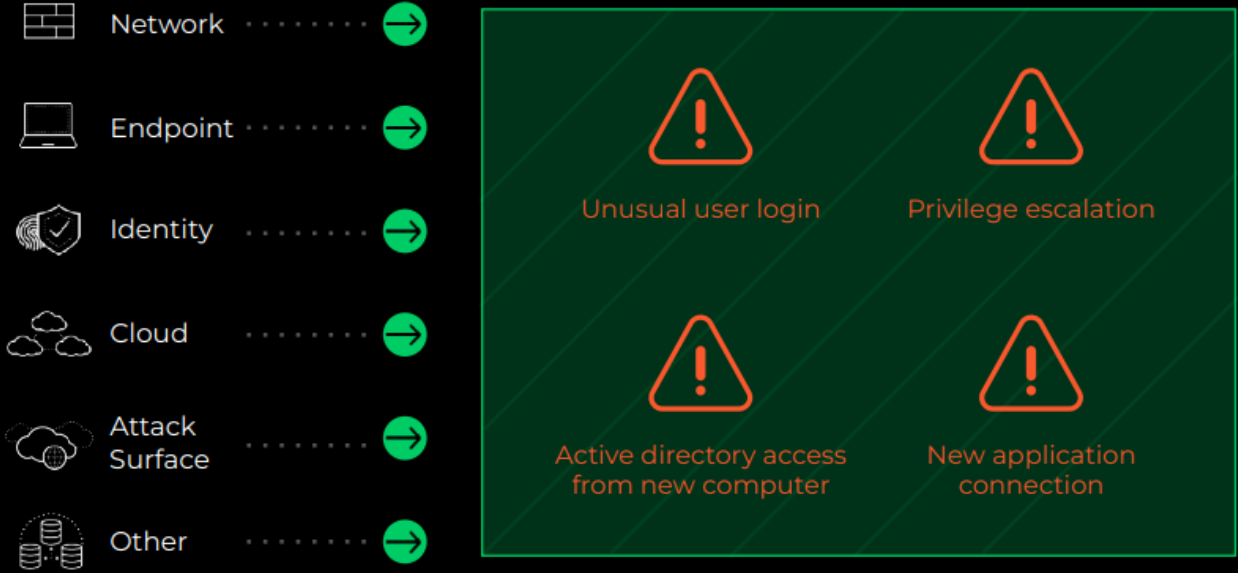


Cortex XSIAM collects complete context and uses the power of AI to detect attacks that siloed tools miss



Stitching and normalizing alerts, augmented with contextual data...

Cortex XSIAM collects complete context and uses the power of AI to detect attacks that siloed tools miss



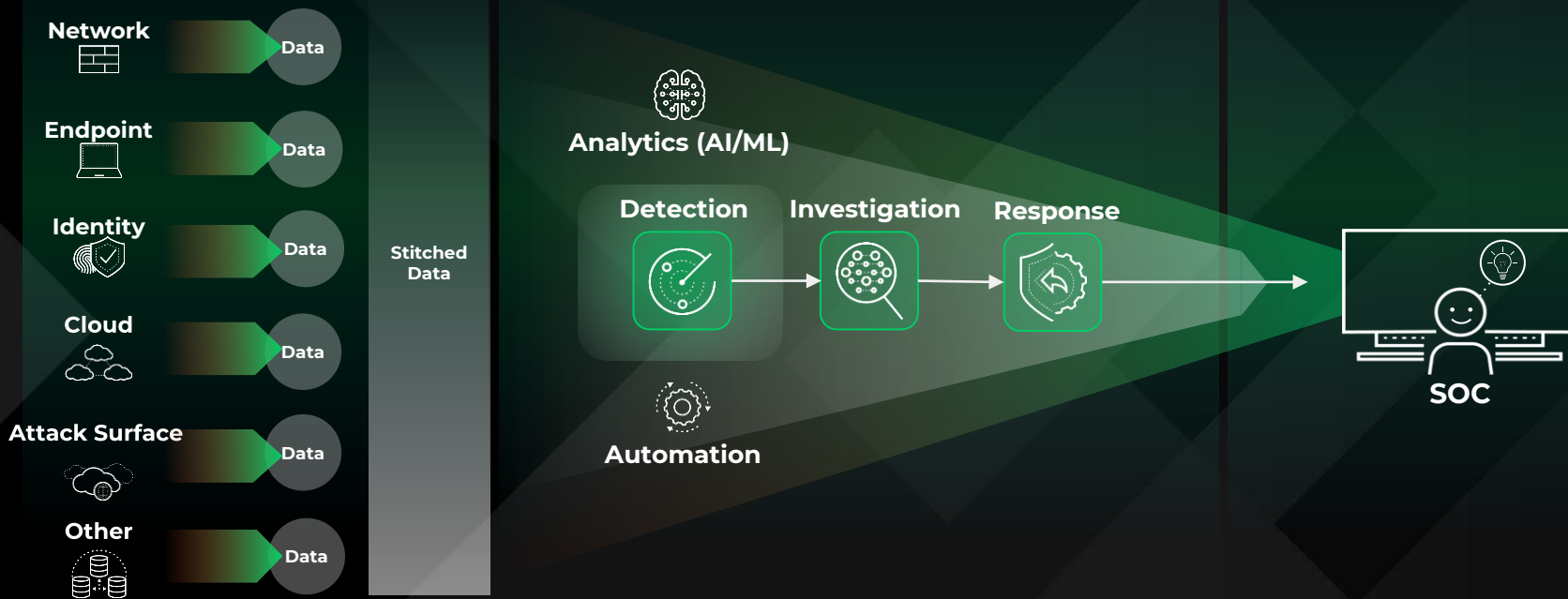
...enables us to automatically respond with high confidence.

We Must Transform the SOC to be Machine-led, Human Empowered

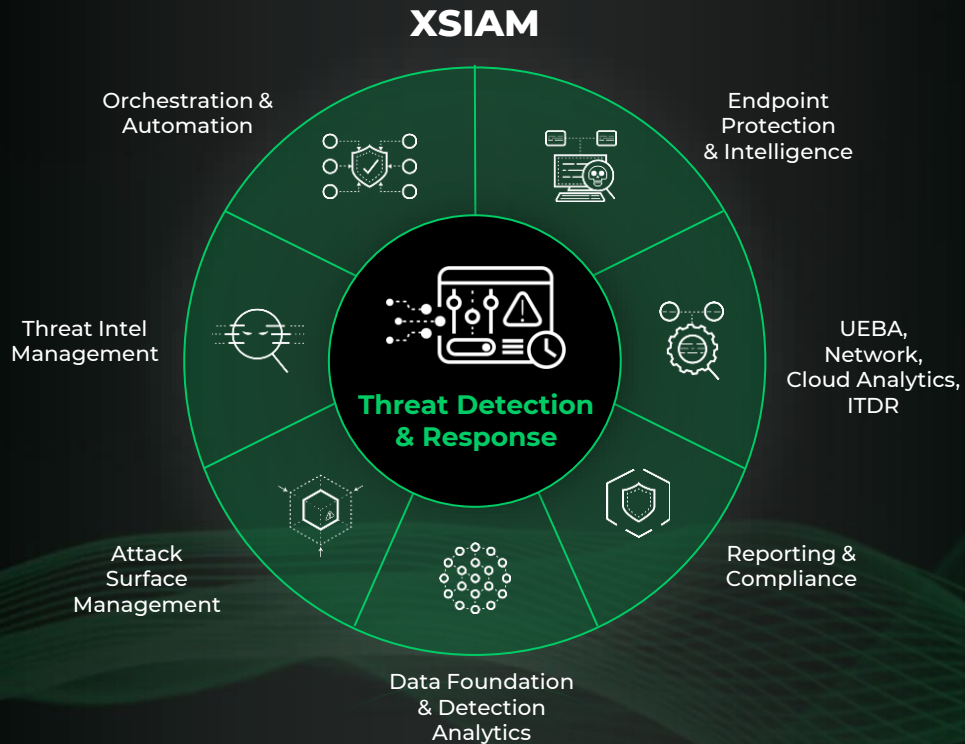
Massive amounts of data improve detection efficacy

Machines automate detection, investigation, and response and make recommendations

Empowered analysts become more proactive



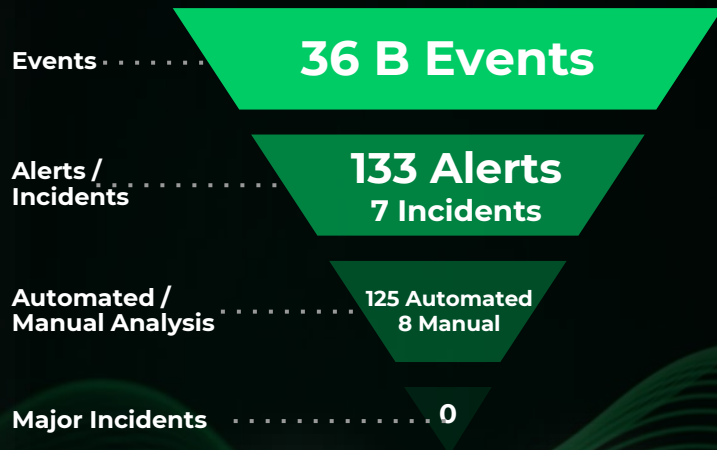
XSIAM Is the Next Big Transformation in Security Operations



XSIAM Is the Next Big Transformation in Security Operations



WHAT'S POSSIBLE WITH THE AUTOMATED SOC



Mean Time
to Detect



Mean Time
to Respond
(High priority)

XSIAM: Three things to remember

AUTOMATION 1st

- From Analyst led to Machine led
- Incidents are unique, alerts repeat

ANY LOG DATA ANY SOURCE

- Ingest, digest and alert on any log data from any source
- Unified backend (including EDR data)

EXTENDABLE

- Supported Content (over 900 packs)
- Threat Intel Management (TIM)
- Attack Surface Management (ASM)
- Identity Threat Detection and Response (ITDR)
- Cortex XDR Included

Thank You!

