CERBERUS SENTINEL

Expensive Toolsets Leaving You Open to Attack?
Close the Gaps with XDR

Recognize any of these challenges?

- Attacks are getting stealthier, evading detection
- Poor ROI on your security tools
- Huge security hire costs
- Silos reducing utility of security information
- Burdensome processes impeding rapid responses
- Security blind spots
- Exposure to costly breaches

Which means...

Slow detection and remediation of attacks -- costs BIG money

Poor visibility and weak defences on multiple assets

Increased opportunity for cyberattacks to penetrate and to remain covert for longer

AVERAGE COST OF A BREACH

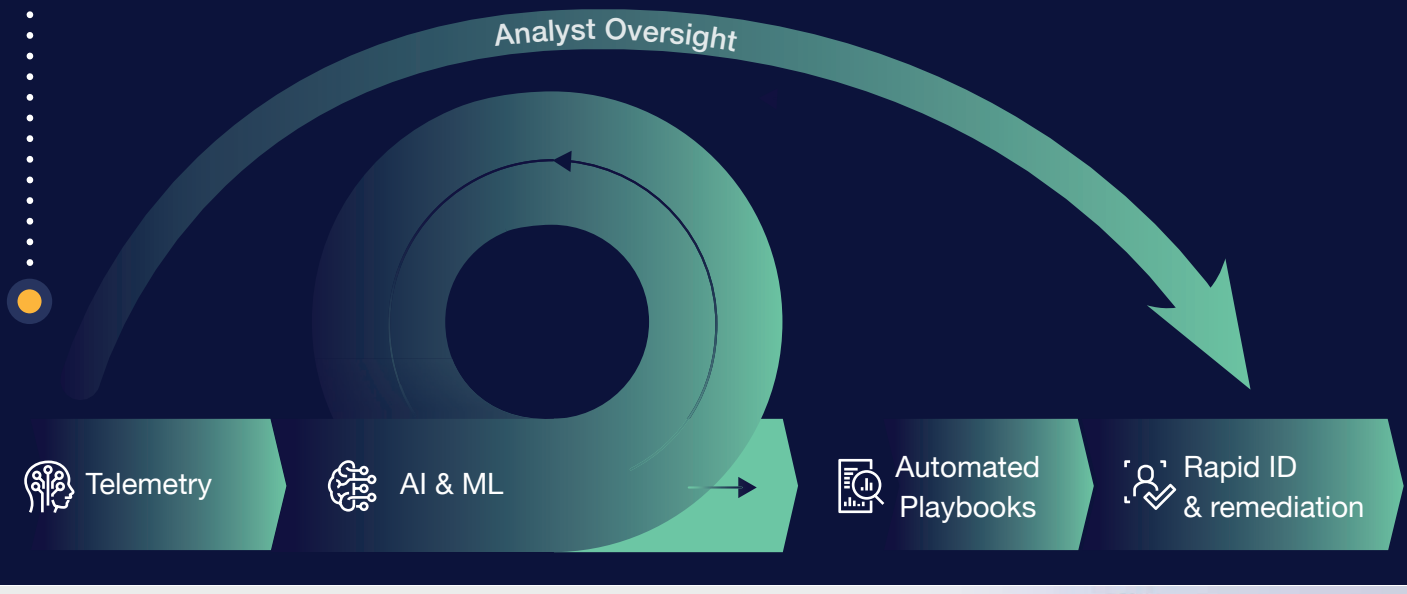
Under 200 days to contain:
$3.61 million

Over 200 days to contain:
$4.87 million

Source: Cost of a Data Breach, Ponemon, 2021

XDR

- Accepts security information from your existing systems
- Leverages customized automation to accelerate threat responses - remediation in minutes, not weeks or months
- Uses behavioral analysis, artificial intelligence and machine learning to spot covert threats
- Leverages the expertise of Cerberus Sentinel's 24/7/365 SOC analysts



Learn more in our white paper,

Will the real XDR please stand up

- What XDR is and how it works
- Why it's rapidly becoming an essential
- What to look for in XDR and what to avoid
- A real world attack (that XDR would have foiled)

DOWNLOAD HERE

CERBERUS SENTINEL

sales@cerberussentinel.com | 866-430-2595 | www.cerberussentinel.com