ONESEC

ALWAYS SECURE, *NEVER AT RISK*

ONESHIELD

Our Solution

ONESEC

Francisco Ovalle
COO

✉ fovallef@onesec.mx

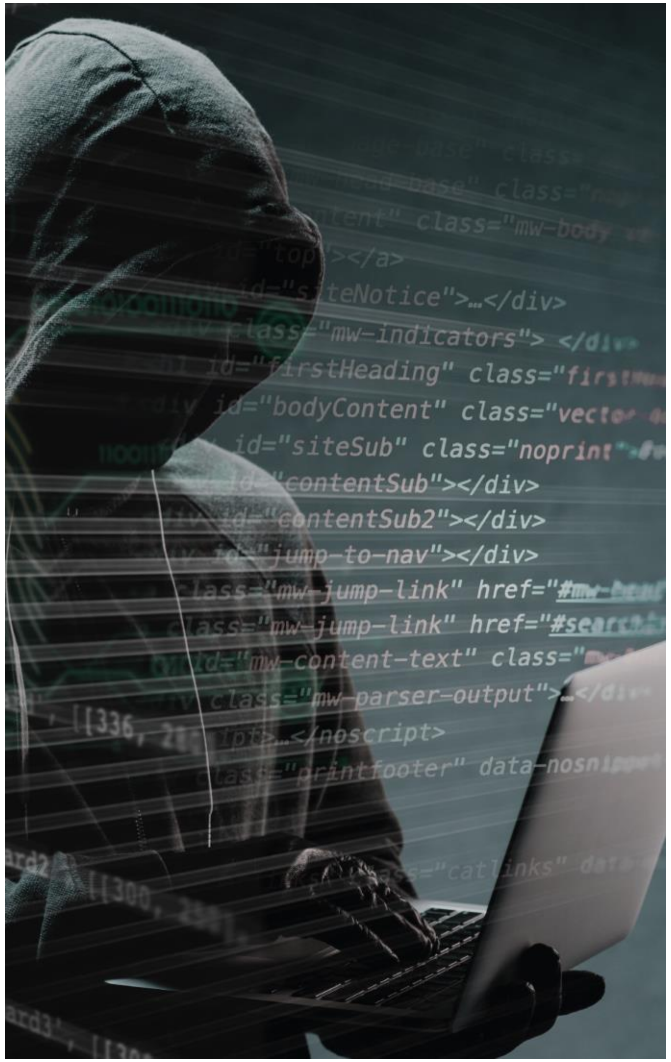
☎ +52 55 5104 8285

¡Alert!

In the past year, Mexico encountered over **85 billion attempted cyberattacks**. Unfortunately, **less than 18% of companies** were adequately prepared to withstand the harassment from hackers and cybercriminals. These cyberattacks don’t solely target large corporations; nearly **50% of them** are aimed at the very core of the country’s economy, affecting both major companies and small and medium-sized enterprises (PyMES).

¿What I can do?

(1). Asociación de Internet MX (AIMX) y el Consejo de Datos y Tecnologías Emergente (CDETECH). (2023). Tercer estudio de ciberseguridad en México 2023. 39.


id="siteNotice">…</div>
class="mw-indicators"> </div>
id="firstHeading" class="firs
id="bodyContent" class="vecto
id="siteSub" class="noprint"
id="contentSub"></div>
id="contentSub2"></div>
id="jump-to-nav"></div>
class="mw-jump-link" href="#mw-head
class="mw-jump-link" href="#search
id="mw-content-text" class="
class="mw-parser-output">…</div>
</noscript>
class="printfooter" data-nosnippet

Context

If measured as a country. **Cybercrime**, with an estimated impact of **$6 trillion**, would be the **third largest economy** in the world after the United States and China.

- Cybersecurity Ventures.

The odds are stacked **against our clients**

3.68 M USD

The cost of a data breach in Latin America[2]

263 mil

3.4 millones mundial

Cybersecurity professionals missing in Mexico

7 meses

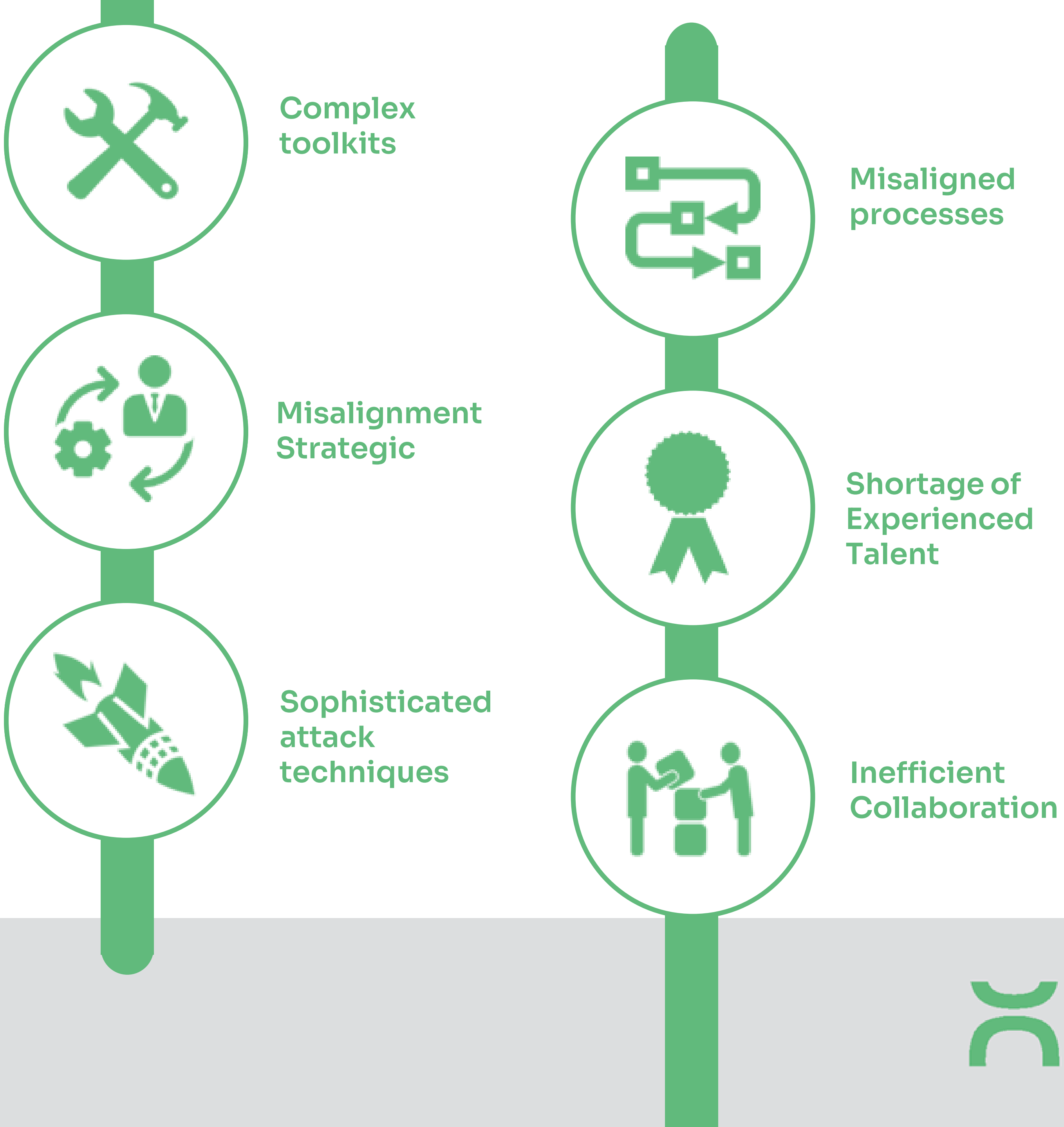
The time it takes for a company to identify that it had a data breach[1]

43%

Of the attacks targeted PyMES, less than 14% were prepared[1]

[1] Data Breach Investigations Report 2022, Verizon
[2] Cost of a Data Breach Report 2022, IBM

Companies need a different approach to face these challenges:



Complex toolkits

Misalignment Strategic

Sophisticated attack techniques

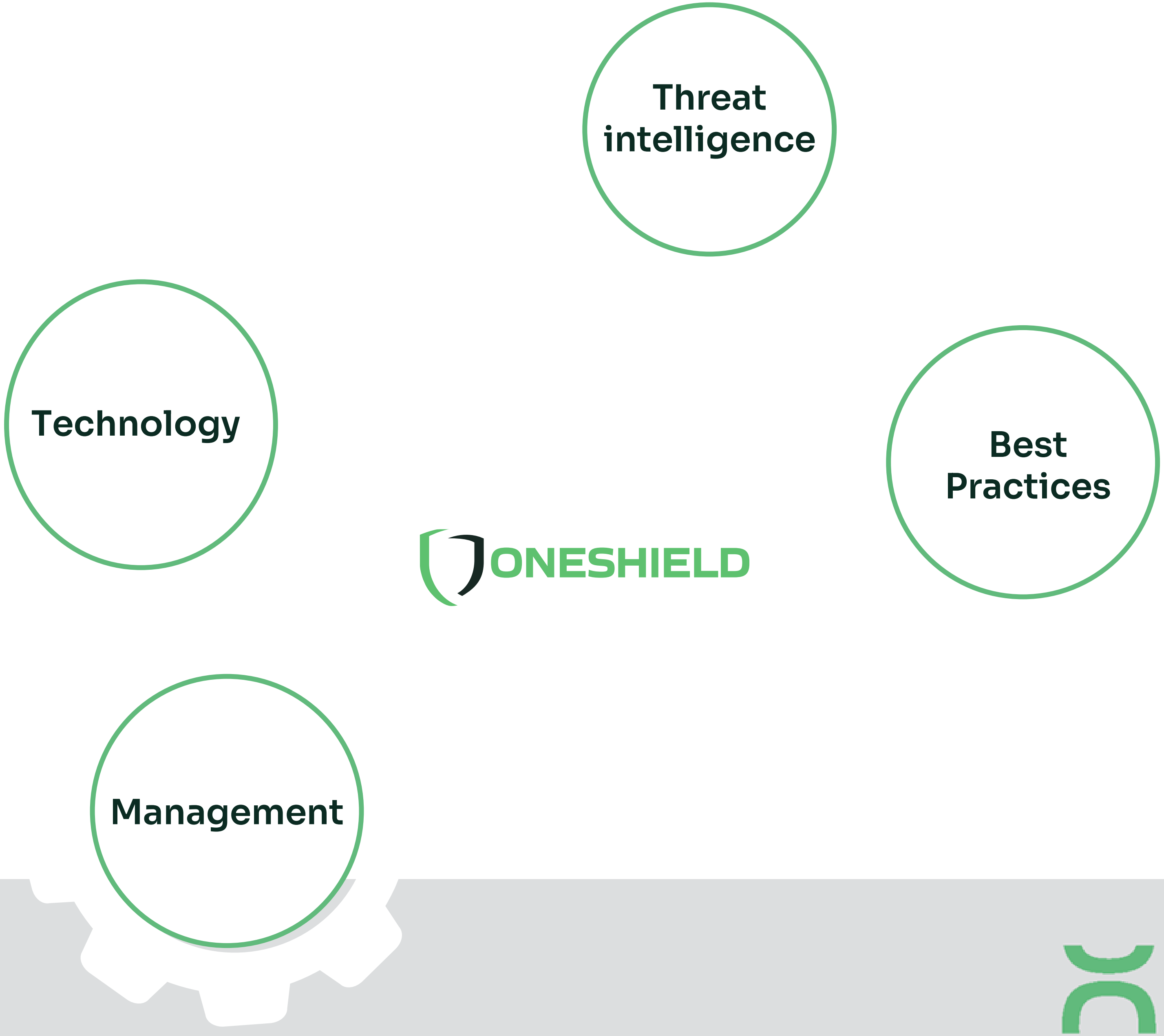
Misaligned processes

Shortage of Experienced Talent

Inefficient Collaboration

ONESHIELD

The first **COMPREHENSIVE** solution that empowers companies and ensures their protection



Threat intelligence

Technology

Best Practices

ONESHIELD

Management

ALWAYS SECURE, *NEVER AT RISK.*

ONESHIELD

Deliver a **comprehensive protection offering that includes** both technology and ongoing implementation, operation, and continuous protection services under a single multi-year contract. This eliminates all the complexity typically associated with this type of solution, making it ideal for **Corporate and Medium Enterprise segments**

The Oneshield offering is designed to support the client by delivering value through a single solution that includes:

Deployment: Once the necessary technology is acquired, Oneshield incorporates the required remediations and configurations to deploy the tools defined in the protection plan according to the client's strategy.

Risk assessment: Drawing from the CIS framework1, we identify the highest security risks within organizations and design and deliver a customized protection strategy for each client and industry.

Managed Service and Continuous Protection: Oneshield manages, operates, and monitors the platform, responding to any threats that jeopardize both the client's operations and their data, applications, and users. The client's security environment remains secure while ensuring swift incident response and mitigation of risks posed by new threats

[1]***CIS**: CIS flt was created in the late 2000s by a coalition of experts and volunteers with the goal of establishing a framework to protect companies from cybersecurity threats. It consists of 20 controls that are regularly updated by experts from various fields (government, academia, and industry) to remain consistently modern and stay ahead of cybersecurity threats (https://www.cisecurity.org/)*

ONESHIELD

Packages

ONESEC

Our Packages

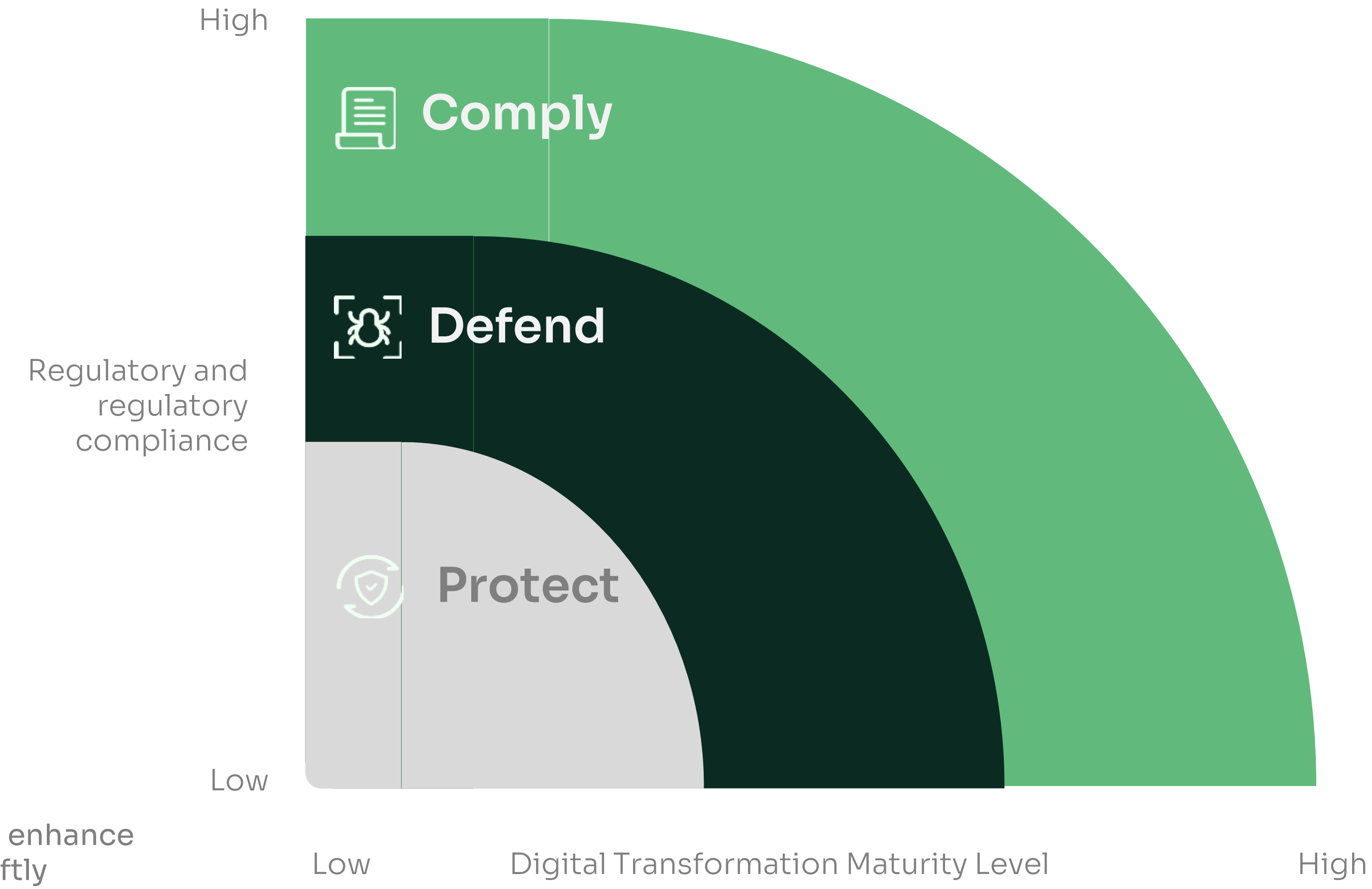
ONESHIELD Microsoft

Oneshield It is built upon the XDR platforms included in **Microsoft 365 Business Premium and Microsoft 365 Enterprise** Security (add-on), as well as Microsoft 365 E5, along with Microsoft Sentinel..

Protect For organizations in the early stages of digital transformation, with the need to protect themselves effectively against modern digital threats and risks.

Defend For organizations with a significant cloud adoption level (Saas, PaaS, and IaaS) and a high reliance on their digital assets for business continuity

Comply For organizations with advanced regulatory compliance needs and requirements for the protection of intellectual and industrial property


High
Comply
Defend
Regulatory and regulatory compliance
Protect
Low
Low
Digital Transformation Maturity Level
High

Oneshield constantly evolves. Soon, we will offer AddOns to enhance security, implement change management practices, and swiftly respond to incidents.

ALWAYS SECURE, *NEVER AT RISK.*

Nuestros Paquetes

	Protect	Defend	Comply
Estrategia de Ciberseguridad	**Incluido**		
Acceso seguro y gobierno de identidad			
Gobierno de identidad	◔	●	●
Doble factor de autenticación	●	●	●
Reglas y control de accesos	●	●	●
Portal de auto-servicio de contraseñas	●	●	●
Protección de contraseñas	●	●	●
Detección, investigación y mitigación de riesgos de identidad	—	●	●
Gestión de privilegios	—	●	●
Acceso basado en riesgos de usuario	—	●	●
Passwordless (Requiere llaves FIDO2 con costo adicional)	◑	●	●
Administración dispositivos de usuario			
Control de dispositivos de usuario	●	●	●
Protección de aplicaciones móviles	●	●	●
Protección contra amenazas avanzadas			
Protección avanzada y filtrado de amenazas que afectan al correo electrónico	◑	●	●
Protección contra amenzas que afectan a las herramientas de colaboración	—	●	●
Detección y respuesta a amenzas en equipos de cómputo	●	●	●
Protección contra amenzas avanzadas y gestión de vulnerabilidades en el equipo de cómputo	—	●	●
Protección contra amenzas avanzadas que afectan a la identidad del usuario	—	●	●

	Protect	Defend	Comply
Estrategia de Ciberseguridad	**Incluido**		
Protección y prevención de fugas de información			
Gobierno de la información	◔	◑	●
Protección de acceso a la información	—	—	●
Prevención de fugas de información	—	—	●
Protección contra riesgos internos	—	—	●
Descubrimiento de datos electrónicos para auditorías.	—	—	●
Control y prevención de fugas de información hacia aplicaciones en la nube (SaaS)	—	●	●
Operación de la plataforma	●	●	●
Monitoreo y respuesta a incidentes 7x24	●	●	●
Monitoreo de fugas o accesos no autorizados a la información.	—	—	●
Suscripciones Microsoft mínimas requeridas.			
De 100 a 300 usuarios	Microsoft 365 Business Premium	Microsoft 365 E3 + AddOn E5 Security o Microsoft 365 E5	Microsoft 365 E5
Más de 300 usuarios	Microsoft 365 E3 + AddOn E5 Security		
*Aplica para cualquier rango de usuarios	Azure Suscription – Microsoft Sentinel		

*Microsoft 365 Business Premium no podrá ser utilizado para más de 300 usuarios.
*Todos los servicios de monitoreo y respuesta a incidentes operan a través de Microsoft Sentinel.

— Funcionalidad no incluida	◔ Algunas funcionalidades incluidas	◑ Mayor implementación de funcionalidades	● Funcionalidad totalmente implementada

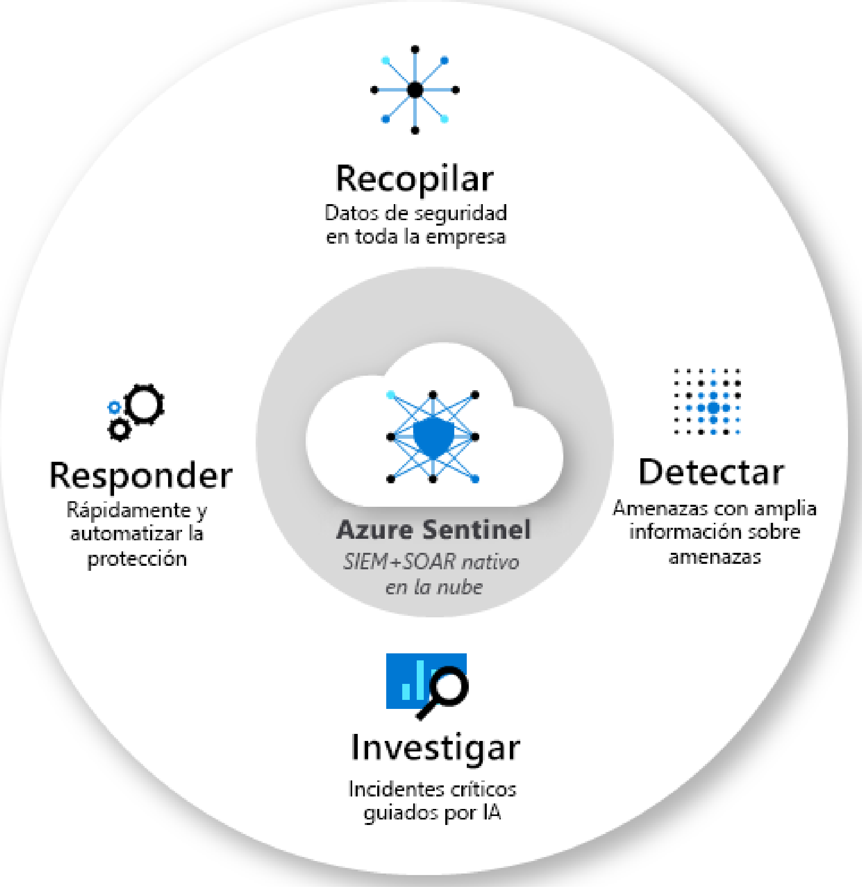
Condiciones comerciales:

- No incluye las suscripciones Microsoft mínimas requeridas, estas deberán ser adquiridas a través de un distribuidor.
- La contratación deberá hacerse de forma anual o trianual con opción de pagos mensuales.
- El número máximo de usuarios es de 1000, cualquier rango extra, deberá cotizarse por separado.
- Atención a requerimientos no críticos de lunes a viernes en horario laboral.
- Monitoreo y respuesta a incidentes los 365 días del año.

ONESHIELD

Incident Monitoring and Response Service

All Oneshield packages come with the 24/7 SOC/MDR service from Onesec. This service is delivered by the same team responsible for protecting hundreds of thousands of users across various industries and segments. They utilize **Microsoft Sentinel** as the SIEM/SOAR solution for monitoring, identification, and response to information security threats


Recopilar
Datos de seguridad en toda la empresa
Responder
Rápidamente y automatizar la protección
Azure Sentinel
SIEM+SOAR nativo en la nube
Detectar
Amenazas con amplia información sobre amenazas
Investigar
Incidentes críticos guiados por IA

Regarding Microsoft Sentinel, here are some important notes:

- Microsoft Azure subscription: The deployment of Microsoft Sentinel is provided as part of the service and incurs an additional cost beyond the solution itself.
- Microsoft sources only: Only Microsoft sources are supported. Connecting other sources may result in additional costs.
- Azure subscription costs: The Microsoft Azure subscription under which Microsoft Sentinel operates will generate additional monthly costs on top of the chosen Oneshield package. These costs depend on:
    1. Variations in the client's business activity.
    2. The number of connected data sources to the solution.
    3. Changes in Microsoft policies related to service costs.
- Oneshield monthly consumption estimate: As part of the initial project activities, Oneshield provides an estimate of monthly consumption.

Please note that these details are subject to change based on specific circumstances and policies.

ONESEC

ONESHIELD

ONESHIELD

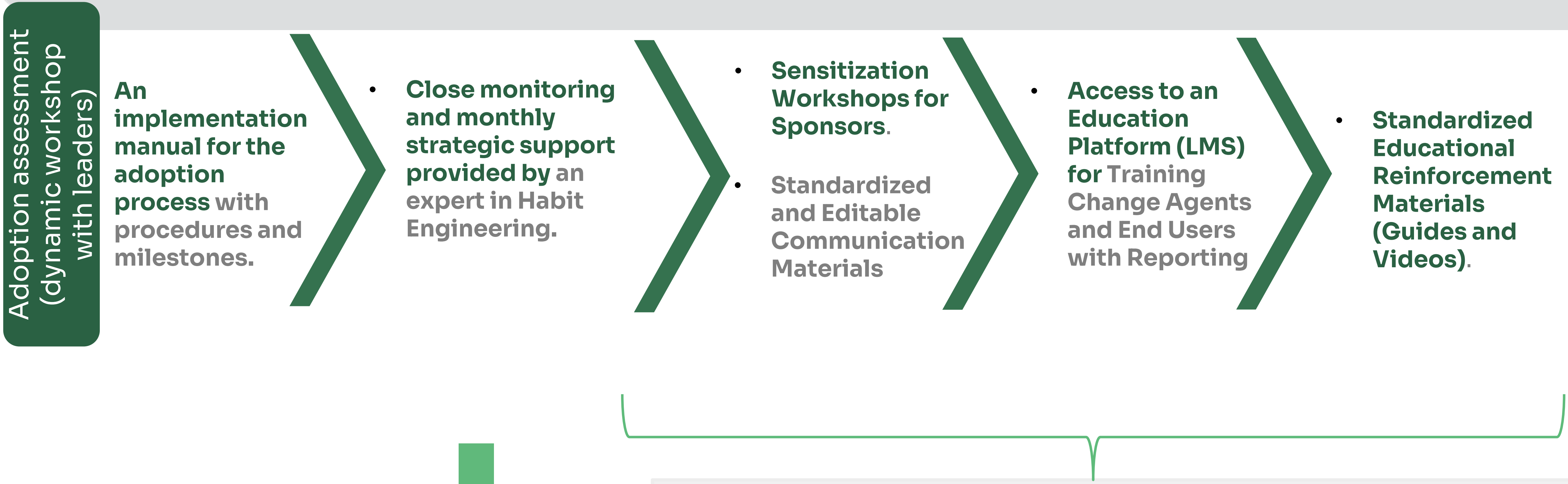
AddOns

ONESEC

Adoption and Change Management (ACM)

To establish a lasting culture of robust cybersecurity through a comprehensive process of technology adoption, as well as emphasizing best protection practices.

The benefits for clients include a security-conscious culture, effective communication, training, and continuous reinforcement.



Adoption assessment (dynamic workshop with leaders)

An implementation manual for the adoption process with procedures and milestones.

- **Close monitoring and monthly strategic support provided by** an expert in Habit Engineering.

- **Sensitization Workshops for Sponsors**.
- Standardized and Editable Communication Materials

- **Access to an Education Platform (LMS) for** Training Change Agents and End Users with Reporting

- **Standardized Educational Reinforcement Materials (Guides and Videos)**.

Based on the contracted technology, its scope, and impact on the end user

UN DIA EXTRA

Crisis management

A **cyberattack** not only has **financial repercussions**, but it can also have **irreparable consequences** on the reputation of products, services, individuals, and companies, **jeopardizing business continuity**.

¿How well-prepared are we to handle a challenging situation in front of the media, authorities, clients, allies, etc.?

We assist you in preparing to manage and reduce the reputational impact of a cyber crisis

- **Prevention and management.**
  - Crisis workshops and manuals
  - Risk identification and signals
  - Situation records and traceability
  - Preemptive mitigation
  - Spokespersons

- **Activation and operation**
  - Assessment and escalation
  - War Room
  - Audiences, messages, and spokespersons
  - Execution/crisis management

- **Recovery**
  - Closure
  - Post-crisis management
  - “Come back” plan

tascomm

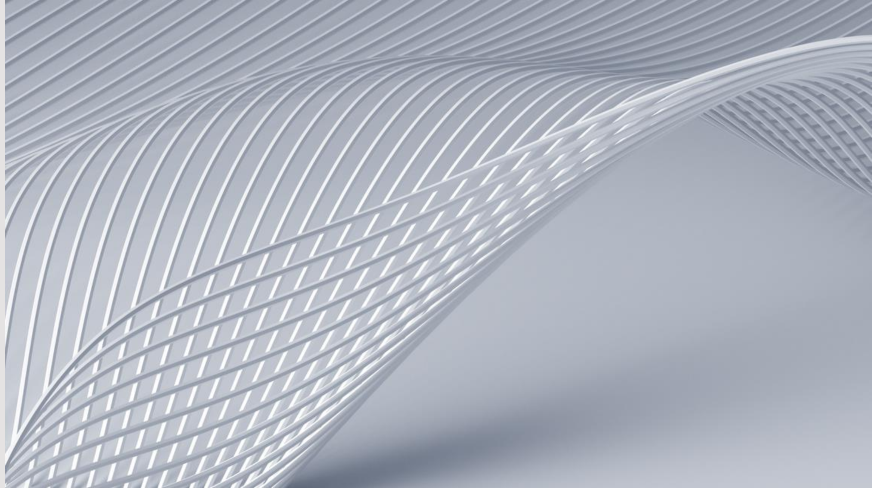
NESEC

ONESHIELD

¿Why Onesec?

ONESEC

¿WHY ONESEC? – MICROSOFT PROFILE
"Better Together"



One of our main advantages is the synergy we have with major allies

Acceda a nuestro perfil y ubíquenos con la razón social * **Secure Nextgen Systems**

MAICPP – Microsoft AI Cloud Partner Program

Microsoft Cloud Partner Designations:

Microsoft Solutions Partner
Security

Microsoft Solutions Partner
Infraestructura Azure

Microsoft Solutions Partner
Digital & App Innovation Azure

Microsoft Solutions Partner
Modern Work

Advanced Specializations:

- Security: Identity and Access Management
- Security: Information Protection and Governance
- Security: Threat Protection
- Security: Cloud Security
- Modern Work: Modernize Endpoints

Member of the specialized programs:

- ✓ FastTrack Ready Partner liga
- ✓ CSI (antes MSSP) Partner (Managed Security Service Provider) liga
- ✓ MISA Partner (Microsoft Intelligent Security Association) liga
- ✓ Microsoft Elite Security Partner
- ✓ FY24 Programs:
  - ✓ ECIF Ready Partner | México y Colombia
  - ✓ Microsoft FY24 Secure Productivity
  - ✓ Microsoft Sentinel Migration and Modernization Investment

Awards:

2023-2024:
Microsoft Security Partner of the Year – LATAM & Caribbean

2022-2023:
Microsoft Country Partner of the Year – MEXICO
Microsoft Compliance Partner of the Year - LATAM

ONESEC

WHY ONESEC? – CERTIFIED EXPERIENCE AND TALENT

ONESEC ONESHIELD

Cybersecurity challenges demand specialized personnel to ensure the success and expected value of projects. Taking this into account, ONESEC has assembled a team backed by international certifications and organizations, thereby ensuring the achievement of our clients' objectives.

Mejores Prácticas

- CISM – Certified Information Security Manager. An ISACA Certification
- CDPSE – Certified Data Privacy Solutions Engineer. An ISACA Certification
- CISA – Certified Information Systems Auditor. An ISACA Certification
- CRISC – Certified in Risk and Information Systems Control. An ISACA Certification
- CGEIT – Certified in the Governance of Enterprise IT. An ISACA Certification
- CCSK v.4 – Certificate of Cloud Security Knowledge – Cloud Security Alliance
- COBIT 2019 Foundation – An ISACA Certificate
- ISO/IEC 27001:2022 Implementer Certified – CertJOIN
- Certified CertiProf – ISO 27001 LEAD AUDITOR
- HCISPP
- SSCP
- ITIL

Defensivas

- GIAC Reverse Engineering Malware – GREM
- GIAC Certified Web Application Defender – GWEB
- GIAC Certified Unix Security Administrator – GCUX
- CISSP – ISSAP, ISSEP, ISSMP
- CSSLP
- CAP
- CCSP
- CHFI – Computer Hacking Forensic Investigator
- ECSS – EC-Council Certified Security Specialist
- ECSA – EC-Council Certified Security Analyst

Ofensivas

- GIAC Penetration Tester – GPEN
- Offensive Security – OSWE
- GIAC Web Application Penetration Tester – GWAPT
- Offensive Security – OSCE
- Offensive Security – OSEP
- Offensive Security – OSCP
- CEH – Certified Ethical Hacker

+52 (55) 8525 4111

SAN JACINTO NO. 8
COL. SAN ÁNGEL, C.P. 01000
ALCALDÍA ÁLVARO OBREGÓN, CDMX.

info@onesec.mx
support@onesec.mx
sales@onesec.mx

LINKEDIN | INSTAGRAM

PRESENCIA EN: CDMX | MONTERREY | GUADALAJARA