Infopercept

Secure . Optimize . Strengthen

An introduction to OODA - Observe, Orient, Decide and Act Strategy for Strengthening your Cyber Security Posture

Table of Contents

Setting the Context 3

OODA Strategy 4

Security Architecture 7

An Integrated Approach 9

Key Benefits of this Approach 11

Way Forward 12

Contact Us 13

Setting the Context

This whitepaper explores an approach where we can bring together an integrated platform consisting of strategy, solutions, and services to effectively detect and respond to cyberattacks on an ongoing basis. As any reader is aware, we have a myriad of technologies and service offerings that touch upon one or some of these critical areas and not all. The challenge with such an approach is that the organization and the team miss the bigger picture and always fall short of putting the right foot forward when it comes to detecting and responding to attacks in real-time.

Current Challenges:

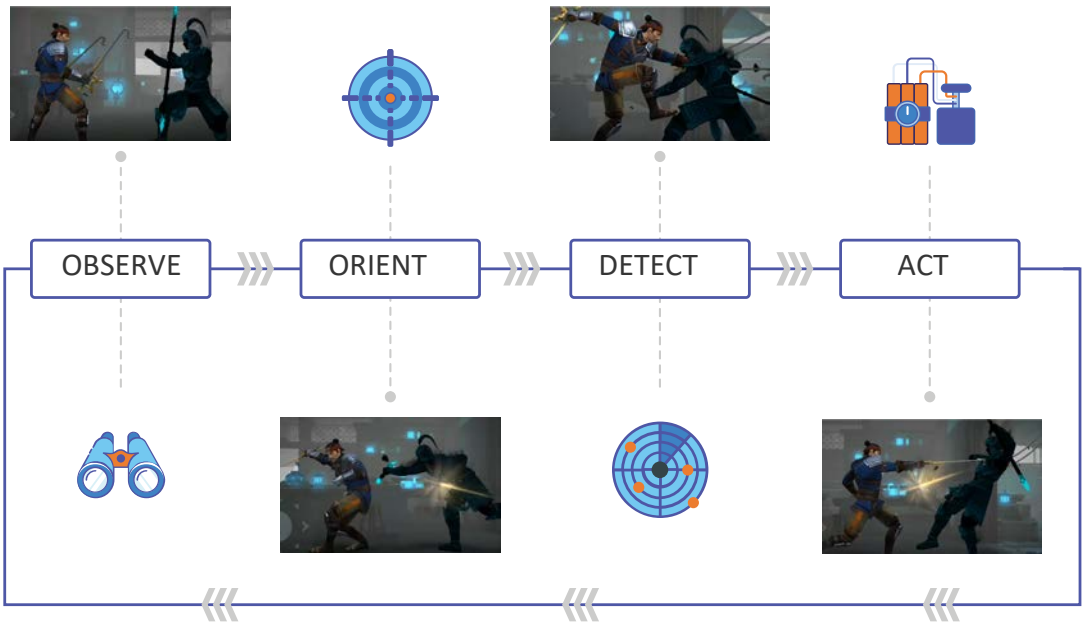
Currently we are spending a lot of time skimming through event logs and performing pattern analysis to eventually arrive at detecting a breach. This is time consuming and what is missing out is the tighter integration of Intelligent Security Orchestration and Automation solutions and approach. As many studies prove, any organization is losing anytime between 1 month to a year or more in finding out about a breach or an attack. This is a costly affair as we are left with not many options after. Another drawback with this approach is the lacklustre Incident Response Strategy and the overall delay with it. We are faltering at two places – one at the incident detection and the other at the response stage. Irrespective of all these, we are spending huge amounts of money in procuring tools and technologies that do not integrate well with each other or rather fit the overall objectives.

What shall be the approach then?

What we need in such a scenario is developing an Integrated platform that brings together the strategies, services, and solutions, it takes to detect and respond to any sophisticated attacks on an ongoing basis. We achieve a one-stop solution for the problem rather than multiple technologies and approaches that would not serve the purpose in the long run. What we introduce here is a concept called “OODA” (Observe; Orient; Decide; Act; and Adapt) whereby solutions such as SIEM, SOAR and EDR are all brought under one platform wherein one would get a unified approach to detect and respond to cyberattacks on an ongoing basis.

OODA Strategy

Security Optimization is the key here. We shall need to put in a simple and coercive strategy that answers “Why” we do this in the first place. Why we do this is to achieve the overall objective of detecting and responding to cyberattacks on a real-time basis.

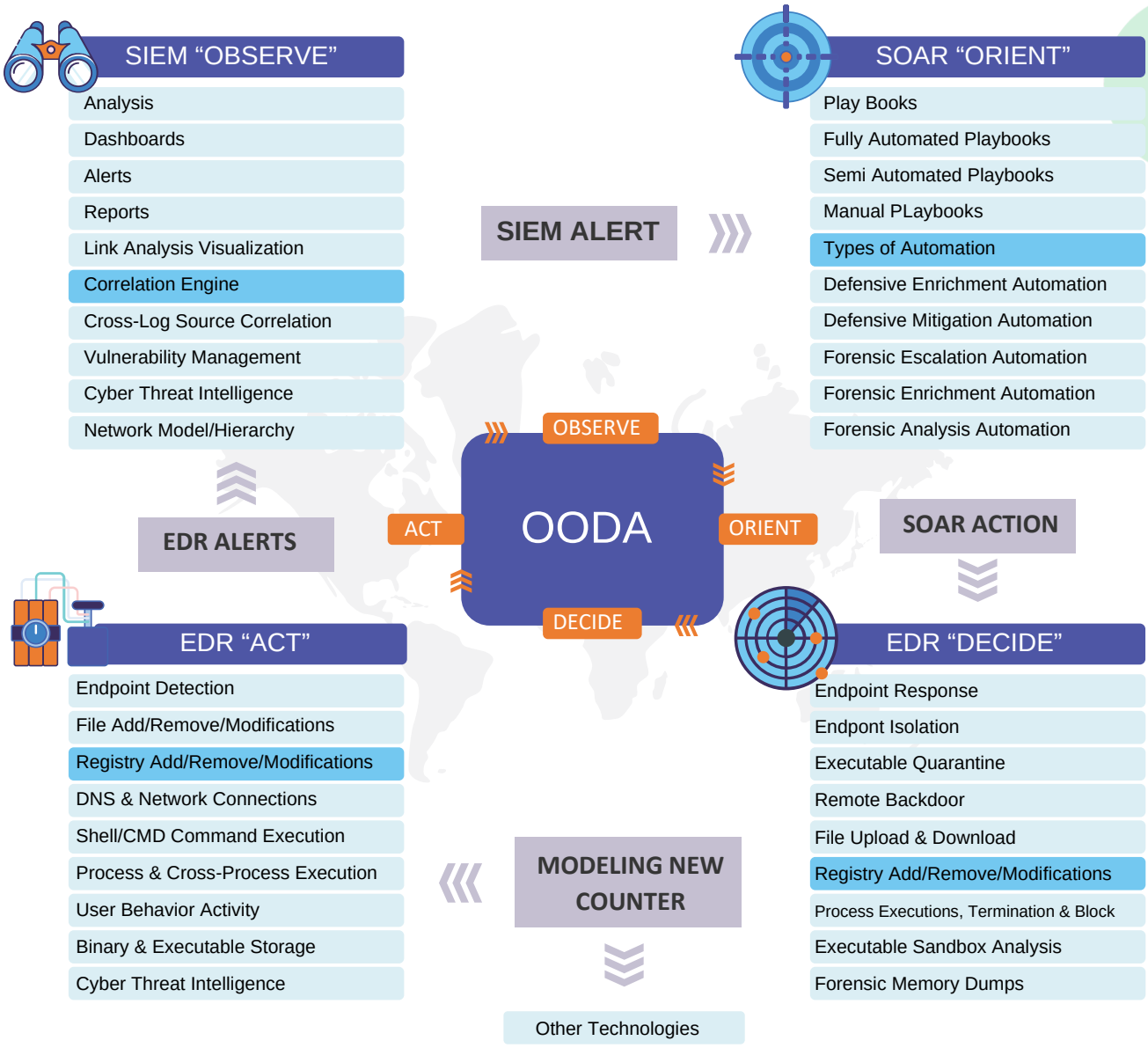


This will cover the stages of Observe, Orient, Decide, Act, and then ADAPT as a continuous process to achieve Optimization in terms of People, Process and Technology.

The Observe Process covers the part of observing and analysing the SIEM, its alerts and correlation engine’s behaviours.
Orient is the next process where depending on the SIEM alerts, the SOAR- ORIENT is done which takes feedback of Play Books, and different types of Automation deployed.
Under the DECIDE process, different security Solutions are identified and EDR.
ACT is when the real execution of the plan happens, and the decision is taken.

All this is not a one-time effort and shall need to be improvised and customised as in the ADAPT phase to achieve a continuous process of Security Optimization.

This is summarised in the next diagram.



What we need here is a strategy to integrate the need of more than 3 technologies and methodologies under one holistic approach to achieve the end objective.
The plan is to combat threats with synchronization and optimization of your security solutions to not only take actions but also make your systems adapt to be ready for any such attack in the future.

Observe - SIEM
Orient - SOAR
Decide - Security Solutions in the landscape and EDR
Act - Security Solution in the landscape and EDR

Why SIEM, SOAR and EDR?

SIEM - - Ability to Systematically Store and retrieve the logs for Compliance requirements, Cyber Crime Investigation

SOAR - - It does something similar to SIEM but at a much higher level. The primary focus of SOAR is on gathering cybersecurity information and then putting it all together in a way that cybersecurity professionals can easily manage and process

EDR - Catch malicious activities delivered by exploit through Zero-Day-Attack and not just focussed on Compliances

We know that SIEM provides us with the capabilities of logging and monitoring security incidents thereby putting in all the necessary measures to easily detect and respond to any such incidents before it creates havoc. What we often see is that due to the absence of coercive strategy or lack of integration among tools or a team that understand the various strategies involved, the process is not effectively set up and monitored. More often, the technology behind is also cumbersome and exceedingly difficult to get onboard and implement. The use cases and configurations that shall need to account the ever-changing threat landscape is also extremely hard to come by.

We have evaluated quite many technologies in the space and various strategies to arrive at an approach that is highly effective and can be a game-changer in the days to come. This phase is rather the starting point of any detection process and shall need to be fool proof. What we propose is a tool that is easily adapted to any technology environment and easy to manage.

This tool has the Analysis and Correlation capability that any SIEM tool that is currently available. The key differentiator here is the tighter integration with the other technologies we are going to implement and the achievement of the key objective of OBSERVE phase as that of going through tons and tons of data to analyse and correlate on a real-time basis to weed out as many false positives as possible to alert the team to get ready to act.

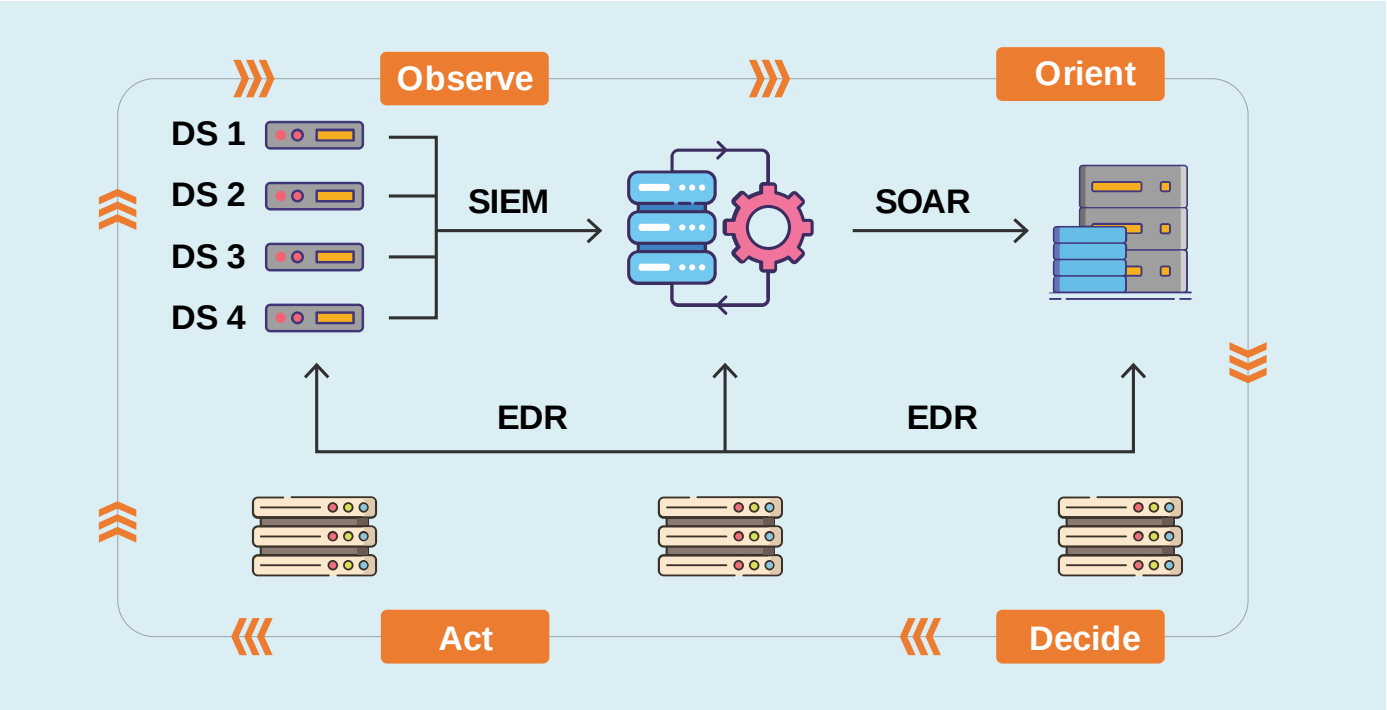
Once the SIEM Alert is generated, then it is the SOAR solution that performs the various kinds of orchestration and automation to prepare the defences against the alert. This is the ORIENT phase the necessary techniques are formulated based on the intelligence. What is required here is a SOAR solution that considers various Orchestration and automation techniques possible to define a strategy for incident response.

Security Architecture

Now, we have the incident identified and the necessary techniques / methods to respond readily. This is where we DECIDE and ACT. For this, we need the support of an Endpoint Detection and Response (EDR) tool to facilitate the action. A capable EDR solution along with the various security solutions will help in endpoint detection and response. A comprehensive Threat Intelligence aids in Detection and host of analysis along with Forensic techniques help in a highly effective Incident Response.

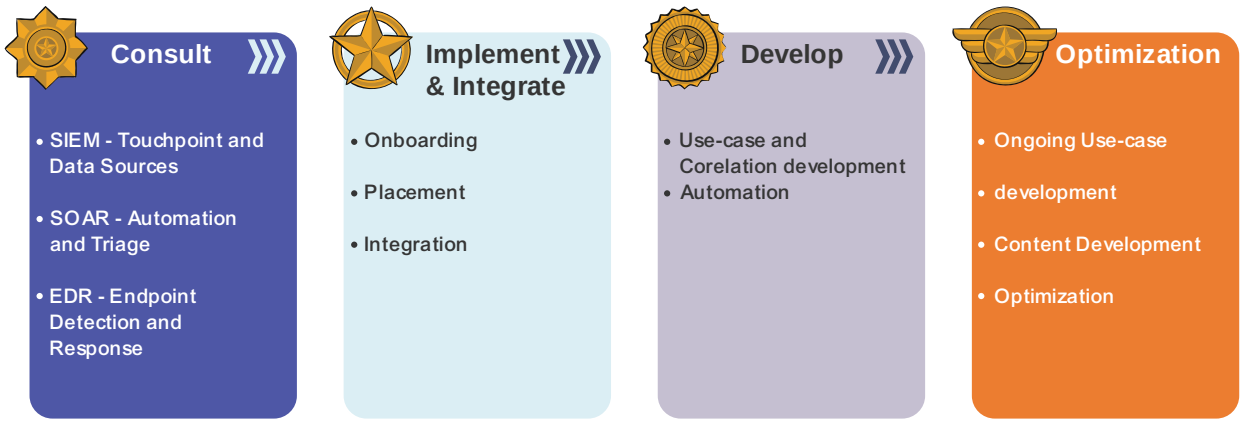
A snapshot view of the effective Endpoint Detection and Response is captured as below:

The 3 major components that constitute the Security Optimization Centre to seamlessly integrate and to deliver the OODA Strategy is shown below:



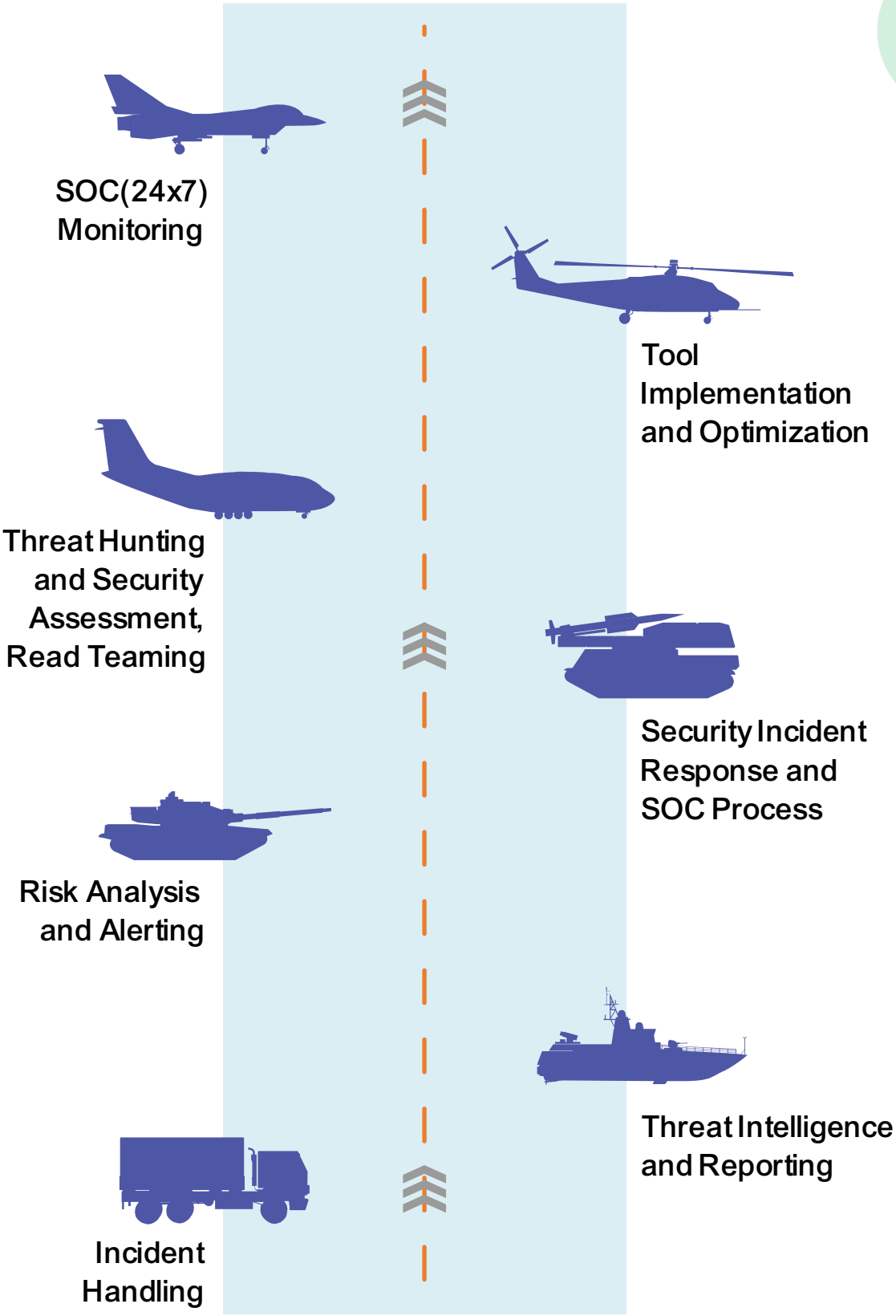
An Integrated Approach

We have seen the benefits of using multiple solutions and methodologies related to Incident Detection and Response to bring together a holistic integrated approach that delivers as promised and more in this ever-changing environment. The OODA Approach to implementation is captured in the below diagram:



The key objectives that are met in a single approach can bring in much ease to the security team in any organization. What we see as different tools with different outcomes and different teams with different objectives are all brought under one umbrella to solve a complex problem i.e. how we detect and respond to security incidents in a timely manner. This objective is not that easy to achieve as can be seen from the queries and concerns expressed by the security teams globally.

What has always been a missing link was the tighter integration of these strategies, solutions, and services all under one platform. And that is exactly what we are trying to solve here and trying to achieve. OODA Strategy and Approach is an attempt to achieve all these seemingly tougher goals in one shot. These are summarized as below:



Key Benefits of this Approach

This approach comes with a whole of key benefits that shall be music to the ears of any Security Defenders.

24x7 Monitoring

Strategic Alignment

Integration of SIEM, SOAR and EDR

Environment Agnostic

Ongoing Use Case Development

Threat Intelligence

Optimization as a Strategy

Automation of repetitive tasks

Realtime Incident Detection and Response

Way Forward

This methodology is proving to be a game changer in devising a Security Incident Detection and Response Strategy for any Organization. It is a highly evolved approach that marries the advantages of the various Incident response and detection strategies to achieve multiple security goals. This Approach believes in a coercive strategy that has its DNA in automating all the repetitive, mundane tasks and freeing up the security team to focus on delivering a detection and response strategy that is tightly integrated with real-time Threat Intelligence.

This approach is an integrated platform model that seamlessly fits into your Cyber Program and enhances the overall Cyber Security Maturity of the organization. This shall give the Management the much-needed confidence and the ammunition to fight the menace.

For more information, please reach out to us sos@infopercept.com

Contact Us

Infopercept

Phone
+91 989 885 7117

Email
E: sos@infopercept.com
W: www.infopercept.com

USA
New York

UK
London

INDIA
Ahmedabad | Bangalore
Hvderabad | Mumbai

KUWAIT
Kuwait City

SRI LANKA
Colombo