ONESEC

ALWAYS SECURE, *NEVER AT RISK*

Onesec 7x24 Managed Security Operation Services

For Microsoft Sentinel + Microsoft Defender

Onesec 7x24 Managed Security Operation Services for Microsoft Sentinel + Microsoft Defender

Onesec® Managed Security Operation Services takes care of your organization using the full artificial intelligence and machine learning power of Microsoft Sentinel to detect potential threats that can cause a significant loss. With the full coverage of diverse Microsoft Sentinel integration with Microsoft Defender Suite we can provide full visibility and wide protection across your hole IT infrastructure, from endpoint, to email, user account, to cloud apps.

In addition, the Microsoft Sentinel implementation provides full integration with several cybersecurity makers in order to keep a centralized point of log keep and collection, monitoring and orchestration automation to reduce the attack surface and to simplify breach prevention. Onesec services sets your complete Microsoft Sentinel integration by analyzing and assessing your company in order to discover vulnerabilities and breaches that can harm the organization, the solution delivers a Microsoft Sentinel optimization plan so our MDR team can efficiently detect, contain and eradicate potential threats.

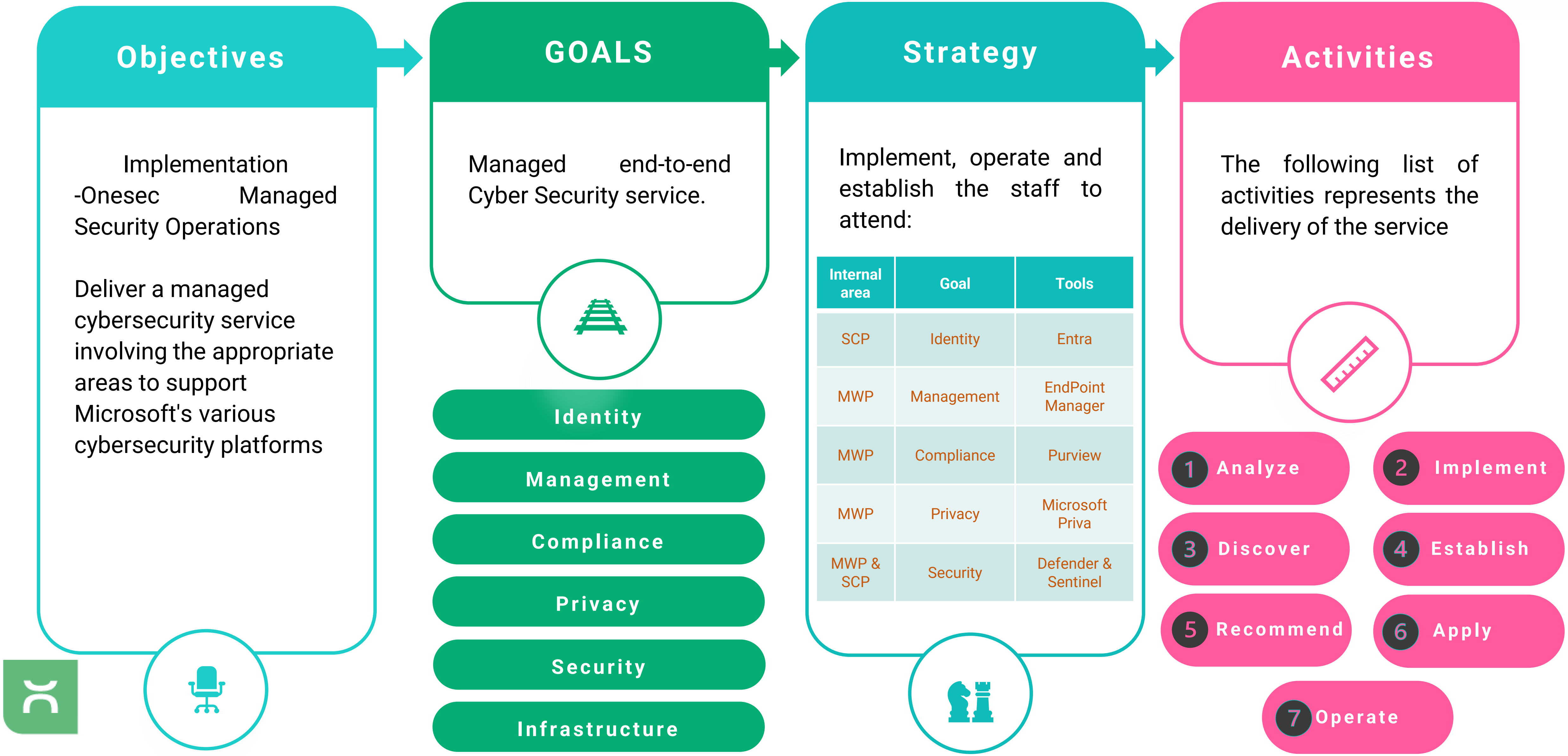
We deliver a 24x7x365 service using market highest Cybersecurity Standards such as ISO/IEC 27035, NIST Cybersecurity Framework and CIS Security Controls in a 3 level Tier operation which integrates highly trained personal with expertise in Microsoft Security having MS-500: Microsoft 365 Security Administration, SC-900, SC-200 and AZ-500: Microsoft Azure Security Technologies certifications.

XNESEC

Service Features

- Microsoft Sentinel assessment and optimization.
- Microsoft Defender assessment and optimization.
- Alert triaging and investigation
- Remote incident response
- Threat Hunting
- Threat Eradication
- Threat Intelligence
- Log source collection, optimization
- Escalations and notifications as appropriate
- Microsoft Sentinel integration for Imperva, Checkpoint, Tenable, Infoblox, Darktrace, F5, Netskope

ONESEC



Objectives

Implementation -Onesec Managed Security Operations

Deliver a managed cybersecurity service involving the appropriate areas to support Microsoft's various cybersecurity platforms

GOALS

Managed end-to-end Cyber Security service.

- Identity
- Management
- Compliance
- Privacy
- Security
- Infrastructure

Strategy

Implement, operate and establish the staff to attend:

Internal area	Goal	Tools
SCP	Identity	Entra
MWP	Management	EndPoint Manager
MWP	Compliance	Purview
MWP	Privacy	Microsoft Priva
MWP & SCP	Security	Defender & Sentinel

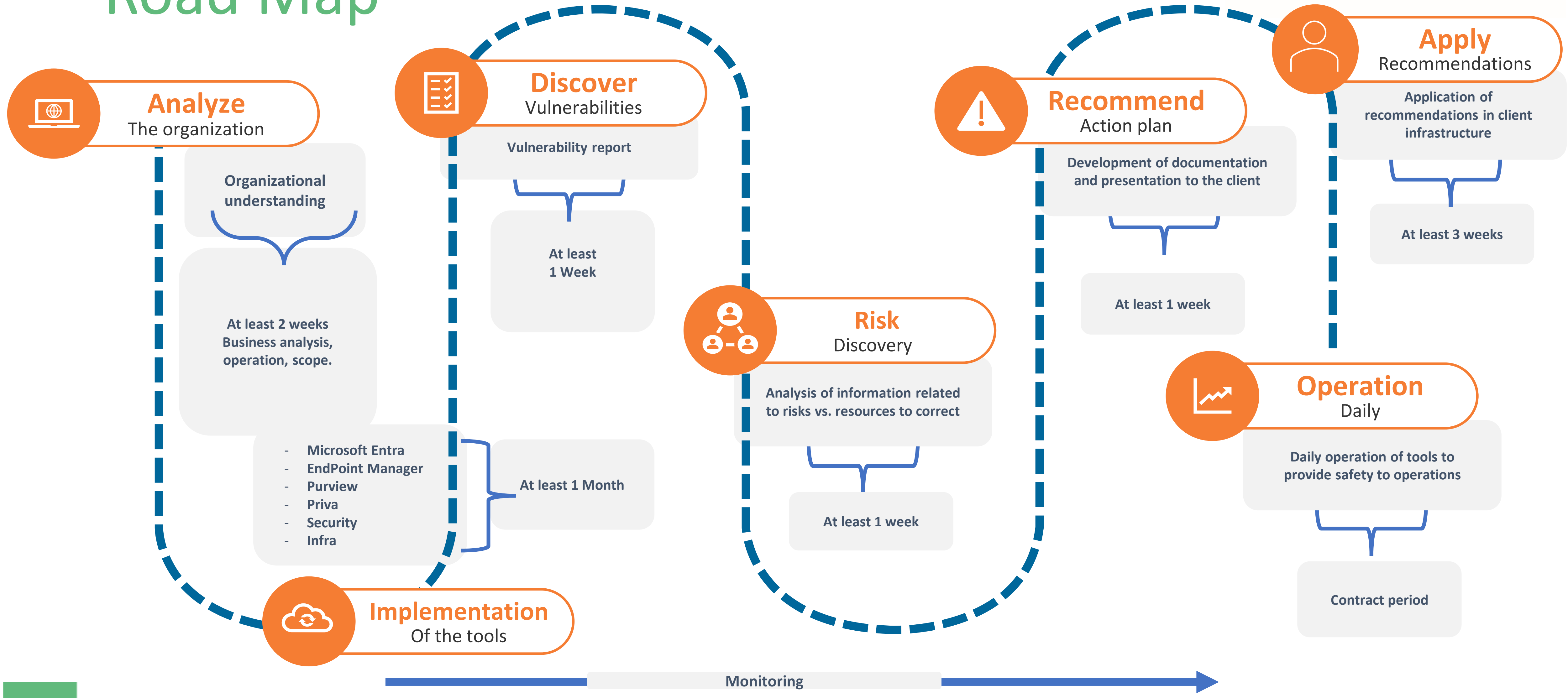
Activities

The following list of activities represents the delivery of the service

1 Analyze
2 Implement
3 Discover
4 Establish
5 Recommend
6 Apply
7 Operate

Road Map

NESEC



Analyze
The organization

Organizational understanding

At least 2 weeks
Business analysis, operation, scope.

Discover
Vulnerabilities

Vulnerability report

At least
1 Week

Implementation
Of the tools

- Microsoft Entra
- EndPoint Manager
- Purview
- Priva
- Security
- Infra

At least 1 Month

Risk
Discovery

Analysis of information related to risks vs. resources to correct

At least 1 week

Recommend
Action plan

Development of documentation and presentation to the client

At least 1 week

Apply
Recommendations

Application of recommendations in client infrastructure

At least 3 weeks

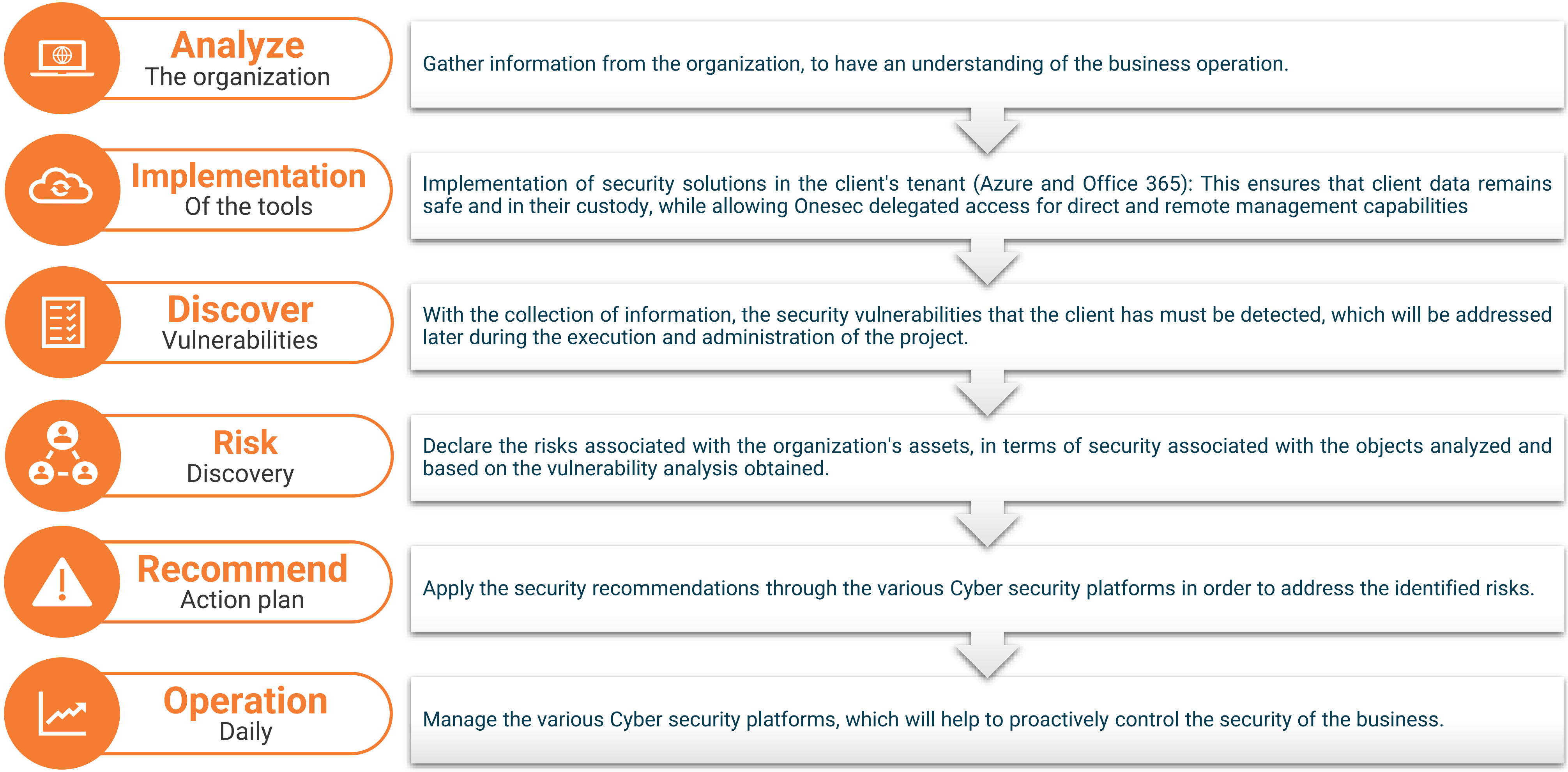
Operation
Daily

Daily operation of tools to provide safety to operations

Contract period

Monitoring

Descripción del Road Map



Analyze
The organization

Gather information from the organization, to have an understanding of the business operation.

Implementation
Of the tools

Implementation of security solutions in the client's tenant (Azure and Office 365): This ensures that client data remains safe and in their custody, while allowing Onesec delegated access for direct and remote management capabilities

Discover
Vulnerabilities

With the collection of information, the security vulnerabilities that the client has must be detected, which will be addressed later during the execution and administration of the project.

Risk
Discovery

Declare the risks associated with the organization's assets, in terms of security associated with the objects analyzed and based on the vulnerability analysis obtained.

Recommend
Action plan

Apply the security recommendations through the various Cyber security platforms in order to address the identified risks.

Operation
Daily

Manage the various Cyber security platforms, which will help to proactively control the security of the business.

Detection and Response Management Service – MDR

Monitoring

Through Sentinel Artificial Intelligence, constant monitoring in a 7x24x365 scheme, operated by first level analysts (Tier

Detection

Alert detection based on classification in BlueTeam playbooks that analysts investigate to confirm or exclude potential incidents.

Classification

Faced with a potential incident, analysts classify the event prioritizing it according to its level of potential impact.

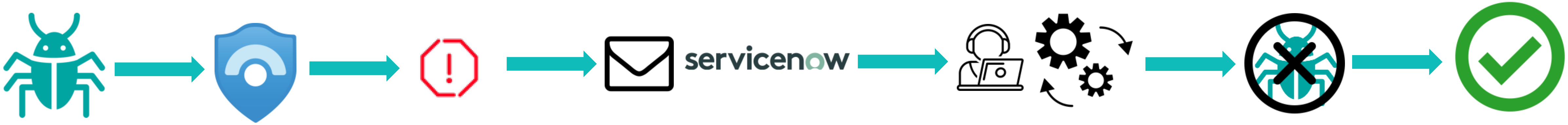
Containment

Analysts perform different containment activities to prevent the attack from spreading, isolating computers, activating cleaning routines, rules on network computers, IPS/IDS, etc.

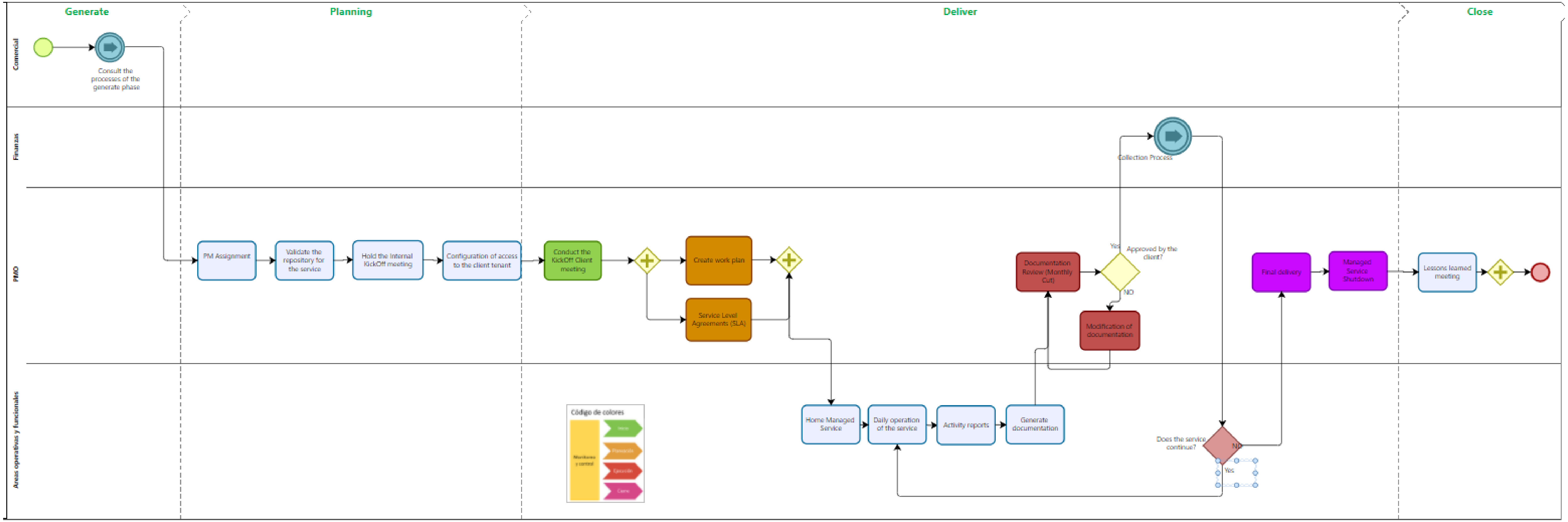
Resolution

Analysts take action to resolve the event, or escalate to specialized analysts at the next levels (Tier 2 and Tier 3).

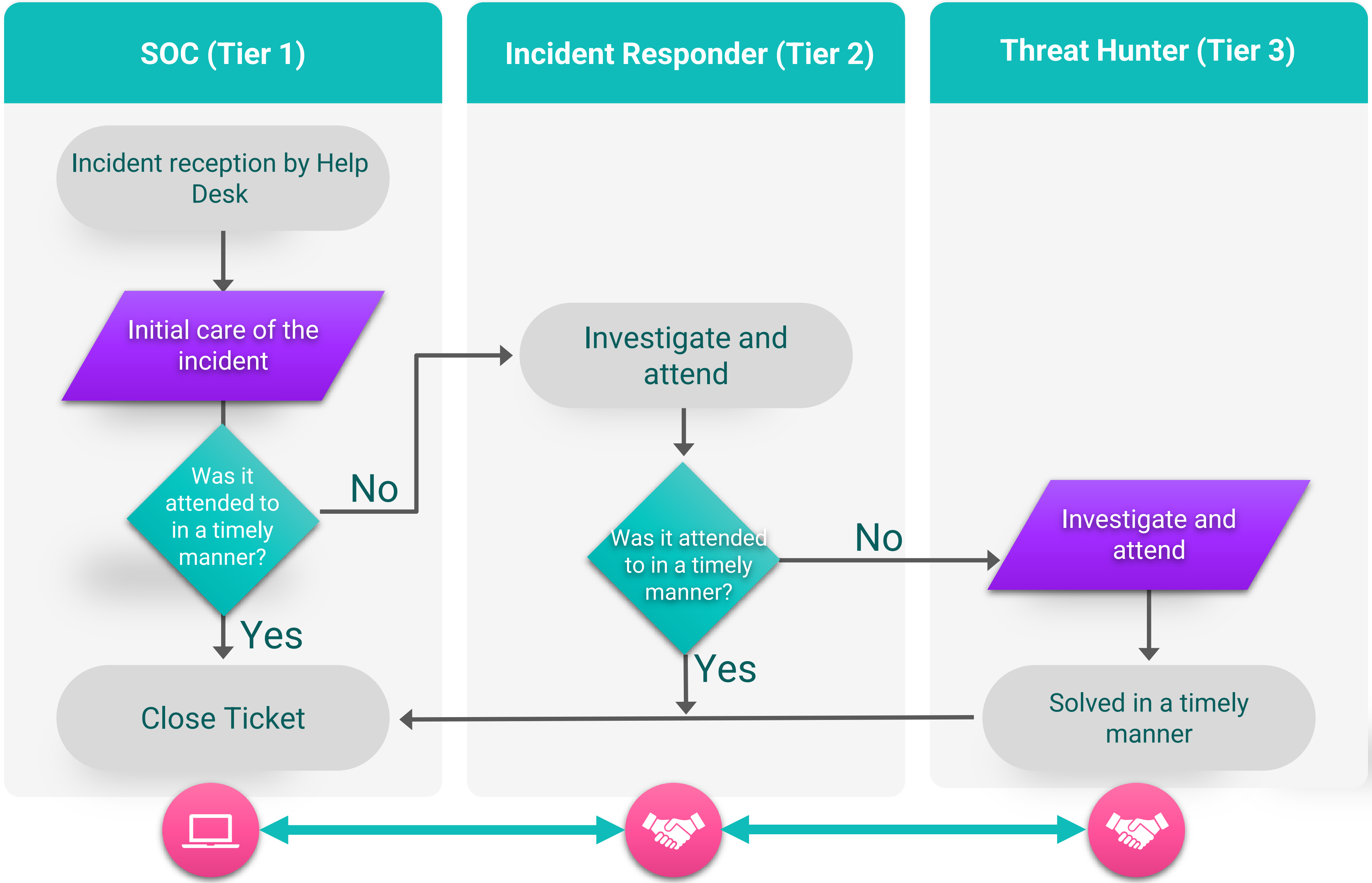
Threat Hunters T3



Daily operation through Service Desk


Generate
Planning
Deliver
Close
Comercial
Finanzas
PMO
Áreas operativas y funcionales
Consult the processes of the generate phase
PM Assignment
Validate the repository for the service
Hold the Internal KickOff meeting
Configuration of access to the client tenant
Conduct the KickOff Client meeting
Create work plan
Service Level Agreements (SLA)
Home Managed Service
Daily operation of the service
Activity reports
Generate documentation
Documentation Review (Monthly Cut)
Yes
Approved by the client?
NO
Modification of documentation
Collection Process
Does the service continue?
NO
Yes
Final delivery
Managed Service Shutdown
Lessons learned meeting
Código de colores
Inicio
Planeación
Ejecución
Cierre
Monitoreo y control

Managed Service Flow and SLA's



SOC (Tier 1)

Incident Responder (Tier 2)

Threat Hunter (Tier 3)

Incident reception by Help Desk

Initial care of the incident

Was it attended to in a timely manner?

No

Yes

Close Ticket

Investigate and attend

Was it attended to in a timely manner?

No

Yes

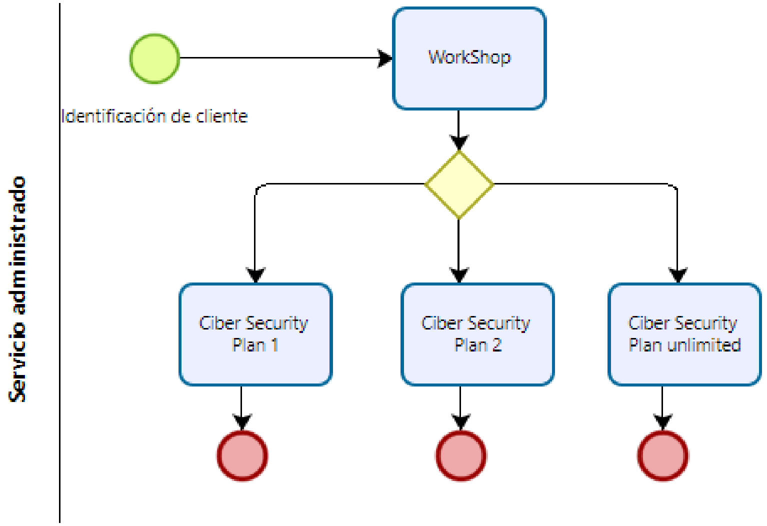
Investigate and attend

Solved in a timely manner

SLAs

P1 – Critical:	4 horas
P2 - High:	6 horas
P3 - Medium:	16 horas
P4 - Low:	24 horas

SM-SOC life cycle



- Onesec MDR services leverage Microsoft Sentinel to protect your organization against advanced threats.
- Onesec specialized services monitor your most important assets in 7x24 schemes to, in conjunction with the Microsoft Sentinel security analytics platform, the use of Machine Learning capabilities and the use of Playbooks, detect and respond to advanced threats, both internal and external. external.
- The security analytics capabilities obtain events and signals from the most important elements of your organization's infrastructure, for their correlation with external intelligence sources on the most current threats, allowing the detection of malicious behaviors, and consequent activation of the protocols. response through a team of analysts, response specialists and threat hunters, which allow threats to be eliminated from their earliest stages.
- Proactive response approaches enable the organization to significantly minimize risk to its core operations by protecting underlying infrastructure elements and applications. Providing benefits to the organization in terms of reducing economic, operational, regulatory and reputational impacts.

NESEC

Gracias

ONESEC

Onesec.mx

+52 (55) 85254111

San Jacinto No. 8
Col. San Ángel, C.P. 01000
Alcaldía Álvaro Obregón, CDMX