The Modern SOC Platform

Göran Strandberg
Systems Engineering Specialist, Cortex | Sweden

SOC effectiveness - MTTD/MTTR

Mean Time to Detect (MTTD) is the average time it takes a team to discover a security threat or incident.

Mean Time to Respond (MTTR) measures the average time it takes to control and remediate a threat.

The Proof: We have achieved a 1 min. response time

10 SECONDS

Mean Time to Detect

1 MINUTE

Mean Time to Respond
(High priority)

SOC Challenges

- 24/7
- People / Resourses
- Learn new tools
- Education
- Build integrations
- Repetetive tasks / boring
- Employment period
- MTTD/MTTR

Lots of tools!

Network Detection & Response

DARKTRACE

CISCO

STEALTHWATCH By Lancope

VECTRA

Behavioral Analytics & SIEM

exabeam

IBM

SECURONIX

aruba a Hewlett Packard Enterprise company

Microsoft

splunk>

Endpoint Detection & Response

Carbon Black.

cybereason

CYLANCE

SentinelOne

FireEye

CROWDSTRIKE

Endpoint Protection Platform

Symantec

KASPERSKY lab

TREND MICRO

SOPHOS

McAfee Together is power.

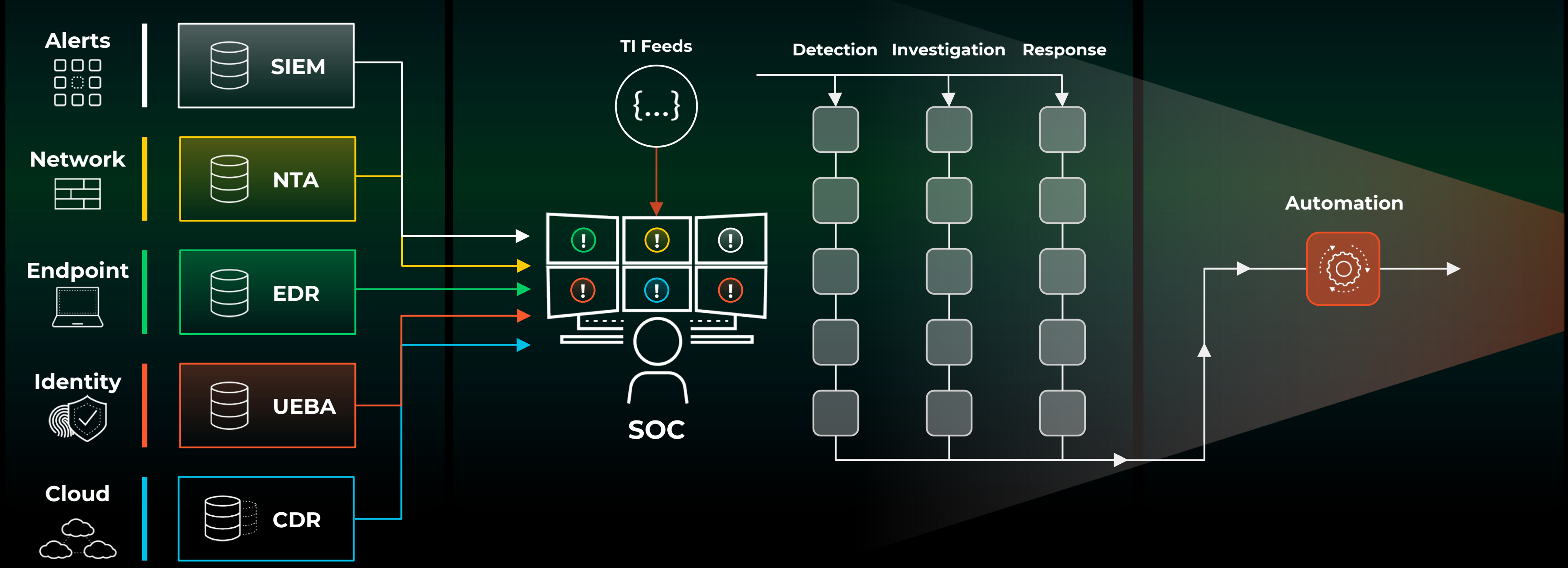
Microsoft

The Current State of the SOCs

Too many data silos make it hard to detect attacks

Teams build and maintain detection content, use multiple tools to manually investigate & respond

Automation is bolted on at the end to scale it



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

Network

Perimeter

↓

Zero Trust & SASE

Infrastructure

Data Center

↓

Cloud

Endpoint

AV

↓

EDR/ XDR

SOC

SIEM

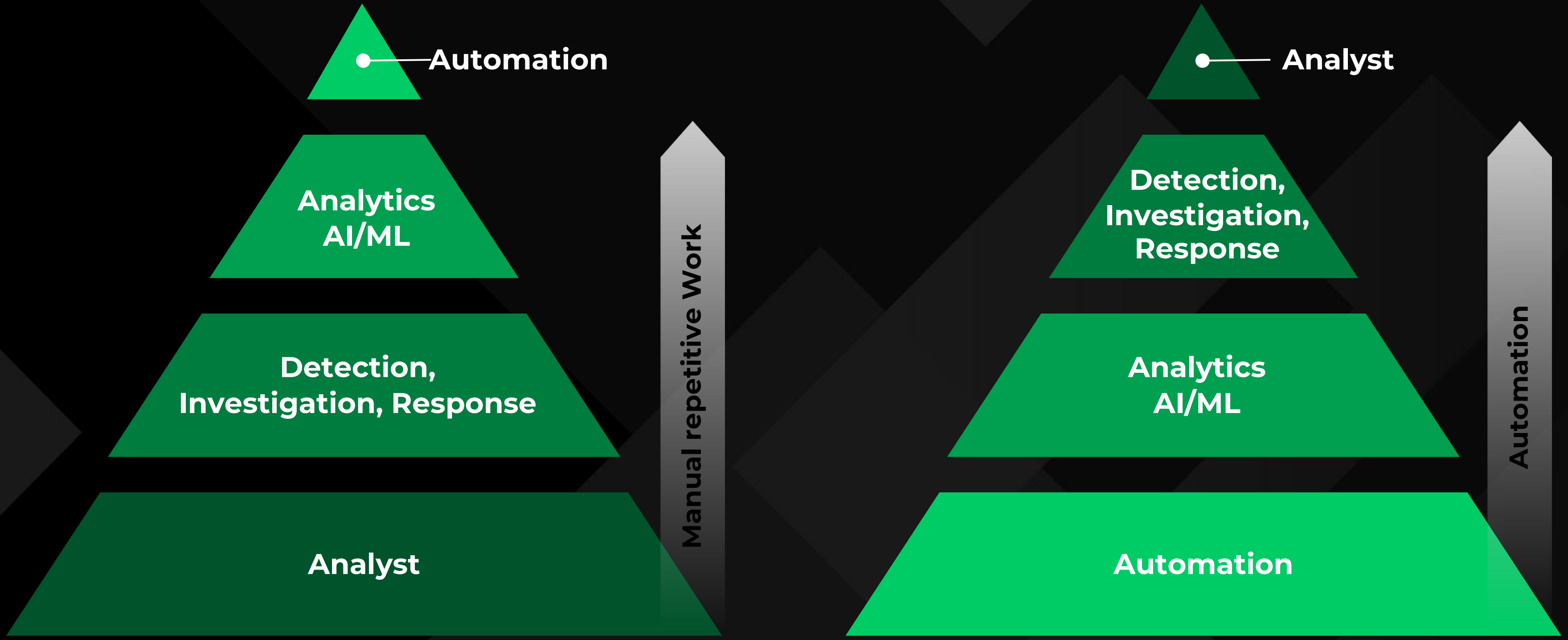
↓

???

Cortex XSIAM

The Autonomous Security Platform
Powering the Modern SOC.

Palo Alto Networks is changing the Focus



Orange Restricted

XSIAM: Designed Around Three Key Concepts

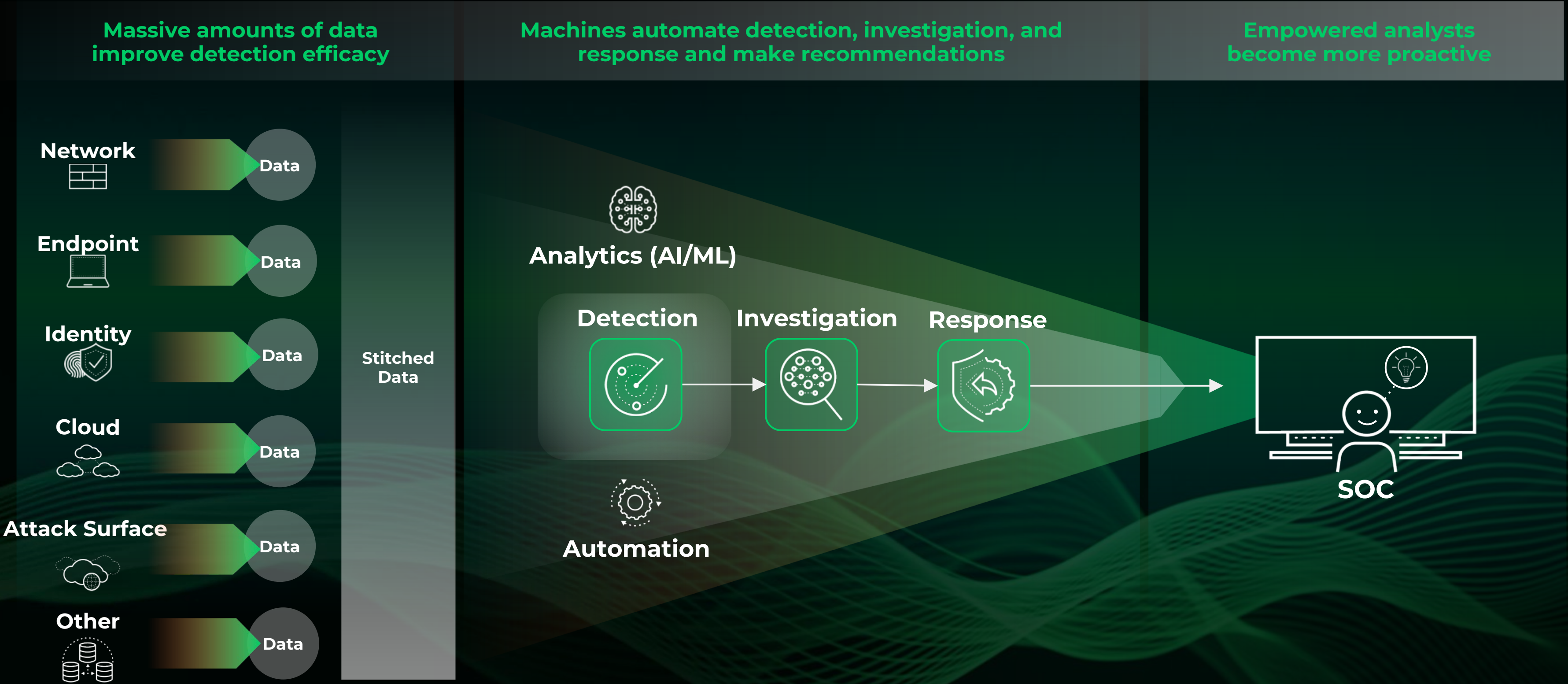
Intelligent Data & Analytics

Automation First

Proactive Security

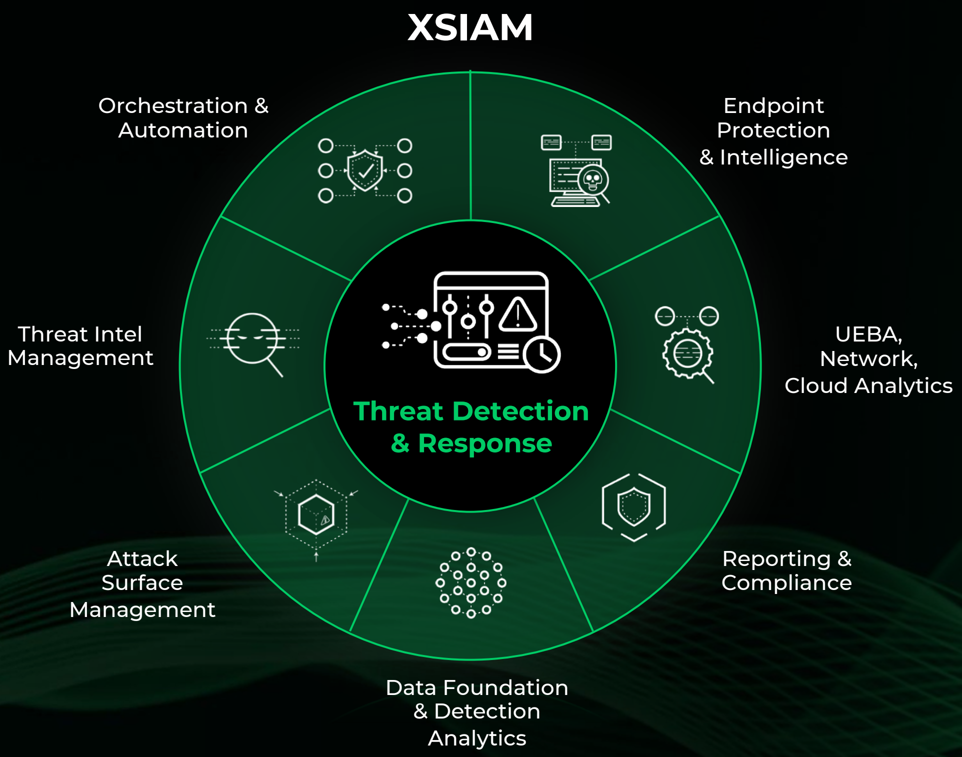
XSIAM delivers a transformation in detection and response, analyst experience, and continuous risk reduction.

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

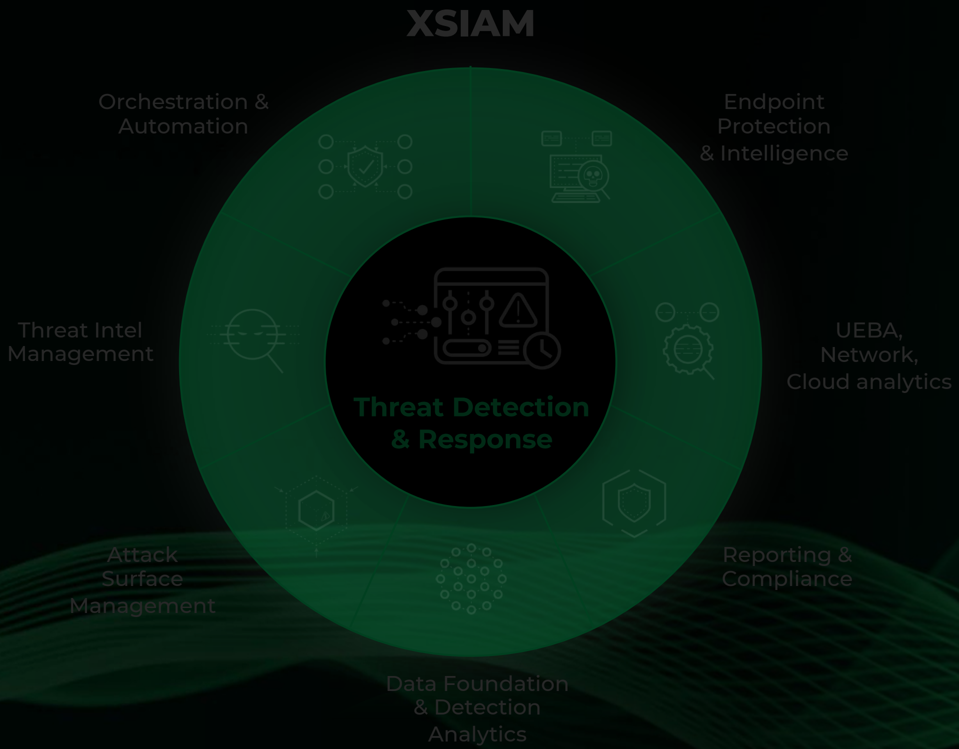


Massive amounts of data improve detection efficacy
Machines automate detection, investigation, and response and make recommendations
Empowered analysts become more proactive
Network
Data
Endpoint
Data
Identity
Data
Cloud
Data
Attack Surface
Data
Other
Data
Stitched Data
Analytics (AI/ML)
Detection
Investigation
Response
Automation
SOC

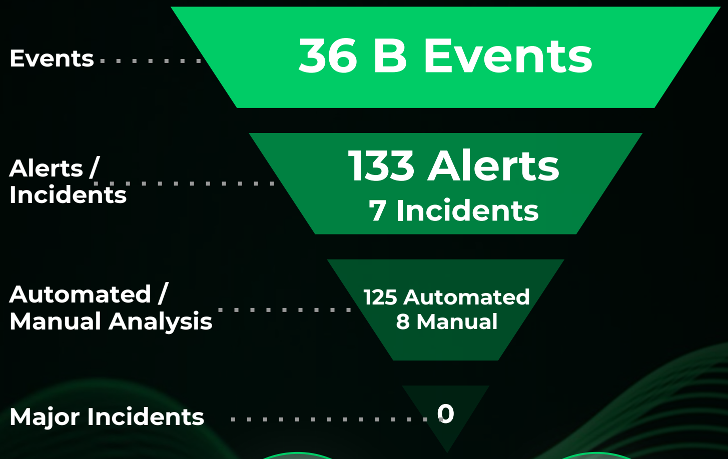
XSIAM Is the Next Big Transformation in Security Operations


XSIAM
Orchestration & Automation
Endpoint Protection & Intelligence
Threat Intel Management
Threat Detection & Response
UEBA, Network, Cloud Analytics
Attack Surface Management
Reporting & Compliance
Data Foundation & Detection Analytics

XSIAM Is the Next Big Transformation in Security Operations


XSIAM
Orchestration & Automation
Endpoint Protection & Intelligence
Threat Intel Management
Threat Detection & Response
UEBA, Network, Cloud analytics
Attack Surface Management
Reporting & Compliance
Data Foundation & Detection Analytics

WHAT'S POSSIBLE WITH THE AUTOMATED SOC



Events: 36 B Events

Alerts / Incidents: 133 Alerts, 7 Incidents

Automated / Manual Analysis: 125 Automated, 8 Manual

Major Incidents: 0

10 SECONDS
Mean Time to Detect

1 MINUTE
Mean Time to Respond
(High priority)

Cortex: A Path to the Modern Automated SOC

Cortex EDR
Advanced Endpoint Protection

Real-time endpoint analysis for malware/threat prevention

Cortex XDR / Cortex XSOAR
Extended Detection & Response / SOC Automation

Endpoint+network+cloud data stitching and analytics for enterprise-wide threat detection

SOC Automation for faster responses

Cortex XSIAM
Security Operations Platform

XDR+automation, extensible detection and data, compliance audit, advanced intelligence

SOC Challenges

- 24/7
- People / Resourses
- Learn new tools
- Education
- Build integrations
- Repetetive tasks / boring
- Employment period
- MTTD/MTTR

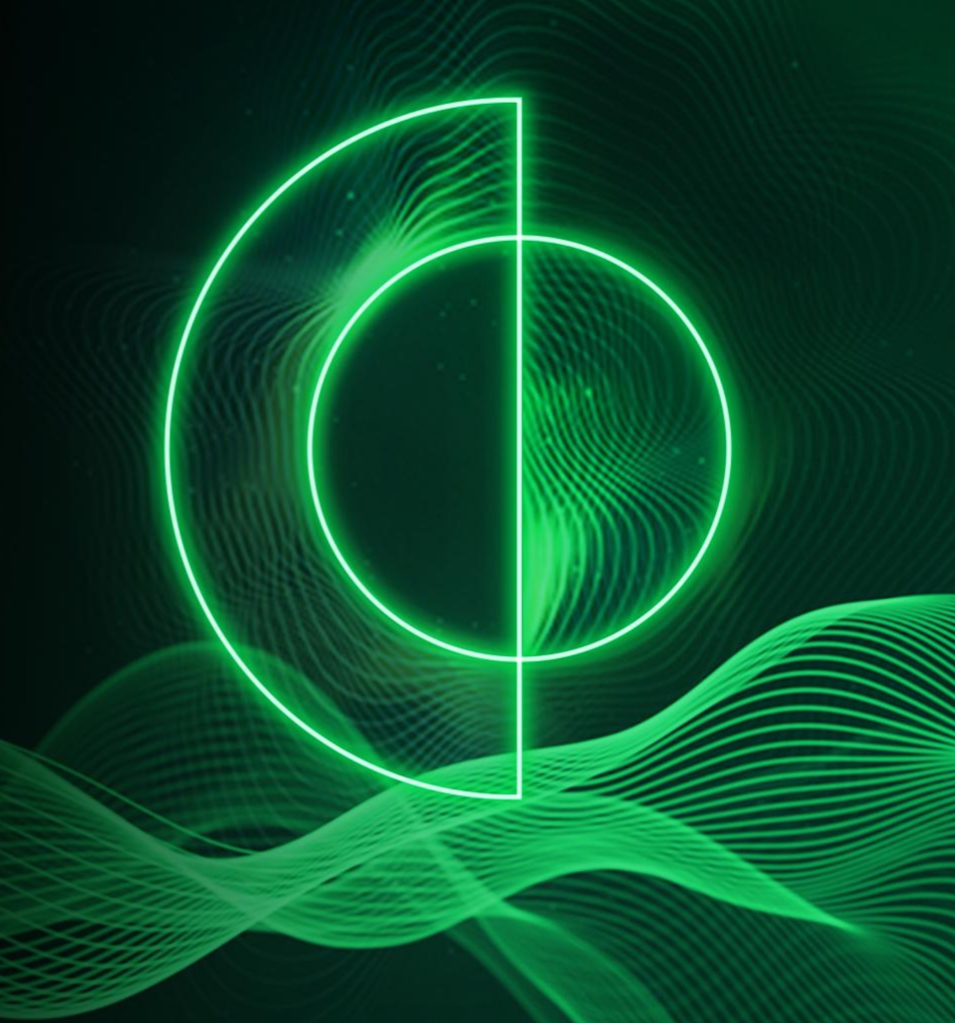
10
SECONDS

Mean Time to Detect

1
MINUTE

Mean Time to Respond
(High priority)

Tack!



Cortex Solution Flexibility & Growth

CHOOSE FROM BEST-IN-CLASS INTEGRATED PRODUCTS

Cortex XDR

Prevent. detect & investigate attacks across the enterprise

Cortex XSOAR

Automate response and improve with every incident

Cortex Xpanse

Discover & protect your entire internet attack surface

SELECT OR EASILY MIGRATE TO A UNIFIED SECOPS PLATFORM

Cortex XSIAM

The autonomous security platform for the modern SOC

COMPLIMENT CORTEX WITH UNIT 42 EXPERT SECURITY SERVICES

Incident Response

Respond in record time with Incident Response and Digital Forensics Services

Proactive Services

Assess and test your security controls against the right threats

Managed Services

Unit 42 monitors and hunts in your environment for anything suspicious.