SOCURA

7 Essentials for Detection and Response

The top capabilities needed to protect your organisation against evolving and sophisticated attacks.

paloalto NETWORKS

The State of Security Operations Today

The stakes for cyber threat detection and response have never been higher. As digital investments grow, so does an organisation's attack surface and Security teams are struggling to keep up with the volume of work generated by siloed threat prevention and detection tools while also trying to be proactive.

Today's siloed tools force analysts to pivot from console to console to verify threats, resulting in missed attacks. Visibility gaps are common, making it harder for analysts to correlate and prioritise events and alerts pertaining to threats. Exhausted analysts and longer mean time to respond (MTTR) will usually follow.

A lack of orchestration and automation is often part of the problem outlined above. It opens the door to extra complexity, human error, slow & manual response, in turn resulting in attacker dwell time being lengthy enough for the threat actor to achieve their objectives (lateral movement, encryption, ransom demands, data destruction, data exfiltration, and extortion).

In this eBook we outline 7 capabilities that will help overcome some of these challenges and protect your organisation against evolving and sophisticated attacks.

11,047 Alerts a Day

Security teams need help keeping up with an endless backlog of alerts. Analysts face a deluge of alerts – 11,047 alerts a day on average*. This can cause many teams to ignore low-priority alerts.

A shortage of over 3 million security professionals

Organisations can't hire and retain the seasoned analysts they need. Faced with a shortage of over 3 million security professionals worldwide, organisations are increasingly turning to managed services to augment their SecOps team. MDR services can be deployed rapidly.

*2021 State of SecOps Report, Forrester Consulting

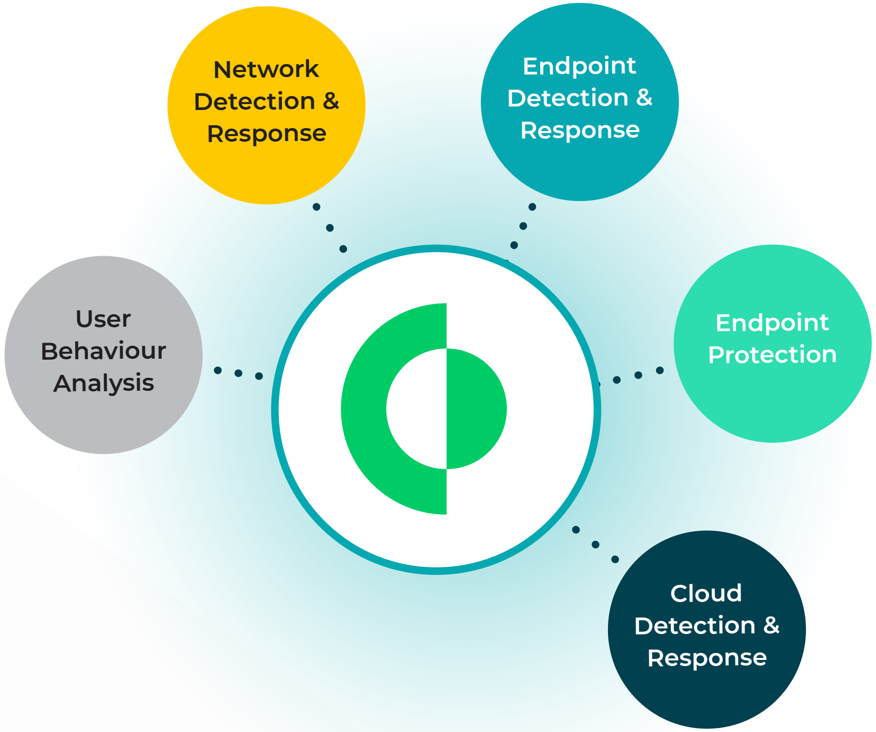
Visibility Across Data Sources

To reduce the risk of a successful attack, you need a holistic approach to detection and response that eliminates blind spots, increases accuracy, and streamlines investigations.

We need to stitch together events across cloud, network, and endpoint layers for comprehensive insight - an approach known as extended detection and response (XDR).

XDR accelerates investigations by providing a complete picture of every threat and automatically revealing the root cause. Intelligent alert grouping and alert deduplication simplify triage and reduce the experience required at every stage of security operations. Tight integration with enforcement points lets analysts respond to threats quickly.

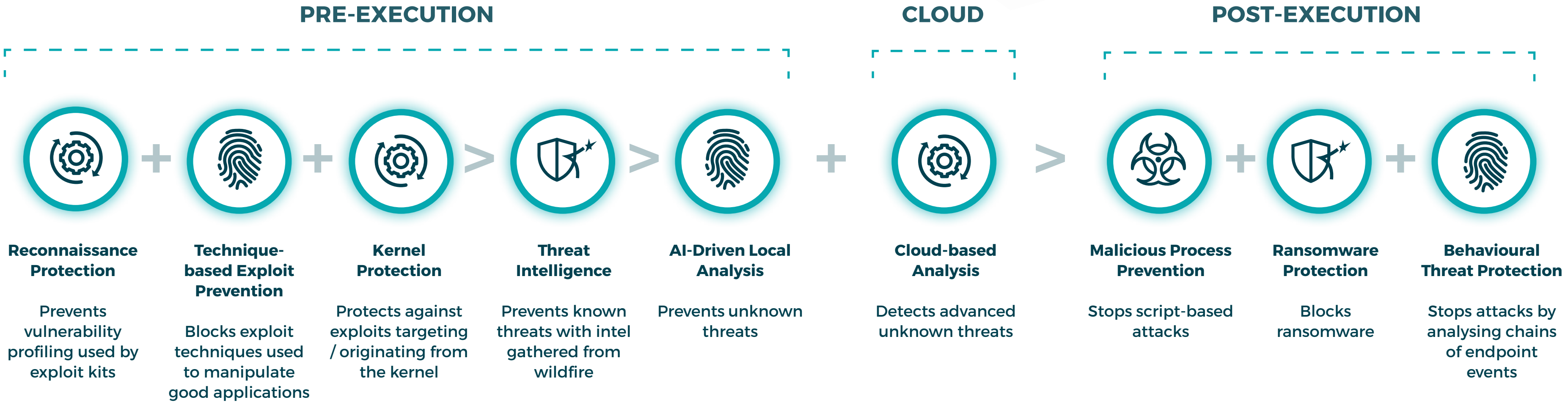
The Socura service is built upon Cortex XDR, the industry's first extended detection and response platform that natively integrates endpoint, network and cloud data to stop sophisticated attacks. By correlating and analysing threats across networks, cloud, identity, and endpoint you can simplify and strengthen threat protection.


Network Detection & Response
Endpoint Detection & Response
User Behaviour Analysis
Endpoint Protection
Cloud Detection & Response

2 Best-in-Class Attack Prevention

To shield your endpoints, you need ironclad protection that blocks known and unknown malware, fileless attacks and exploits.

Adversary strategies have evolved from simple malware distribution to a broad set of automated, targeted, and sophisticated attacks that can bypass traditional endpoint protection.



PRE-EXECUTION

Reconnaissance Protection
Prevents vulnerability profiling used by exploit kits

+

Technique-based Exploit Prevention
Blocks exploit techniques used to manipulate good applications

+

Kernel Protection
Protects against exploits targeting / originating from the kernel

>

Threat Intelligence
Prevents known threats with intel gathered from wildfire

>

AI-Driven Local Analysis
Prevents unknown threats

+

CLOUD

Cloud-based Analysis
Detects advanced unknown threats

>

POST-EXECUTION

Malicious Process Prevention
Stops script-based attacks

+

Ransomware Protection
Blocks ransomware

+

Behavioural Threat Protection
Stops attacks by analysing chains of endpoint events

Cortex XDR provides everything you need for threat prevention, detection and response with a single, cloud-native agent. It safeguards your endpoints with battle-tested and proven next-gen antivirus.

3 Simplified Investigations

Today's siloed security tools generate endless alerts with limited context. To reduce response times, security tools must provide a complete picture of incidents with rich investigative details.

By aggregating alerts and indicators of compromise (IOCs) from detection sources - XDR, SIEM, security analytics solutions, network security tools, threat intelligence feeds, mailboxes and more - and then executing automatable, process-driven playbooks to enrich and respond to these incidents, you can streamline security processes and connecting disparate security tools.

These playbooks coordinate across technologies, security teams, and external users for centralised data visibility and action. Cortex XDR also helps to simplify investigations by automatically revealing the root cause, sequence of events, and threat intelligence details of alerts from any source.

Socura's MDR service benefits from simplified security operations by unifying case management, real-time collaboration, threat intelligence management, and automation of containment actions.

88%

Reduction in investigation time

with Cortex XDR by revealing the root cause of alerts from any source.

98%

Alert reduction

due to intelligent alert grouping and deduplication using Cortex XDR.

4 Analytics and Machine Learning

You need a comprehensive set of machine learning and analytic techniques to stay ahead of rapidly evolving threats.

Security orchestration, automation, and response (SOAR) allows security teams to efficiently carry out security operations and incident response whilst maintaining the right balance of machine-powered security automation and human intervention. You also need:

AI-driven local analysis to block malware

Behavioural analytics to detect intrusions and active attacks

Global analytics to improve detection accuracy and coverage

This is no time for relying solely on signatures and static rule-based approaches alone. Your tooling must evolve to adapt to the use of LOLBins and other covert techniques such as lateral movement with stolen credentials. Behavioural detection uses machine learning to baseline normal behaviour across both managed and unmanaged devices. The idea is that, once trained, it will be able to spot suspicious activity more easily. Enhanced with local business context, such as who are your VIP users and which are your critical devices, it can offer a much-enhanced method of threat detection whilst improving the effectiveness of incident response efforts.

Cortex XDR profiles user, endpoint and network behaviour whist machine learning models develop a baseline of expected behaviour to detect anomalies indicative of attacks and uncover stealthy threats.

5 Coordinated Response

The cyber security industry has a problem. Global spending continues to rise, yet this rise in spending doesn't correlate with a decrease in breaches.

Back in 2015 it took on average 206 days to identify a breach, and many more to contain it. Fast forward five years and the situation had greatly improved, with the global median dwell time dropping below one month (24 days) for the first time in 2020 (although the report* also noted that "...it is also likely the preponderance of ransomware that helped drive down the time between initial infection and identification").

However, 24 days is still plenty of time for threat actors to achieve their objectives. We need to get faster at catching and evicting them, reducing their dwell time such that it can be measured in hours or minutes, not days.

In order to do that, there needs to be increased focus on the common sources of hidden malicious behaviour inside organisations. Let's explore that and some best practices to mitigate the risk.

Visibility, context, and control is the name-of-the-game for IT security teams. But it can be a challenge even understanding the size of the organisation's existing endpoint and cloud environment, let alone securing it. Several best practice approaches are worth considering here:

1. An XDR/MDR approach

Cortex XDR lets your security team instantly stop the spread of malware, isolate endpoints, run scripts, and even restore endpoints without reimaging devices. With Search and Destroy, you can even sweep across all endpoints in real time to find and delete malware.

2. Behavioural analysis

As mentioned on the previous page, behavioural detection uses machine learning to baseline normal behaviour across both managed and unmanaged devices. The idea is that, once trained, it will be able to spot suspicious activity more easily.

3. Zero Trust

Another best practice many organisations are increasingly adopting is zero trust - an approach which boils down to "never trust, always verify." It's formulated around the idea that you must remove inherent trust from the network, treat it as hostile and instead gain confidence that you can trust a connection.

*M-Trends 2021, Fireeye

6 A Flexible Suite of Endpoint Protection

Addressing security challenges and visibility gaps in the post-Covid era is no mean feat. Aside from securing adequate resourcing and funding, CISOs need to put in place the tools and processes to tackle the growing levels of threat as well as their evolving sophistication.

Find out how the pandemic has introduced a new era of cyber security sophistication in our **blog**. To overcome these new security challenges and visibility gaps, you need an easy way to identify and prioritise endpoint risks, reduce your attack surface, and stop data loss:

Host firewall

Centrally manage inbound and outbound communications on your endpoints.

Disk Encryption

Apply encryption or decryption policies on your endpoints and view lists of all encrypted drives.

Vulnerability Assessment

Ensure you have real-time visibility into vulnerability exposure and current patch levels across all your endpoints.

Device Control

Monitor and granularly control USB access to protect your endpoints from data loss and malware.

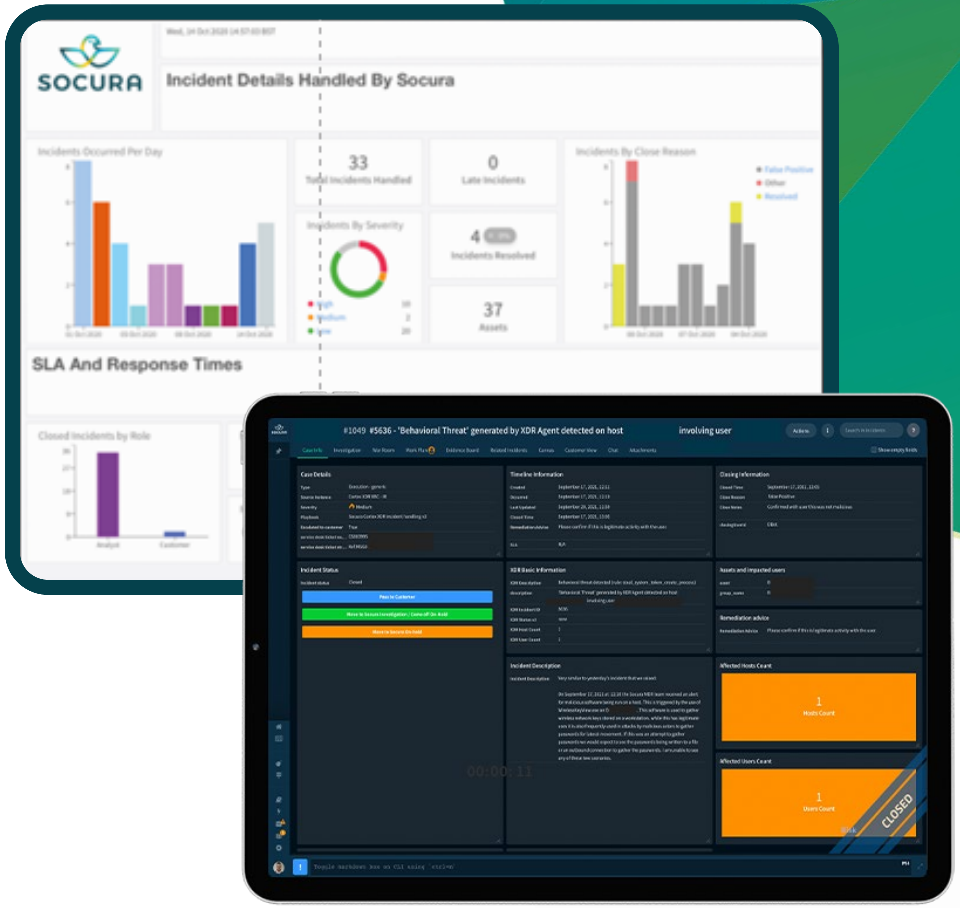
7 Autonomous Security Operations

Manual processes slow down incident response and increase the cost of security operations. To move at pace, analysts need to be able to:

- Automatically collect and update incident information from the XDR tool
- Present detailed context including the severity, timeline and affected hosts and users of security incidents
- Use incident playbooks to streamline investigations by automatically assigning owners to incidents, performing enrichment and reputations checks, plus much more
- Receive notifications, review incidents and perform tasks from their mobile device

The Socura MDR service is built from the ground up on a security orchestration, automation and response (SOAR) platform that will deliver all of the above and allow our team to support yours by helping to manage alerts from any source, standardise processes to act upon those alerts using playbooks, act upon threat intelligence, and automate response for any security use-case.

Our clients can interact with live incidents and work collaboratively with the Socura team to minimise the threat and secure their environment.



Why Socura?

Setting up an effective detection and response program is easier with a helping hand.

MDR is increasingly favoured, as building and manning a 24x7 security operations centre (SOC) in-house is hard to justify from a cost perspective. Organisations can instead utilise the economies of scale that a specialist provider offers, and the enhanced visibility they have into multiple customer environments.

The Socura MDR service offers a 24×7 proactive threat detection, hunting and response capability that identifies and contains cyber threats in near real-time.

Our service is designed to protect organisations of all sizes from data breaches, reduce attacker dwell time, and negate the impact of any malicious activity on your business operations. Our partnership approach makes this happen by collecting the right data, at the right time - with no compromises.

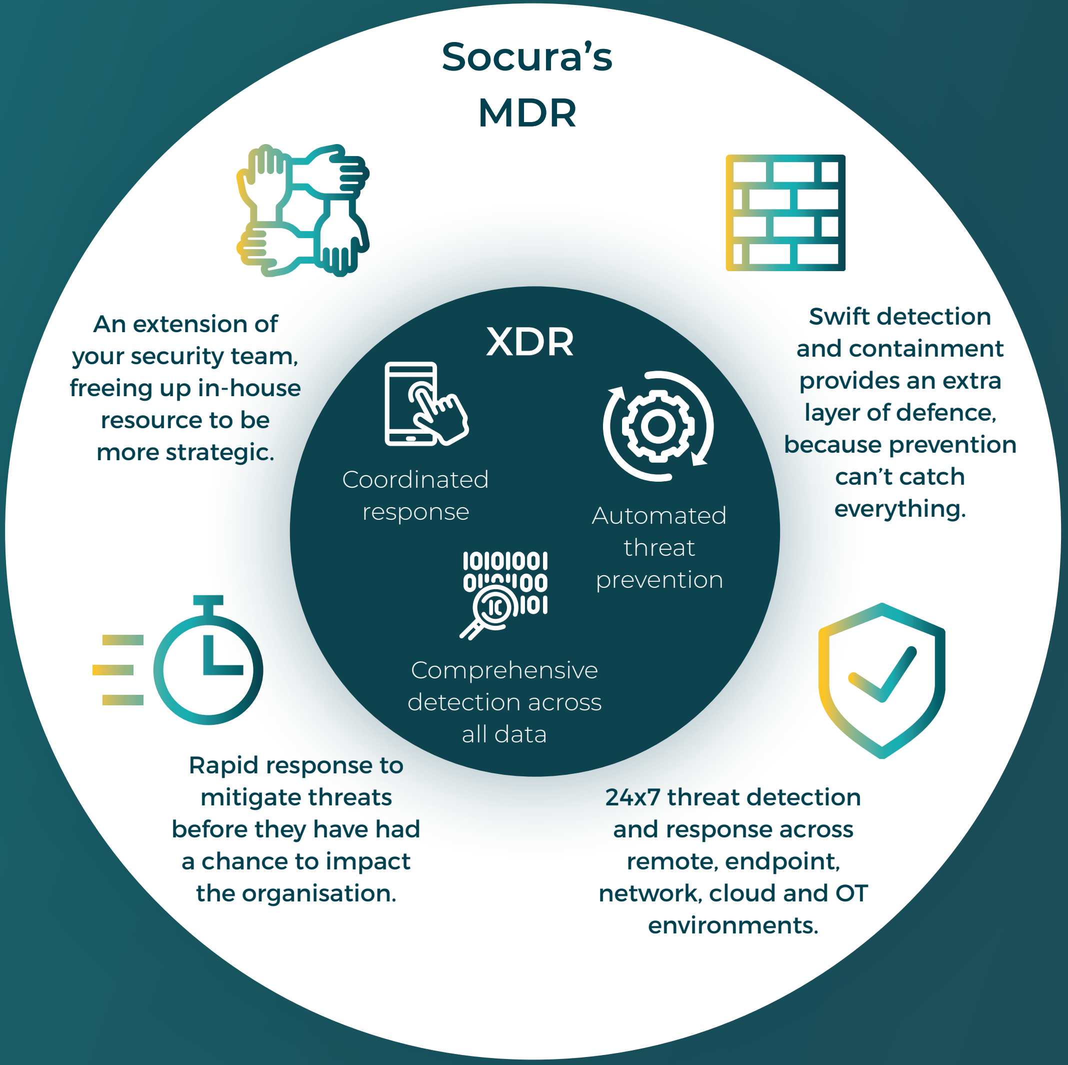
- Detection and response
- Monitoring and triage
- Expert security analysis
- Dedicated, proactive threat hunting
- Guided remediation actions

This is MDR built for a world of heightened digital risk. With Socura you get a trusted partner that works as an extension of your own security team, but with the support of the latest cloud-based and machine-powered security technologies.

Did you know?

"Nearly 50% report struggling to hire and retain the right staff to manage workloads." Forrester (2021).

State Of SecOps In 2021 Report



Socura's MDR

An extension of your security team, freeing up in-house resource to be more strategic.

Swift detection and containment provides an extra layer of defence, because prevention can't catch everything.

Rapid response to mitigate threats before they have had a chance to impact the organisation.

24x7 threat detection and response across remote, endpoint, network, cloud and OT environments.

XDR

Coordinated response

Automated threat prevention

Comprehensive detection across all data

SOCURA

Socura Limited Registered in England No. 12200836 I Email: hello@socura.co.uk I SOCURA 2021. All rights reserved