An introduction to Invinsense Platform for Strengthening your Cyber Security Posture In AWS

April 20, 2021

Infopercept Consulting
# Table of content

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting the context</td>
<td>3</td>
</tr>
<tr>
<td>Introduction to Invinsense</td>
<td>5</td>
</tr>
<tr>
<td>Invinsense Platform</td>
<td>7</td>
</tr>
<tr>
<td>Invinsense Components:</td>
<td>8</td>
</tr>
<tr>
<td>OODA Strategy</td>
<td>14</td>
</tr>
<tr>
<td>Security Architecture</td>
<td>17</td>
</tr>
<tr>
<td>ODS Strategy</td>
<td>19</td>
</tr>
<tr>
<td>Deception Technology</td>
<td>19</td>
</tr>
<tr>
<td>Solution</td>
<td>20</td>
</tr>
<tr>
<td>What is advantage of using Deception?</td>
<td>21</td>
</tr>
<tr>
<td>Moving Target Defense</td>
<td>22</td>
</tr>
<tr>
<td>Our Approach</td>
<td>23</td>
</tr>
<tr>
<td>Moving Target Defense - Common Practices:</td>
<td>24</td>
</tr>
<tr>
<td>An Integrated Approach</td>
<td>26</td>
</tr>
<tr>
<td>RBAS Strategy</td>
<td>27</td>
</tr>
<tr>
<td>Red Teaming</td>
<td>27</td>
</tr>
<tr>
<td>Our Approach</td>
<td>28</td>
</tr>
<tr>
<td>RED Teaming Exercise</td>
<td>29</td>
</tr>
<tr>
<td>Methodology of Red Team</td>
<td>30</td>
</tr>
<tr>
<td>Breach and Attack Simulation</td>
<td>31</td>
</tr>
<tr>
<td>Infopercept's Integrated Approach</td>
<td>32</td>
</tr>
<tr>
<td>G–SOS Strategy</td>
<td>33</td>
</tr>
<tr>
<td>SOS</td>
<td>34</td>
</tr>
<tr>
<td>G–SOS Components</td>
<td>34</td>
</tr>
<tr>
<td>Key Benefits of this Approach</td>
<td>42</td>
</tr>
<tr>
<td>Way Forward</td>
<td>43</td>
</tr>
</tbody>
</table>
Setting the context

This whitepaper explores a very relevant topic in today’s COVID-19 scenario where Cloud adoption is the new norm, which is how do we address the pertinent question related to Security and Compliance in the Cloud. We tend to get confused between Security of Cloud and Security in Cloud. The businesses do not want to miss out on the key advantages such as efficiency, elasticity and innovation on Cloud that makes them resilient in today’s rapidly changing times.

Current Challenges:

How are we addressing ‘Security in Cloud’ is a key challenge in itself as the parties are yet to come to terms as to who is really responsible for the same. Is it the responsibility of the Cloud Service Provider or the Company whose digital assets are on the Cloud? Further, how shall we address Security from the time one decides to migrate on to Cloud to an ongoing basis. What are the areas to be considered from Strategy to Governance to Architecture and what security controls to be integrated is a challenging task in itself?

What shall be the approach then?

What we try to address here is what are enterprise responsibilities, what are shared responsibilities, what are cloud provider responsibilities and overall how is Security tackled across.

What we need in such a scenario is a Security Reference Architecture that helps in putting together an Integrated Platform that addresses Security and Compliance on Cloud. The platform shall need to put together various strategies, services and solutions to detect and respond to any security incidents on an ongoing basis. What we introduce here is ‘Invinsense in AWS’ that addresses real-time detection and response to security incidents through a combination of an Integrated Security Operations Center (SOC), Offensive Defensive Security Tactics, Deception Strategies and 24/7 Monitoring. The platform addresses technologies such as Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), Endpoint Detection and response (EDR), Threat Intelligence, Deception, Moving Target Defense (MTD), Simulation etc. combined with a team of cloud security professionals and Project Governance. This helps in putting together a Security–First Approach for any company who is starting their Cloud Adoption journey by putting together a safety net on Cloud to detect and respond to security incidents.

Invinsense in AWS addresses People, Process and Technology through 4 focus areas as below:

- Invinsense OODA (Observe, Orient, Detect and Act) – SIEM + SOAR + EDR + Blue Team
- Invinsense ODS (Offensive Defensive Strategy) – Deception Technologies + MTD + Purple Team
- Invinsense RBAS (Red Team Breach and Attack Simulation) – Red Team + Breach & Attack Simulation
- Invinsense G-SOS (Green – Secure Optimize Strengthen) – Compliance Platform + VCISO + Pink Team
License management

We at Infopercept do take the open-source license management seriously and abide by the terms. We utilize the tools under the following licenses

- The Hive – GENERAL PUBLIC LICENSE, Version 3
- Wazuh Inc – GENERAL PUBLIC LICENSE, Version 2
- The MIT License
- Apache License, Version 2.0
Introduction to Invinsense

The attackers are getting smarter day by day and with the resources they have at their disposal, they always have the first-mover advantage. They have mastered the tactics and are objective driven combined with the might of Human intelligence and Machines. This has always proved beneficial to them in the cat and mouse game where Cyber Security Strategies always seem to play the catch-up game.

What we need is a Focus on Tactics rather than Techniques, which can always be manipulated. This focus on tactics will help in understanding the adversary mind-set deeper and paying back in the same coin. The attackers’ sense is what is core to Invinsense. The outcomes drive reduction in Mean Time to Detect a security incident and reduction in Mean time to Respond.

FIG: The most effective strategy in such a scenario is to break the Kill Chain at each phase as shown below:

Complexity and Threat Landscape of Cloud Environments:

Cloud architectures are getting complex day by day from Monolithic to Container to Serverless for microservices architectures. Combined with the limited view of the Threat landscape, it is proving to be difficult to detect and respond to security incidents on real-time basis. Once gaining foothold into Cloud environments, attackers are exploiting all possibilities through Lateral Movement to inflict as much damage as possible. Once gaining access to exposed credentials and through network reconnaissance, they are moving seamlessly across EC2 instances thereby escalating existing AWS privileges and going after the crown jewels.
Security paradox for Cloud Customers:

Customers are confused often between ‘Security of Cloud’ and ‘Security in Cloud’. Hence, to understand the Security Responsibilities in the right spirit, the concept of Shared Security Responsibility on Cloud was introduced. What it essentially addresses is what are Customer’s Security Responsibilities (‘in’ Cloud) and what are AWS’ Security Responsibilities (‘of’ Cloud).

Customer is responsible for Data, platform, applications, identity and access management, encryption and network traffic management.

At the same time, AWS is responsible for Computing capabilities, Storage, database and networking, Physical security along with managing the Cloud Infrastructure globally.

<table>
<thead>
<tr>
<th>Security Governance, Risk &amp; Compliance (GRC)</th>
<th>Private Cloud (Self-Hosted)</th>
<th>Private Cloud (Co-Located)</th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Platform Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Enterprise Responsibility

Shared Responsibility

Cloud Provider Responsibility

Integrated Security across the Landscape with Attackers Sense:

We require an integrated security approach across the platform with attacker’s sense that will detect and respond to security incidents on a real-time basis. That takes into account the complexity of the environment, threat landscape, and should be an amalgamation of security process, technology and people that addresses the need in a coercive manner. This is what is being addressed through ‘Invinsense on AWS’.

Understanding the AWS Shared Security responsibility, and understanding various use cases related to early detection to response through log management and continuous monitoring is the key.

Another major advantage of ‘Invinsense on Cloud’ is the tighter integration with ‘AWS Security Hub’. Integrating Invinsense with AWS Security Hub is a game changer in itself as Invinsense Capabilities as well as the tighter security monitoring and reporting capabilities of the AWS Security Hub comes in a seamless platform for AWS customers.

AWS Security Hub:

AWS Security Hub provides centralized event & alert management system providing a comprehensive view of security alerts and security posture across AWS accounts. With Security Hub, one gets a single view that aggregates, organizes, and prioritizes security alerts, or findings, from multiple AWS services, as well as from AWS Partner Network (APN) solutions such as Invinsense. AWS Security Hub continuously monitors the Cloud environment using automated security checks based on the AWS best practices and industry standards such as Payment Card Industry Data Security Standard (PCI DSS), Center for Internet Security (CIS) etc. AWS Security Hub helps in aggregating and prioritizing findings and conducting security checks.
Invinsense Platform

Increasingly it’s observed that there is no single integrated platform that addresses a key problem faced by an organization today; how to put in an Offensive & Defensive Strategy to combat cyber security threats? We have Offensive strategies and technologies as well as Defensive techniques available. But, what is missing is a coercive approach as well as a platform that addresses both these areas in one tightly integrated platform.

To address these concerns, we are introducing our Invinsense platform based on Open-sources technology stack that addresses the following areas in a seamless integration of strategy, services and solutions.

Key Areas integrated within the Invinsense platform:

- **SIEM** – Security Information and Event Management: - This is where Log Retention and Analysis, Correlation, alerts etc. are managed

- **SOAR** – Security Orchestration, Automation and Response: - This is the heart of the platform where the intelligence to take corrective actions, automation of run books, alert generation, trigger for incident management etc. happen

- **EDR** – Endpoint Detection and Response: - This is a vital link to the overall process where the endpoints are monitored on real-time basis to detect responses to incidents

- **Incident Management:** - We believe that what cannot be detected, cannot be prevented, Hence, the trigger to the incident management process where the incidents are detected, analyzed and responded comes from the SOAR engine. The actions in terms of response will follow the run book and will be logged and tracked with the ticketing tool and shall involve the security team.

- **Threat Intelligence:** - This is what really helps the SOAR engine to make informed decisions in case of an incident. Threat intelligence feeds from various sources are analyzed and contextualized by the Automation engine to arrive at the incident response.

- **Deception Technologies:** - These are real offensive techniques used to lure the attackers to commit mistakes and detect them as they enter the network.

- **Breach & Attack Simulation:** - The approach is to simulate various breach scenarios on an ongoing basis, thereby evaluating the control gaps within the environment and remediating those real-time.
Invinsense Components:

- **Wazuh**
  Wazuh is an open-source security monitoring solution which collects and analyzes host security data. The Wazuh server component integrates closely with Elasticsearch and Kibana while the agent is capable of many security related tasks such as log analysis, rootkit detection, listening port detection, and file integrity monitoring. For this project we’ll utilize these capabilities to generate alerts.

- **Elasticsearch**
  Elasticsearch will act as our log repository. It is incredibly powerful and versatile; and when coupled with Logstash for log ingestion and Kibana for visualization, provides a robust platform for all types of data.

- **ElastAlert**
  ElastAlert is an open-source project that provides an alerting mechanism for Elasticsearch. It simply queries Elasticsearch through the REST API and has numerous outputs to alert on a match. One of those outputs will feed the information into The Hive and another to Shuffle. This is how we distinguish the noise from the important events in the logs and generate alerts.

- **Shuffle**
  Shuffle is an Open Source SOAR engine that acts as the core of the Invinsense platform. It acts as a central hub and is the automation and orchestration engine that communicates with Wazuh, Cortex, TheHive and other tools. Shuffle plays a vital role in the overall integration.

- **The Hive**
  The Hive is an alert management platform used for managing an incident alert from creation to closure.

- **Cortex**
  Cortex is a Threat Intelligence Platform that allows the use of “analysers” to gain additional information on the indicators already present in the logs. It allows the querying of third-party services on indicators such as IP, URL, and file hash, and will tag the alert with this additional information.

- **MISP**
  MISP is an open source threat sharing platform maintained by CIRCL which, among many other uses, allows the operator to subscribe to threat intelligence feeds. These feeds can either be paid subscriptions or community maintained feeds from various organizations, and are our primary source of data enrichment.

- **Dejavu**
  DejaVu is an open source deception framework which can be used to deploy decoys across the infrastructure. This could be used by the defender to deploy multiple interactive decoys (HTTP Servers, SQL, SMB, FTP, SSH, client side – NBNS) strategically across their network on different VLANs. To ease the management of decoys, we have built a web based platform which can be used to deploy, administer and configure all the decoys effectively from a centralized console. Logging and alerting dashboard displays detailed information about the alerts generated and can be further configured on how these alerts should be handled.
• Caldera

Caldera is an open-source Breach and Attack Simulation (BAS) tool that assesses the resiliency of the customer environment to post-breach attacks and lateral movement.

‘Wazuh’ is the Log collection and Correlation engine that sends alerts to Shuffle, which acts as the SOAR engine at the core of the Invinsense. ‘Shuffle’ does the orchestration and automation in conjunction with the Threat Intelligence platforms ‘Cortex’ and ‘MISP’. Once the incident is identified and analyzed, an alert is created for further action through a ticketing tool called ‘The Hive’.

We perform Breach & Attack Simulation exercises on an ongoing basis through the ‘Caldera’ solution. ‘Déjà vu’ helps in putting a strategy for Deception Technologies and Moving Target Defense. With the might of this tighter integration of Strategy, Solutions and Services, we achieve an Offensive Defensive Strategy to combat Cyber Threats on a real-time basis.

Building Security Data Lake and Actionable Response

A data lake is a system or repository of data stored in its natural/raw format, usually object blobs or files. Our Invinsense real-time threat hunting platform helps the organisations of any size to identify and mine security based threats from the past and real time data within AWS. Not only this data lake can be used as security central but also a centralised log management system to understand the EPS (Events Per Second) and how they can optimise them operationally.

The following figure depicts the pictorial representation of our platform integration within AWS infrastructure that helps the organisation to drive business without the need of worrying about data breaches or data loss by utilising our solution.

Fig: Invinsense Integration with AWS Data Lake
The following are the components

**Amazon SageMaker**

Amazon SageMaker is a fully-managed service that enables data scientists and developers to quickly and easily build, train, and deploy machine learning models at any scale. Amazon SageMaker includes modules that can be used together or independently to build, train, and deploy your machine learning models.

Amazon SageMaker makes it easy to build ML models and get them ready for training by providing everything you need to quickly connect to your training data, and to select and optimize the best algorithm and framework for your application. Amazon SageMaker includes hosted Jupyter notebooks that make it is easy to explore and visualize your training data stored in Amazon S3. You can connect directly to data in S3, or use AWS Glue to move data from Amazon RDS, Amazon DynamoDB, and Amazon Redshift into S3 for analysis in your notebook.

**Amazon Kinesis**

Amazon Kinesis makes it easy to collect, process, and analyse real-time, streaming data so you can get timely insights and react quickly to new information. Amazon Kinesis offers key capabilities to cost-effectively process streaming data at any scale, along with the flexibility to choose the tools that best suit the requirements of your application. With Amazon Kinesis, you can ingest real-time data such as video, audio, application logs, website clickstreams, and IoT telemetry data for machine learning, analytics, and other applications. Amazon Kinesis enables you to process and analyse data as it arrives and respond instantly instead of having to wait until all your data is collected before the processing can begin.

**Apache Kafka**

Amazon MSK is a fully managed service that makes it easy for you to build and run applications that use Apache Kafka to process streaming data. Apache Kafka is an open-source platform for building real-time streaming data pipelines and applications. With Amazon MSK, you can use native Apache Kafka APIs to populate data lakes, stream changes to and from databases, and power machine learning and analytics applications.

Apache Kafka clusters are challenging to setup, scale, and manage in production. When you run Apache Kafka on your own, you need to provision servers, configure Apache Kafka manually, replace servers when they fail, orchestrate server patches and upgrades, architect the cluster for high availability, ensure data is durably stored and secured, setup monitoring and alarms, and carefully plan scaling events to support load changes. Amazon MSK makes it easy for you to build and run production applications on Apache Kafka without needing Apache Kafka infrastructure management expertise. That means you spend less time managing infrastructure and more time building applications.
Amazon Config

Amazon Config is a service that enables you to assess, audit, and evaluate the configurations of your Amazon Web Services resources. Config continuously monitors and records your Amazon Web Services resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between Amazon Web Services resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.

With Amazon Config, you are able to continuously monitor and record configuration changes of your Amazon Web Services resources. Config also enables you to inventory your Amazon Web Services resources, the configurations of your Amazon Web Services resources, as well as software configurations within EC2 instances at any point in time. Once change from a previous state is detected, an Amazon Simple Notification Service (SNS) notification can be delivered for you to review and take action.

Amazon Macie

Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS. As organizations manage growing volumes of data, identifying and protecting their sensitive data at scale can become increasingly complex, expensive, and time-consuming. Amazon Macie automates the discovery of sensitive data at scale and lowers the cost of protecting your data. Macie automatically provides an inventory of Amazon S3 buckets including a list of unencrypted buckets, publicly accessible buckets, and buckets shared with AWS accounts outside those you have defined in AWS Organizations. Then, Macie applies machine learning and pattern matching techniques to the buckets you select to identify and alert you to sensitive data, such as personally identifiable information (PII).
Amazon GuardDuty

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behaviour to protect your AWS accounts, workloads, and data stored in Amazon S3. With the cloud, the collection and aggregation of account and network activities is simplified, but it can be time consuming for security teams to continuously analyze event log data for potential threats. With GuardDuty, you now have an intelligent and cost-effective option for continuous threat detection in AWS. The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats. GuardDuty analyses tens of billions of events across multiple AWS data sources, such as AWS CloudTrail event logs, Amazon VPC Flow Logs, and DNS logs. With a few clicks in the AWS Management Console, GuardDuty can be enabled with no software or hardware to deploy or maintain. By integrating with Amazon CloudWatch Events, GuardDuty alerts are actionable, easy to aggregate across multiple accounts, and straightforward to push into existing event management and workflow systems.

AWS Logging

In AWS, logging, like most tasks, isn’t as simple as it seems it could be, due to an inconsistent use of defaults, differing destination logging services, and a variety of configuration options, sometimes hidden in layers of submenus and API parameters. I guess we can blame the pizza teams for this too.

Security Hub

The continued evolution of security threats makes it difficult, expensive, and time-consuming for security teams to react. The AWS Security Hub Automated Response and Remediation solution addresses this challenge by providing predefined response and remediation actions based on industry compliance standards and best practices. AWS Security Hub Automated Response and Remediation is an add-on solution that works with AWS Security Hub to provide a ready-to-deploy architecture and a library of automated playbooks. The solution makes it easier for AWS Security Hub customers to resolve common security findings and to improve their security posture in AWS.

Amazon Detective

Amazon Detective makes it easy to analyze, investigate, and quickly identify the root cause of potential security issues or suspicious activities. Amazon Detective automatically collects log data from your AWS resources and uses machine learning, statistical analysis, and graph theory to build a linked set of data that enables you to easily conduct faster and more efficient security investigations.

AWS CloudTrail

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. In addition, you can use CloudTrail to detect unusual activity in your AWS accounts. These capabilities help simplify operational analysis and troubleshooting.
Amazon Step Functions

AWS Step Functions is a serverless function orchestrator that makes it easy to sequence AWS Lambda functions and multiple AWS services into business-critical applications. Through its visual interface, you can create and run a series of checkpointed and event-driven workflows that maintain the application state. The output of one step acts as an input to the next. Each step in your application executes in order, as defined by your business logic.

Amazon Simple Notification Service

Amazon Simple Notification Service (Amazon SNS) is a fully managed messaging service for both application-to-application (A2A) and application-to-person (A2P) communication.

The A2A pub/sub functionality provides topics for high-throughput, push-based, many-to-many messaging between distributed systems, microservices, and event-driven serverless applications. Using Amazon SNS topics, your publisher systems can fanout messages to a large number of subscriber systems including Amazon SQS queues, AWS Lambda functions and HTTPS endpoints, for parallel processing, and Amazon Kinesis Data Firehose. The A2P functionality enables you to send messages to users at scale via SMS, mobile push, and email.

AWS Lambda

AWS Lambda is a compute service that lets you run code without provisioning or managing servers. Lambda runs your code only when needed and scales automatically, from a few requests per day to thousands per second. You pay only for the compute time that you consume—there is no charge when your code is not running. With Lambda, you can run code for virtually any type of application or backend service, all with zero administration. Lambda runs your code on a high-availability compute infrastructure and performs all of the administration of the compute resources, including server and operating system maintenance, capacity provisioning and automatic scaling, code monitoring and logging. All you need to do is supply your code in one of the languages that Lambda supports.

Amazon CloudWatch

Amazon CloudWatch is a monitoring and management service that provides data and actionable insights for AWS, hybrid, and on-premises applications and infrastructure resources. With CloudWatch, you can collect and access all your performance and operational data in form of logs and metrics from a single platform. This allows you to overcome the challenge of monitoring individual systems and applications in silos (server, network, database, etc.). CloudWatch enables you to monitor your complete stack (applications, infrastructure, and services) and leverage alarms, logs, and events data to take automated actions and reduce Mean Time to Resolution (MTTR). This frees up important resources and allows you to focus on building applications and business.
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, and ACT (OODA) as a continuous process to achieve Optimization in terms of People, Process and Technology.

- The OBSERVE Process covers the part of observing and analyzing the SIEM, its alerts and correlation engine’s behaviors.
- ORIENT is the next process where depending on the SIEM alerts, Orientation is done which takes feedback of Play Books, and different types of Automation deployed.
- Under the DECIDE process, different security Solutions are identified and Endpoint Detection and Response (EDR) strategy is decided.
- 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 customized to achieve a continuous process of Security Optimization.
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 focused 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 analyze 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 defenses 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.

Fig: OODA Use Case Example-2 (EDR)
1. SOC (24x7) Monitoring

2. Tool Implementation and Optimization

3. Threat hunting and security assessment, red teaming

4. Security Incident Response and SOC Process

5. Risk Analysis and Alerting

6. Threat Intelligence and Reporting

7. Incident Handling

Fig: Objectives achieved using Integration of SIEM, SOAR and EDR
Deception Technology

Deception Technology is a Defense practice in cybersecurity which aims to deceive attackers. This is done by the distribution of a collection of traps and decoys across your organization’s systems infrastructure, to replicate legitimate assets.

The main objective of employing deception technologies in the environment is to reduce the false positives and catch the attacker before they commit any misdeeds.

Deception technologies must be designed in a way to entice the attackers so that they consider it to be a worthy asset and inject a malware. Upon injection of the malware into the decoy, automated static and dynamic analysis of the injected malware is conducted and reports are automatically generated and sent to the Information Security team of your organization.

Deception occurs more in cyber-warfare than in any other field. The reason could be the ease of impersonation in a virtual world. People do it on the Internet very extensively, be it intentional or unintentional. And since impersonation on the internet is easy, many hackers exploit it.

Types of impersonation:

- **Phishing**
  It is a particularly dangerous kind of impersonation for social engineering that has increased recently in frequency and severity. Here, a perpetrator sends an email to a large group of potential targets, urging them to visit a website with a familiar-sounding name to resolve a bogus issue. For example, a fake email from "PayPal, Inc" may state that "Security updates require you to re-enter your username and password." The information provided by the victim is then used to commit identity theft or enable espionage.

- **Spear Phishing**
  It is like phishing except that in this case the attacker targets individuals rather than the mass, and it is usually more customized. The hacker finds out personal information about the user and makes use of it in his email to make it appear more authentic. use of it in his email to make it appear more authentic. use of it in his email to make it appear more authentic.

- **Whaling**
  Another example could be of Business Email Compromise (BEC) email fraud, also known as "CEO Fraud" or "Whaling". It has become a major financial cyber threat, affecting businesses of all sizes globally. In such attacks, the targets are usually high-profile employees such as a CEO or a CFO to steal sensitive information. Email fraud can take the form of a "con game" or scam as it provides lucrative business for cybercriminals and internet con artists. So, what can be the solution to this problem? Something that can beat attackers at their own game. The answer to this could be in deception itself.
Solution

**Turning deception into a weapon - Using Deception Technology.**

The idea behind deception technology is to prevent cybercriminals from inflicting significant damage. It is akin to using a decoy to run in a real or virtual operating system to trick the fraudsters into thinking they have breached the security systems.

The distributed deception platforms have grown well beyond basic honeypot trapping techniques and are designed for high-interaction deceptions, early detection, and analysis of attackers’ lateral movement. Apart from this, the platforms give security teams an upper hand by changing the asymmetry of an attack. It always forces the perpetrator to be on their toes and be on a constant vigil, lest their presence in the system be revealed.

**FIG: Deception Sample**

**Reduced False Positives**

**Personalized Threat Intelligence**
What is advantage of using Deception?

Your Deception is a real-time detection technique whereby attackers are tricked and lured into our fake decoys strategically placed within the environment. This puzzled arrangement for attackers, traps and keeps the attackers engage. With this cutting-edge deception technology, powered by a deep understanding of attacker behavior, the Blue Team Ninja sets irresistible traps to draw out malicious behavior earlier in the attack chain and buy the security team the time and insight needed to respond effectively.

What Type of Activities Do Deception Systems Detect?

- **Credential Theft:**
  It detects the theft of login credentials like username and password details of users from directories such as OLAP where they are stored.

- **Lateral Movement:**
  It detects the movement of a hacker across networks.

- **Hacking into directory systems:**
  It detects an attack on the file systems or directories of the end-users.

- **Man-in-the-middle:**
  This potentially occurs when communication between two parties is involved. The hacker tries to infiltrate the network and change communication between the involved parties unknown to them.

- **Access to sensitive information:**
  When the cyber-criminal tries to steal sensitive and/or confidential data.

- **Geo-fencing:**
  When the attackers attempt to hack into deception files that provide virtual geographical location when opened.
Moving Target Defense

The current game of hide-n-seek between the attackers and defenders in cybersecurity is unfair. The defenders plan the security architecture of an information security system, to prevent threats from attackers who have their own new and sometimes unpredictable ways of compromising a system. Speaking in technical terms, most of the current security systems are static in nature, hence giving the attackers the time to study a system, find its vulnerabilities, and plan an attack. They have an asymmetric advantage, which gives the security architects a hard time predicting a possible exploit.

So, what is the way out of this never-ending game? What if we make our security systems dynamic? What if we give the same asymmetric disadvantage to the attacker? Moving Target Defense systems is the solution we need. It is a whole new revolution in the field of cybersecurity. Instead of defending unchanging infrastructure by detecting, preventing, monitoring, tracking, or remediating threats, moving target Defense dynamizes the attack surface and imposes uncertainty in attack reconnaissance and planning. A dynamic, moving target attack surface imposes asymmetric disadvantages on cyber opponents. It invalidates the collected information and thereby prevents the attacker from building a weaponized attack. This may not end the game but would surely throw the ball in the attacker’s court. Some of the developing moving target techniques are system randomization, bio-inspired moving target Defense, dynamic network configurations, cloud-based moving target Defense, and dynamic compilation.

Amongst the advantages of a moving target strategy, the first prominent advantage is that it frustrates the attacker. With a continuously and dynamically changing attack surface, the difficulty of the attack goes up with time. Attackers are forced to spend resources for monitoring and assessing a changing attack surface for an indefinitely long period. Secondly, it can be a considerable advantage when an organization goes for scaling. In a static scenario, the expansion of an organization invites more attacks as there is a greater possibility of a vulnerability left exposed. While in the case of a dynamic security system, the asymmetric disadvantage imposed on an attacker increases. Hence, moving target strategies increase system entropy and efficiency over time and scale.

Such systems also increase the worth of existing controls and methods since it uses orchestration techniques. Speaking in a simplified way, if an endpoint is exploited, shift the attack surface there, or if your cryptographic key is stolen, move your data and change the key. We are shifting around our real data. There is a considerable decrease in the requirement of threat detection once moving target strategies are applied. In the static approach, we detect the threats (attacker) and work on mitigating them. Whereas in the dynamic approach, we focus on increasing the difficulty of the attack instead of finding the undetected attacker.

Moving target defense strategies are becoming pivotal in the cybersecurity domain. It has even adopted new cloud-based technologies like containers, infrastructure as a code, and orchestration. It has already started making a noticeable impact in both the private and government sectors. The thought of moving the asymmetric disadvantage from the side of the organizations to that of the attackers is a compelling motivation for development and research. It is strengthening innovation and an embrace of the existing security technologies. As organizations are moving to cloud, newer ways of handling configuration management and security come along with the dynamic environment which cloud infrastructures provide.

It is a perfect opportunity from a business perspective too. As this technology is evolving, it is becoming possible for even the smaller enterprises to leverage the benefits of moving target strategies into their security frameworks. It safeguards the data in untrusted networks and environments too. Hence security teams can convince the management to adopt this technology without breaking policies or compromising security standards. With Moving Target Defense Technology, Cybersecurity experts like us have an unfair advantage over the attackers and the tables are completely turned in favour of enterprises.
Our Approach

It has been observed that a very high percentage of security breaches are caused by file less, in-memory attacks and that up to 80% of the attacks happen at the endpoint. The existing solutions are knowledge based and are defenseless against unknown and evasive threats. There is a refreshed view of looking at things here. The objective is to prevent (tactics) the attack from happening than detect (techniques) it when it surfaces. This reduces the surface area and thereby reducing the risks massively. The idea is to introduce controlled changes, increases uncertainty, increases complexity, reduces window of opportunity thereby increasing the cost of attack. Operating Systems and Applications are the real battlegrounds, and we are presenting a solution here at the OS and applications levels where the informative intelligence collected by the attacker to launch any attack is made futile.

The solution morphs the application memory and prevents any in-memory attacks being launched. It prevents zero-days, targeted and unknown attacks with no prior knowledge in one shot. The memory that is used at various points in the attack kill chain is clearly shielded thereby preventing such attacks from materializing.

We take the Moving Target Defense paradigm to the next level by creating environmental modifications to the application and the operating system, in a manner untraceable by attackers. By forcing attackers to fight on an uncertain battlefield, Moving Target Defense completely changes the rules of conflict.
Moving Target Defense – Common Practices:

In practice, there are three main categories of Moving Target Defense security:

1. Network level MTD.
2. Host level MTD.
3. Application level MTD.
1. **Network level MTD**

Includes several mechanisms that have been developed over the years. IP-hopping changes the host’s IP address, thus increasing the network’s complexity as seen by the attacker. Later, this idea was extended to allow maintaining the hosts IP mutation in a transparent manner. Transparency is achieved by keeping the real host’s IP address and associating each host with a virtual random IP address. Some techniques aim at deceiving the attacker at the phase of network mapping and reconnaissance. These techniques can include using random port numbers, extra open or closed ports, fake listening hosts, and obfuscated port traffic. Other techniques provide the attacker with fake information about the host and OS type and version. This includes random network services responses which prevent OS identification.

2. **Host level MTD**

Includes changing the hosts and OS level resources, naming and configurations to trick the attacker.

3. **Application level MTD**

Involves changing the application environment to trick the attacker. Address Space Layout Randomization (ASLR), which was introduced by Microsoft, implements a basic level of MTD. It involves randomly arranging the memory layout of the process’s address space to make it harder for an adversary to execute its shellcode. Other techniques involve changing the application type and versioning and rotating them between different hosts. Some application level MTDs use different settings and programming languages to compile the source-code, generating different code in every compilation.

<table>
<thead>
<tr>
<th>Information System Component</th>
<th>Deception Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Route change; random addresses, names and ports</td>
</tr>
<tr>
<td>Firewall / IDS</td>
<td>Policy change</td>
</tr>
<tr>
<td>Host</td>
<td>Change host address, replace host image</td>
</tr>
<tr>
<td>OS</td>
<td>Change version and release; change host ID; Change memory addresses, structures, resource names</td>
</tr>
<tr>
<td>Application / Application Code</td>
<td>Randomize addresses of storage fragments, filter input data that cause failures, rotate application among different hosts; multilingual code generation; different code generation</td>
</tr>
</tbody>
</table>
An Integrated Approach

We have seen the benefits of using Deception Technologies to remove false positives and to detect any attacks before it materializes. And we also looked at the Moving Target Defense as a Strategy to prevent attacks. What if we combine these two to bring to the table the advantages and benefits of both and much more?

In this integrated approach what we are trying to do is to efficiently use these 2 technologies under the able guidance of a Blue Team. If the Decoys can detect an attacker, then they are engaged for a fixed short period to not alert them. Post which, they are blocked out whereby they might sense that a cyber defense solution is doing the same. The alert that goes the Blue Team makes them prepare themselves to use the MTD solution to wisely open another service or ip to lure them back to the environment. Again, the same techniques as mentioned earlier follows. This goes on till the time attacker feels frustrated and leave it altogether. What we achieve here are 2 things. One, we can detect any attack before it manifests. Second, is the preventing the further damage by using preventive measures. Further, by the time the loop is closed we would have gotten as much information about the attacker as well as the techniques employed that it can be used to further tighten the counter measures. There is quiet some use cases that we can use that have diffused so many such attacks from materializing. This is a great approach to secure the organization assets in a cloud environment whereby we can lure the attackers and beat them in their own turf.

i.e. Deception and Unpredictability:
Red Team Exercise

The main objective of a Red Team Exercise is to perform a goal-oriented assessment of organizational defences on real-time basis from the perspective of a real attacker.

The scope includes all the available attack surface from the agreed vantage point (internal or external) and will cover the network and application layers as well as physical security and staff security awareness. The assessment will use legal, non-destructive attack vectors to gain access to and compromise customer networks.

With no pre-determined guidelines or instructions, cyber security experts will look for vulnerabilities and exploits in the following areas:

- **Technology:**
  Digital infrastructure, corporate and mobile applications, routers, switches, and a variety of endpoints.

- **People:**
  Employees, independent contractors, high-risk departments, and business partners.

- **Physical:**
  Office, warehouse, substations, data centres, and associated buildings. A comprehensive report detailing vulnerabilities listed by criticality and severity is produced after the assessment, and certified cyber security experts present steps to improve the security posture of the company. Red Team is designed to benchmark an organization’s security controls and processes, particularly around physical security (for example, access to buildings and computers/data held within it), general security awareness of staff, network security, procedures, and monitoring.

- **Red Team operator traits:**
  An effective Red Team is comprised of a team of individuals who can contribute to the overall success. Diversity is crucial, but the team must comprise of the core operator traits. A Team can be even more successful when multiple Team members contribute in multiple areas.
Our Approach:

**FIG**: Our Approach to Red Teaming exercise can be summarized as below:

- **Get In**
  - Reconnaissance
  - Enumeration
  - Exploitation

- **Stay In**
  - Persistence
  - Lateral Movement
  - Continuous Enumeration

- **Action**
  - Action on Objective
  - Operational Impact is assessed here

---

Our Approach:

Our Approach to Red Teaming exercise can be summarized as below:

![Red Teaming Diagram]

- **Recon**
- **Exploitation**
- **Command & Control**
- **Privilege Escalation**
- **Information Gathering**
- **Lateral Movement**
- **Operation Impact**
- **Establish Persistence**
- **Post Exploitation**

---

"Infoparcept Proprietary Material – Please do not copy or distribute"
Red Teaming Exercise

Our Approach to Red Team exercise goes beyond Penetration Testing and Vulnerability Assessments. The focus is on Tactics, Techniques and Procedures (TTP). Red Teaming exercises relies heavily on well-defined TTPs that are critical to the successful simulation of realistic threat and adversary techniques. Red Teaming results are much more than just a list of flaws identified during the tests. It provides a deeper understanding on how an organization would perform against an actual threat and determine what a security operation team’s strengths and weaknesses are.

Red Team is designed to benchmark an organizations’ security controls and processes, particularly around physical security (for example access to buildings and computers or data held within it), general security awareness of staff, network security, procedures, and monitoring.

The end game of a Red Team attack is to provide an organization with a complete ‘warts and all’ look at its security posture. Usually, Red Teaming takes place during the assessment stage of a business’ security process – particularly if it is looking to invest in or upgrade its information security, or if it is carrying out a regular risk audit.

It is particularly valuable to businesses for two key reasons:

- There is no procedure or automated tool in the market that can test an organization’s security as intelligently as the human mind.
- Red Teaming tests an organizations’ security posture from many angles allowing them to pinpoint any holes or gaps more accurately in security and ensure that the right policies, procedures and technology are put in place.

Red Team is an all-out attempt to gain access to a system by any means as in a real-life cyber-attack. The entire environment is within scope and their goal is to penetrate, maintain persistence, pivot, exfil, to examine what a determined enemy can do. All tactics are available including social engineering. Eventually the red team will get to a point where they own the entire network, or their actions will be caught, and they will be stopped by the security administrators of the network they are attacking. At that time, they will report their findings to management to assist in increasing the security of the network. They keep copious notes as this information is valuable later to fix the weaknesses they exploited. Not many organizations do this, but they usually have an organic red team, so the information gleaned from the red team is extremely sensitive. Red team actions are controlled by the manager of the red team.

Traditional Penetration testing uses similar tactics as that of a red team (may be limited by management and the scope of the test). However, it is executed in a controlled fashion usually dictated by management and/or asset owners. Typically, the limiting scope of a Penetration Testing is time (execution time of the event) in which a report will be made to the management. Often in a Penetration Testing exercise, before a flaw is exploited, management and system/network engineers must OK the attack to ensure it doesn’t affect day to day operations. The goal is to find weaknesses in the systems/networks to increase/improve the security posture. The Penetration Tester’s actions are controlled by business management and/or the asset owners.

However, Red Team exercises are simulations of real-life cyber-attacks and the team goes beyond traditional means to perform a concentrated attack with all the defences in place to exploit the vulnerabilities.

Our Approach is to bring out various security loopholes and control weaknesses, how to address the same and train the internal team to be prepared for such scenarios thereby improving the overall cyber security posture of the organization.
Methodology of Red Team

External Reconnaissance → Compromised Machine → Internal Reconnaissance → Local Privilege Escalation (Ext.)

Compromised Credentials → Administrator Reconnaissance → Remote Code Execution → Domain Administrator Credentials

Domain Dominance Remote Code Execution → Asset Reconnaissance → Local Privilege Escalation (Int.)

Asset Access → Exfiltration
Breach and Attack Simulation

Breach and Attack Simulation has gained utmost importance in the recent times due to the immense value it brings to any organization in its preparedness to combat any kind of cyber threats.

**FIG:** It employs a remarkably simple approach as can be seen below:

- **Launch:** *Simulate a Breach:*
  - Run the tool from any machine on any platform of your choosing, whether it’s a public cloud instance or on-premises server. Try different attack scenarios such as stolen credentials, infected internal server, or an external attacker.

- **Attack:** *Go ahead and evaluate the controls present and then identify the gaps:*
  - The automated tests would run in the background
  - Working from the given attack configuration, the tool scans for potential victims in your network, attacks them and propagates further into the network. You can keep track of progress as you watch the tool generate a map of your network from the attackers’ point of view.

- **Assess:** *Remediate the gaps with the insights available:*
  - Remediation based on the tool’s findings and recommendations.
  - The tool generates a comprehensive report detailing the simulated attack flow, highlighting immediate threats and potential security issues. By providing specific and actionable recommendations, per machine, you can use the report to harden your network.
Infopercept’s Integrated Approach

As highlighted earlier, the best possible solution to prepare your organization against the current scenario is to integrate the best of Red Team exercise and Breach and Attack Simulation. Here is how it is done to maximize the value to any organization looking to have an ongoing program to strengthen the defences against cyberattacks.
The main objective of a G-SOS strategy is to establish an integrated platform to effectively establish a Governance, Risk and Compliance Framework that addresses Cyber Risks at Organization level and help the Board / Top Management make decisions on an Ongoing Basis.

This product is a strategic tool focusing on governance, strategy, risk and compliance. This board room tool provides a deep insight on the organizational structure, the vision, the mission, the existing context, the future road map, the plans supporting the strategies, the control system designed and implemented, the metrics, the dashboard, the pivotal risk management component, the communication strategy, the awareness building mechanisms, the control mapping to various international best practice standards and guidelines etc.

This is an integrated platform designed to integrate all the Compliance related best practices into everyday business processes which is indeed the need of the hour.

This platform helps to manage your entire IT landscape, infrastructure, control systems, people and creates a stronger security, risk management, assurance and compliances across the organization. This helps to streamline the operation, effective implementation of various best practice control system, governance and monitoring through a dashboard which provides the overall health of your system. It’s very correctly said “What gets monitored and measured, gets improved”.

Organizations can define their own customized control system environment, type of activity, all kinds of laws and compliance requirements based on standards, guidelines, contractual requirements which needs to be implemented internally and enforced across the organization without much pain and efforts.

This tool helps to identify and mitigate all types of risk including service delivery risk/ quality risks, security risks, privacy risks, continuity risks, technology risks, logical risks, people risk, physical and environmental risks and helps monitor company-wide strategies for risk management.
We are using Secure; Optimize and Strengthen as a Strategy that cuts across People, Process and Technology paradigm.

SOS:
- **SECURE** system components design system components
- **OPERATE AND OPTIMIZE** system components effectively
- Monitor and measure Improve and **STRENGTHEN**

As can be seen, there is a maturity curve that any organization has to pass through to achieve the desired level of maturity when it comes to its overall Cyber Security Posture. The G-SOS Strategy is also greatly tied to the Cyber Security maturity enhancement program that any organization undertake.

The initial phase is to identify and secure the system components that comprise the overall cyber security program. Once that is inventoried, the next logical step is to Design the control environment per the leading compliance practices, frameworks and standards. Post that the Operating Effectiveness of the Controls are tested and Optimized to arrive at the desired maturity level that gives confidence to the Key Stakeholders. This shall need to be Monitored and Measured for the period in consideration. The last and most pivotal step is to Improve and Strengthen the Overall Cyber Security Governance, Risk and Compliance Program to be robust and world-class in alignment with the Strategic Direction of the company.

**G-SOS Components**

**FIG: It constitutes the following modules:**

- Organisational Vision and Mission
- Enterprise Risk Management module
- Policy and Procedure Management
- Security Culture Awareness Programs
- Board Room – War Game
- KPI Dashboards and Actionable
- SOS - Program Management
1. **Organizational Vision and Mission:**

   This is the initial and the most crucial phase where the organization define the goals for the Organization Wide Cyber Security Posture enhancement program. It starts with the Vision and Mission of the organization and require the contribution of all the key stakeholders to arrive at SMART Goals that is in alignment with the Business Strategy of the Organization.

   ![Vision, Mission, Values, Apex Policy, Goals]

   **GOALS**

   For effective governance; establishing the goals is very essential at various levels. Establishing SMART goals/objectives and tracking them is essential for effective governance. Plans shall be established to achieve the goals in a defined period.

   Smart Goals lead to a Measurement System that eventually result in an Objective Management Program.

   ![Goals, Objective Management Program, Measurement System]
2. **Enterprise Risk Management Module:**

Enterprise risk management activities are designed to ensure that management identifies, analyzes, and responds appropriately to risks that may adversely affect realization of an organization's business objectives. Management's response to risks will depend on the likelihood of the event happening and the impact if it does. Based on this risk assessment, an organization will need to choose whether to accept the risk, mitigate the risk, or transfer the risk to another party. When performed effectively, these risk management activities will ensure that the organization's limited resources will be prioritized to most efficiently address the issues that will affect them the most.

Regardless of which framework your risk management program is based on, the very first step will be some form of assessing and documenting your risks. The repository of all of your active risks is what we refer to as a "risk registry". The Enterprise Risk Management Module will immediately enable you to scale beyond your existing capabilities. You'll be able to track all of the fields that you are currently tracking with a ton of flexibility to expand beyond that, with no restrictions on the number of users you can have or the number of risks you can enter. Once your risks are in the registry, you'll have access to a variety of pre-defined reporting along with a Dynamic Risk Report that gives you the ability to report on virtually any aspect of your risk management program.

3. **Policy and Procedure Management:**

In today's dynamic changing world, each of the organizations face an uphill task to manage the compliance requirements that are often managed in a very ad-hoc manner. Also, implementing and then managing various Systems and programs across the organization is quite a challenge. In that scenario, what we need is a Centralized Controls Assurance & Monitoring Program that addresses key features such as below:

Centralized management of control requirements for the compliances in consideration

Structured controls repository

Change Management for Dynamically changing compliance requirements

Common repositories for Documentation requirements

Facilitation per Audit requirements and guidelines

A common approach to managing documentation, risks and controls w.r.t Compliance requirements is the way to go as it would then act as the Single source of truth for anything to do with overall Controls Assurance and Monitoring Program across the organization.
4. **Security Culture Awareness programs:**

Most of the control failure we observe today within an organization is caused due to lack of security awareness and absence of education within the system. For effective governance, the organization needs to improve staff security awareness across the organization using various means.

These can be broadly categorized as below:

- **01** Security Awareness
- **02** Poster
- **03** Quiz
- **04** Phishing / Brute Attack
- **05** Awareness Mail Campaign

An Effective Security Culture Awareness Program shall need to be achieved with focus on areas such as Competency Management, Resource Management, Knowledge Management etc. as can be seen below:
5. Board Room – War Games:

How much ever Cyber Security Defenses one has put in, an organization typically falters at the
time of a crisis or an incident due to primarily the lack of information and the inability of the
leaders to make the right decisions. Hence, security awareness of the Board as well as the Top
Management is of prime importance as these are the key stakeholders who actually get into the
War Room and provide that leadership during a crisis.

War Gaming is a scenario-based warfare model in which the outcome and sequence of events
affect the decision made by the players.

What we have built is a War Game for the Board / Top Management with real life scenarios of
Cyber Security Incidents with outcomes that are impacted by the decisions of the players
involved. That way, the parties get a reality check when it comes to key decision making.

This helps the team who are accountable within the system to anticipate and rehearse the
steps even before it really hits them. It’s a hands-on training on leadership during crisis and
prepare an organization to build a robust incident management program.

The game is kept very simple and with the amalgamation of Virtual Reality into the Gamification
process, a player can really experience the adrenaline rush when playing as if in real-time.

6. KPI Dashboards and Actionable

Key Performance Indicators (KPIs) are the best way to measure the maturity of any Cyber
Security program and helps in decision-making process.

Understanding the KPIs to track and then measuring it on an ongoing basis helps in achieving 2
major objectives – (1) Understanding the preparedness and the maturity of the organization
and (2) communication with the key stakeholders.

Some of the KPIs that are tracked as part of the G-SOS Dashboard are below:

- Incident Management KPI
- Vulnerability Management KPI
- Configuration Review KPI
- Malware Protection KPI
- Cyber Initiatives
- Initiatives Taken
Cyber Security Governance KPI

- Yes
  - Full time senior manager for
    Cyber Security function

- Yes
  - Cyber Security Committee independently headed by
    CRO

- Yes
  - Formation of Cyber security Committee

- Yes
  - CEO as Saudi National & SAMA approved

CEO
Cyber Security function reporting to

- Yes
  - Establishment of Cyber Security Committee

- Yes
  - Cyber Security Committee Charter

- Yes
  - Number of Cyber Security committee meeting per year
    04

- Yes
  - Cyber Function is independent from Information Technology

Mr. Def
Saud National As CEO

Level
04

3.1.1. SAMA Cyber Security
Maturity @ ABC

Fig: Cyber Security Governance KPI

Cyber Awareness

- 2
  - Phishing simulations performed

- 05
  - Cyber security Tip and guidance awareness mails performed

- 456
  - Phishing simulation performed on total number of employees

- 10
  - Cyber Misconceptions Awareness Posters

- 24.56%
  - Primary phishing simulated email opened by employees

- 88.02%
  - Employees passing phishing simulation

- 85%
  - Information security induction / awareness conducted on time

- 90%
  - % of Employees received annual information security awareness refresher training

- 12%
  - Information security induction / awareness not attended after 30 days of joining

Training Feedback
1. Well organized content and easy to follow: ~ 88%
2. Training Relevancy ~ 95%
3. Usefulness in daily work ~ 95%
4. Acknowledgement for adherence ~ 100%

Training Plan for Next Quarter:
1. Annual Policy Refresher
2. Email Security Over & Over
3. Threats in WFH scenario
4. Reporting Phishing
5. Reporting security incidents

Areas of Training & Awareness Performed:
1. Threats in WFH scenario
2. Reporting Phishing
3. Reporting security incidents

Fig: Cyber Awareness
Fig: Information Security Incident Management

Information Security Incident Management

Incident Criticality

- High
- Medium
- Low
- Normal
- Not assigned

Incident Criticality

Number 33
Security Incidents Raised in Manage Engine

Number 07
Unreported Incidents

Number 02
Web Defacements

Number 01
Publicly reported Breaches

Week 1 | Week 2 | Week 3 | Week 4 | Week 5
01 | 05 | 13 | 04 | 02
7. SOS Program Dashboards and Reporting:

1. Goal
2. Measurement system
3. Objective Management Program
4. Complaints
5. Satisfy Rating

SOS Program Dashboards include KPIs and Metrics for cyber risks, compliance risks, third-party risks, compliance measurement, vulnerability management, dark web monitoring, data leakage, incident management etc.

It is one comprehensive platform that provides the management with real-time insights that equips them to make the right decisions.

AI / ML Capabilities embedded within the platform help in faster aggregation and correlation of data thereby providing real-time data visualization dashboards for faster action.
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 on Cloud.

- Cloud-First Approach
- 24*7 Monitoring
- Alignment with ‘Shared Security Responsibility’
- Integration of SIEM, SOAR, EDR, Threat Intel., Red team and Deception Strategies
- Environment Agnostic
- Ongoing Use-Case Development
- Optimization as a Strategy
- Integration with AWS Security Hub
- 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 on Cloud. It is a highly evolved approach that marries the advantages of the various Incident detection and response 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.

About INFOPERCEPT

Infopercept’s vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners’ cybersecurity and accreditation needs.

Our specialized core team comprises experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, latest trends, and security innovations; ensuring that you always get the best security approach & solution for your specific business needs exactly the way you want it to be.

Imprint
© Infopercept Consulting Pvt. Ltd. 2021

Publisher
H-1209, Titanium City Center,
Satellite Road,
Ahmedabad – 380 015,
Gujarat, India.

Contact Info
M: +91 9898857117
W: www.infopercept.com
E : sos@infopercept.com

By accessing/ proceeding further with usage of this platform / tool / site / application, you agree with the Infopercept Consulting Pvt. Ltd’s (ICPL) privacy policy and standard terms and conditions along with providing your consent to/for the same. For detailed understanding and review of privacy policy and standard terms and conditions. kindly visit www.infopercept.com or refer our privacy policy and standard terms and conditions.