TECNOLOGIA AVANZADA
TECNOAV

CIBERSEGURIDAD: POSTURA Y MONITOREO

LÍDERES EN INNOVACIÓN DE SOLUCIONES TECNOLÓGICAS

CARLOS JULIO DIAZ RIVEROS. CEO SOCIETAL SECURITY
IS, MSc, MSi, CEH – AL ISO27001 – LI ISO22301- MBCP – AMBCI - ITIL MCP . LEAD RISK MANAGER - CRISIS MANAGEMENT https://www.linkedin.com/in/carlosjdiaz-ceh-mbcp/

Consultor, instructor y conferencista internacional, con amplia experiencia (24 años) en implementación y capacitación de sistemas de gestión de: **seguridad de la información ISO 7001:2022, ciberseguridad, crisis, resiliencia organizacional.**

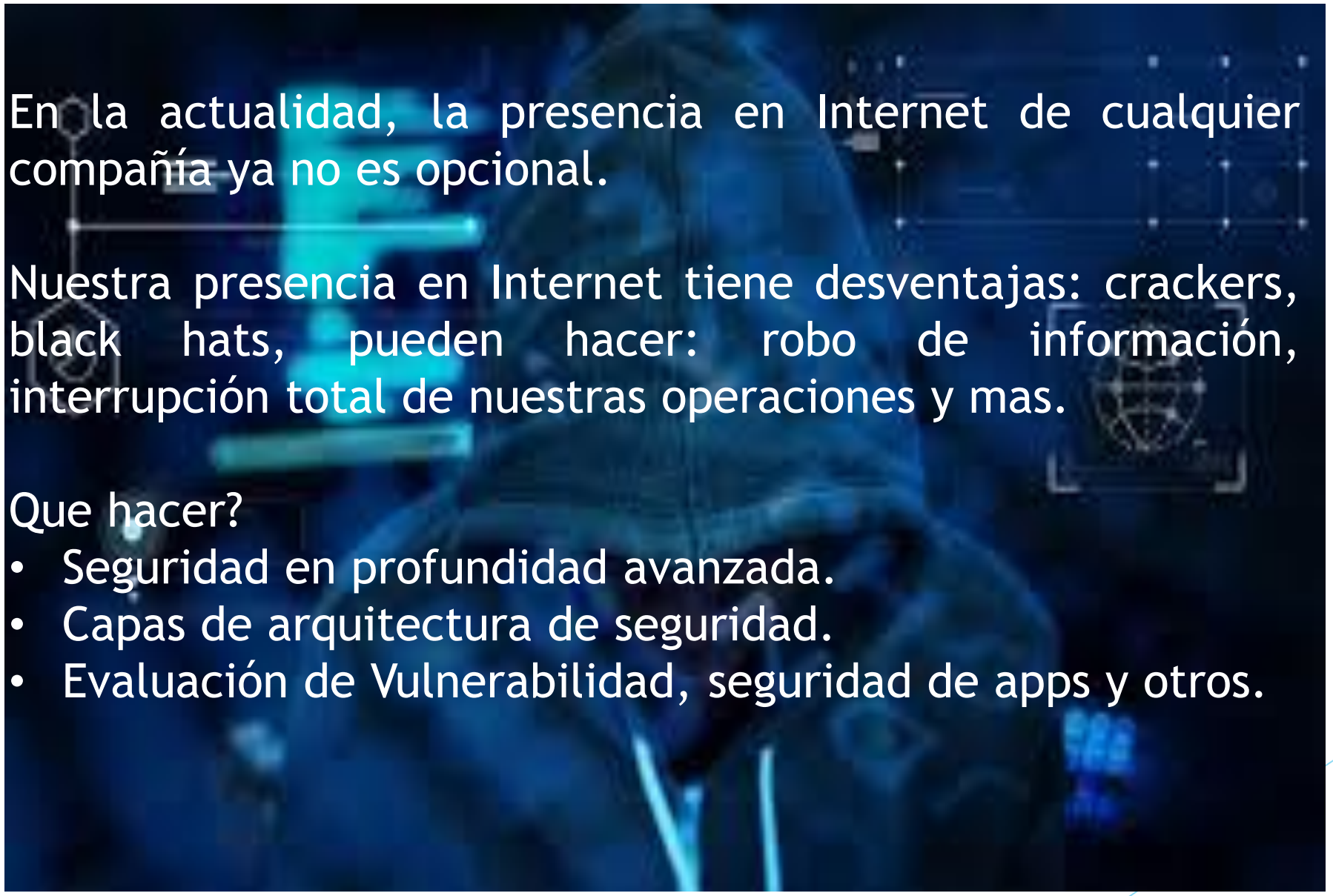
Experto por Colombia en el comité internacional ISO/IEC JTC 001 "Information technology"; donde colaboro en la creación de la NUEVA ISSO 27002 E ISO 27001.

Dirigió **el Working Group 9 ¨Crisis management¨ representando a Colombia.**

A trabajado en diferentes partes del mundo, como **banco Santander, Intel Factory Inc, Ministerio de defensa Israeli, Ministerio de defensa de Colombia,** KPMG, Ecopetrol, DENTONS int; Superintendencia de Panama,….

TECNOLOGIA AVANZADA
TECNOAV

POSTURAS Y CIBERSEGURIDAD



En la actualidad, la presencia en Internet de cualquier compañía ya no es opcional.

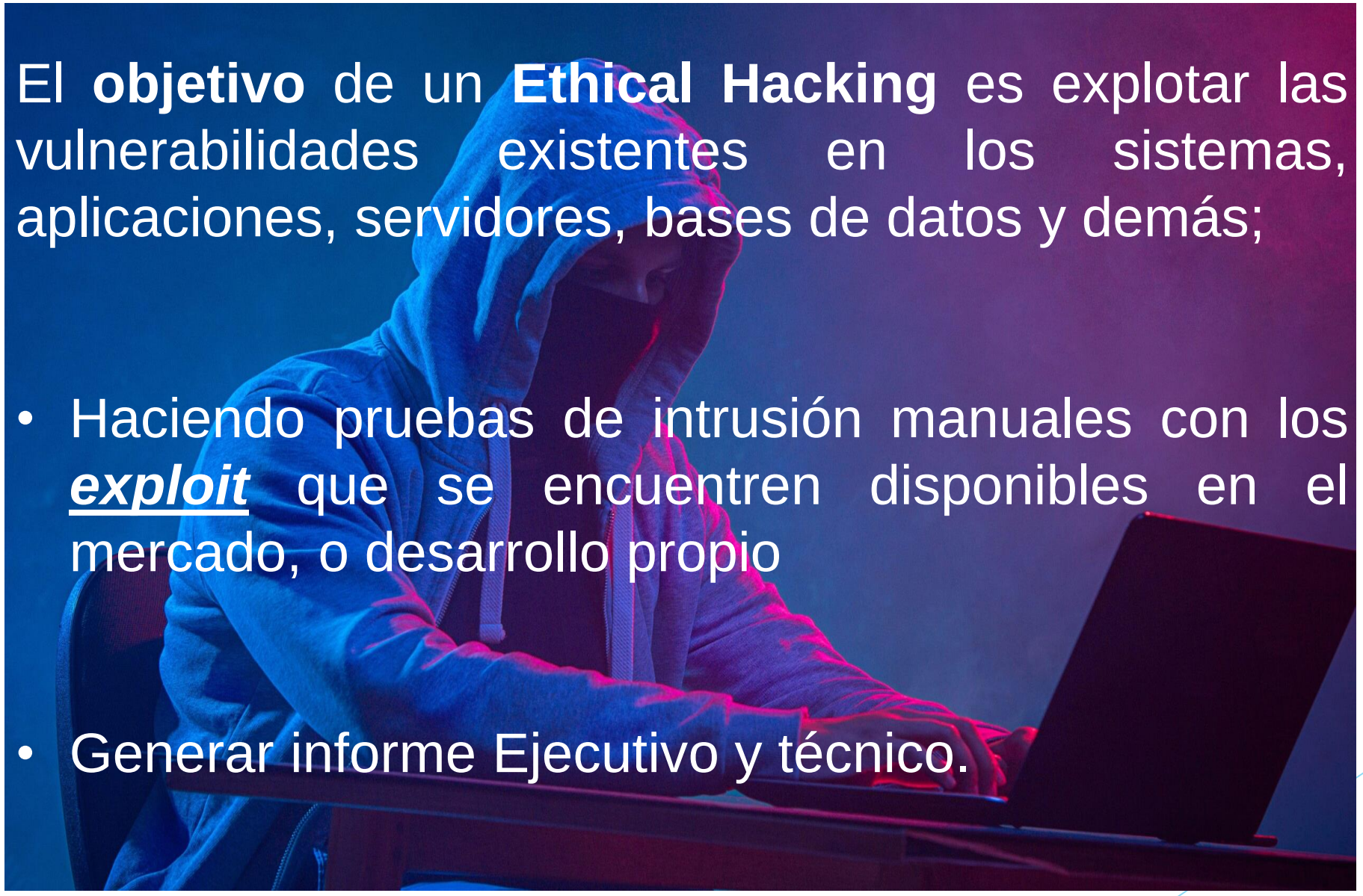
Nuestra presencia en Internet tiene desventajas: crackers, black hats, pueden hacer: robo de información, interrupción total de nuestras operaciones y mas.

Que hacer?

- Seguridad en profundidad avanzada.
- Capas de arquitectura de seguridad.
- Evaluación de Vulnerabilidad, seguridad de apps y otros.

TECNOLOGIA AVANZADA
TECNOAV

MONITOREO: ETHICAL HACKING



El **objetivo** de un **Ethical Hacking** es explotar las vulnerabilidades existentes en los sistemas, aplicaciones, servidores, bases de datos y demás;

- Haciendo pruebas de intrusión manuales con los ***exploit*** que se encuentren disponibles en el mercado, o desarrollo propio

- Generar informe Ejecutivo y técnico.

TECNOLOGIA AVANZADA
TECNOAV

ETHICAL HACKING FASES

- **Fase 1 – Reconocimiento (Reconnaissance)**
- **Fase 2 – Escaneo (Scanning)**
- **Fase 3 – Obtener Acceso (Gaining Access)**
- **Fase 4 – Mantener Acceso (Maintaining Access)**
- **Fase 5 – Limpiar Huellas (Clearing Tracks)**
- **Fase 6 – Generar informe Ejecutivo y técnico.**

TECNOLOGIA AVANZADA
TECNOAV

ETHICAL HACKING FASES

- **Fase 1 – Reconocimiento (Reconnaissance):**

  Se utiliza varias técnicas para investigar y recolectar toda la información necesaria de su objetivo.

- **Fase 2 – Escaneo (Scanning):**

  El hacker utiliza toda la información que recolecto en la Fase de Reconocimiento para identificar vulnerabilidades específicas.

  - ***Posturas de seguridad (positivas y negativas)***
  - ***Líneas bases de seguridad ambientes híbridos - Carbon black***
  - ***Blue team – Red team***
  - ***SOAR - SPLUNK***

- **Fase 3 – Obtener Acceso (Gaining Access):**

  Es la fase de penetración al sistema vulnerable, en esta fase el hacker explota las vulnerabilidades que encontró en la fase de Escaneo MANUALMENTE.

TECNOLOGIA AVANZADA
TECNOAV

POSTURAS DE SEGURIDAD

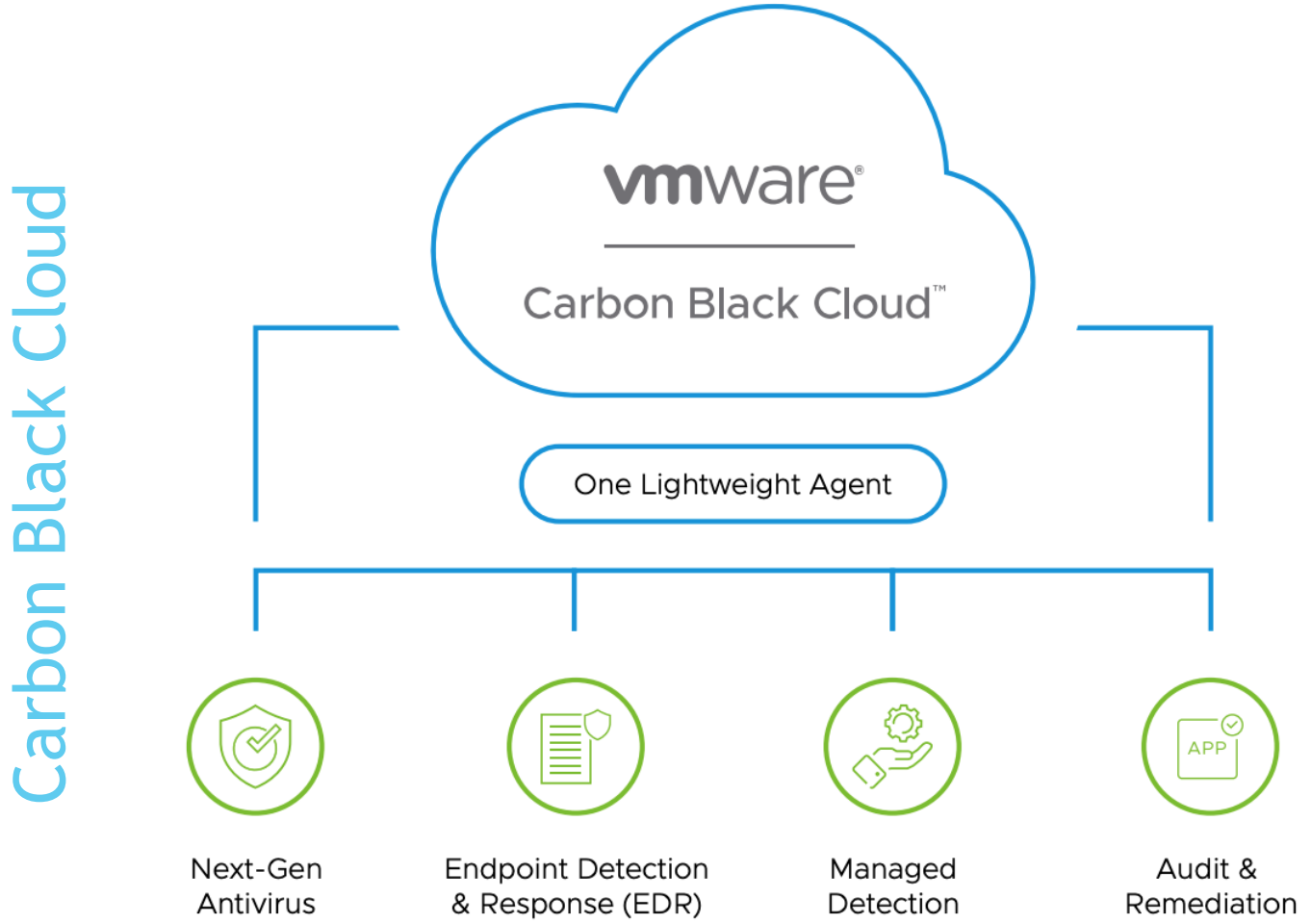
¿Cómo validamos el estado deseado de seguridad de nuestras aplicaciones?

VMware vSphere® Platinum

TECNOLOGIA AVANZADA
TECNOAV

SEGURIDAD EN NUBES HIBRIDAS

¿ Cómo se logra una linea base de seguridad en un esquema hibrido?



TECNOLOGIA AVANZADA
TECNOAV

¿QUÉ FUNCIONES DEBE CUMPLIR UN BLUETEAM EN EL SOC?

TECNOLOGIA AVANZADA
TECNOAV

FUNCIONES DE UN BLUE TEAM

DEFENSA

- Es el equipo de seguridad de la empresa y la primera línea de defensa

CREAN PLANES DE ACCIÓN

- Con el objetivo de mejorar continuamente la seguridad

EVALUAN POSIBLES AMENAZAS

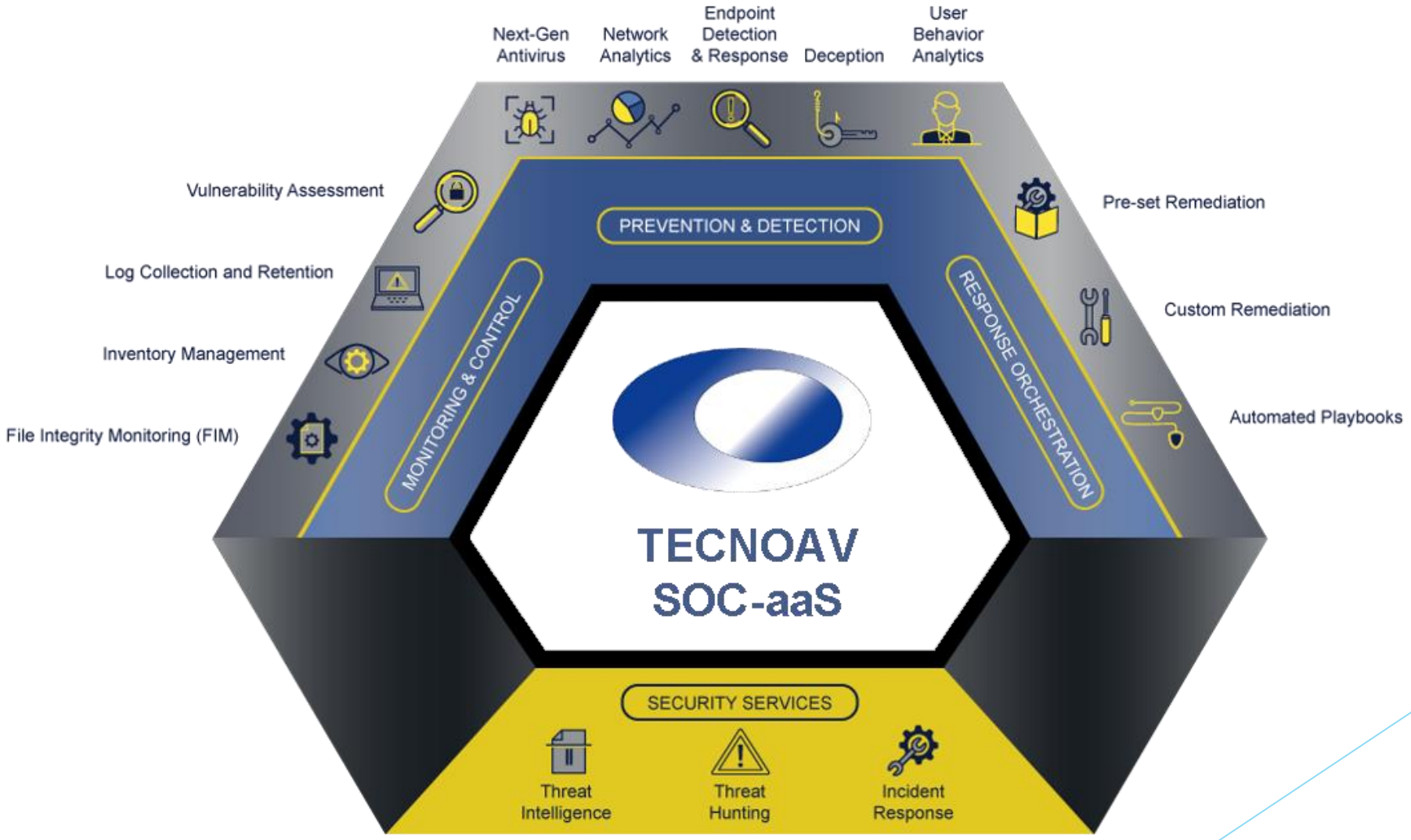
- A través del monitoreo continuo de los sistemas

ANALISIS

- Realizan análisis de patrones y comportamientos para detectar posibles anomalías

TECNOLOGIA AVANZADA
TECNOAV

SOC-AS-A-SERVICE: CAPACIDADES



TECNOLOGIA AVANZADA
TECNOAV

¿CUANDO UNA EMPRESA NECESITA UN SOAR?

TECNOLOGIA AVANZADA
TECNOAV

TECNOLOGIA AVANZADA
TECNOAV

“64% de los eventos de seguridad que se generan al día no son atendidos”

— Enterprise Management Associates

splunk> turn data into doing

TECNOLOGIA AVANZADA
TECNOAV

“46% de los incidentes son automáticamente clasificados como alertas ‘críticas’, pero en verdad solo el 1-5% deberían serlo”

— Enterprise Management Associates

splunk> turn data into doing

TECNOLOGIA AVANZADA
TECNOAV

“30% de las alertas son falsos positivos.”

— Enterprise Management Associates

splunk> turn data into doing

Splunk SOAR

(formerly known as Splunk Phantom)

TECNOLOGIA AVANZADA
TECNOAV

SOAR for Security Operations

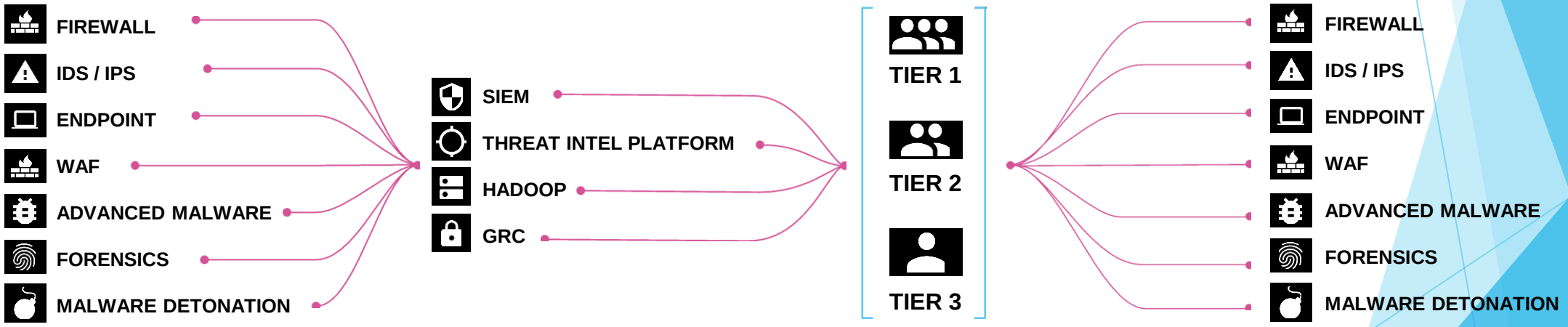
Faster execution through the OODA loop yields better security

Observe
Point Products

Orient
Analytics

Decision Making

Acting



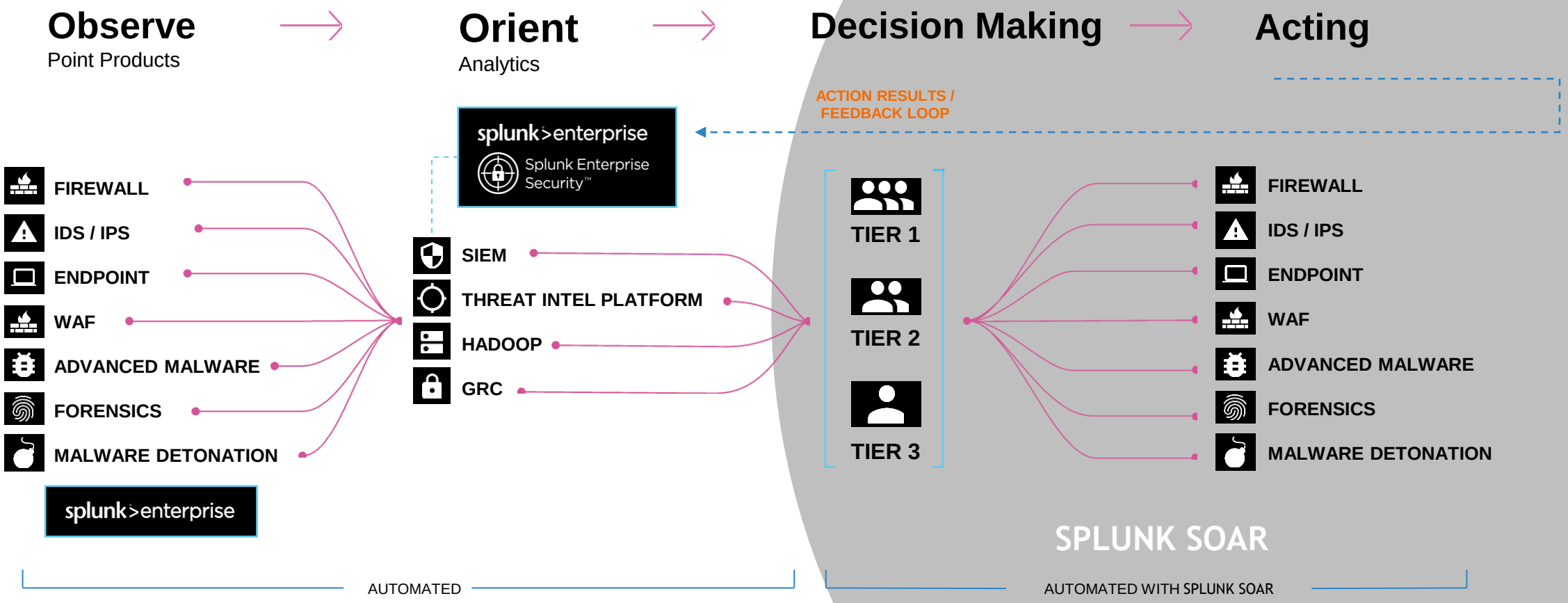
AUTOMATED

WITHOUT SOAR, A MANUAL PROCESS

TECNOLOGIA AVANZADA
TECNOAV

SOAR for Security Operations

Faster execution through the OODA loop yields better security



TECNOLOGIA AVANZADA
TECNOAV

INFORME ETHICAL HACKING
RATING DE RIESGOS ENCONTRADOS

		IMPACTO			
		ACEPTABLE BAJO O NO EFECTO EN EL EVENTO	TOLERABLE EFECTOS EN EL SERVICIO, PERO SIN NO CRITICO	INDESEADO IMPACTO SERIO AL SERVICIO	INTOLERABLE PUEDE RESULTAR EN DESASTRE
PROBABILIDAD	IMPROBABLE RIESGO ES POCO PROBABLE				-
	POSIBLE RIESGO PUEDE OCURRIR EN EL EVENTO		MEDIO R2, R3, R4	ALTO R1, R5	
	PROBABLE RIESGO OCURRIRA				

TECNOLOGIA AVANZADA
TECNOAV

CATEGORIA DE VULNERABILIDADES

Vulnerabilidades de Aplicación

Criticas	Altas	Medias	Bajas
0	15	0	11

Vulnerabilidades de Infraestructura

Criticas	Altas	Medias	Bajas
0	2	20	10

Vulnerabilidades de Arquitectura

Criticas	Altas	Medias	Bajas
0	1	2	0

Vulnerabilidades de Operación y Gestión

Criticas	Altas	Medias	Bajas
0	2	0	0

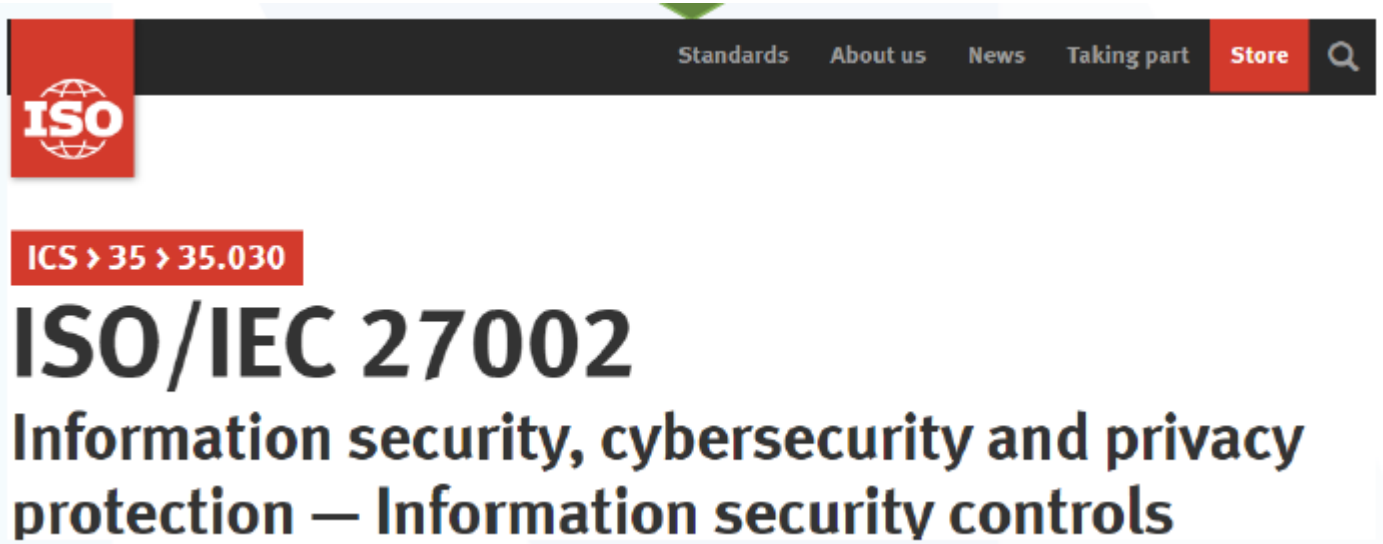
TECNOLOGIA AVANZADA
TECNOAV

RIESGO DISPONIBILIDAD DE SERVICIO

Tema	Detalles	
Detalle de Escenario de Riesgo	R1. Un atacante externo puede causar una negación de servicios a nivel de aplicación utilizando vulnerabilidades en el servidor web de www.s	
Evaluación de Riesgo	Probabilidad	POSIBLE
	Impacto	INDESEADO
	Nivel de Riesgo	ALTO
Tipo de Consecuencias	Perdida de disponibilidad de servicio Impacto en la reputación Disminución en calidad de nivel de servicio	
Detalle de Consecuencias	Debido a vulnerabilidades presentes en el servidor web que provee servicios para ww.set-icap.co y la falta de un firewall de aplicación web para proteger contra ataques web dirigidos a la aplicación y al servidor web. Atacantes con intención maliciosa pueden generar un ataque de negación de servicio y potencialmente pueden exigir el pago de dinero o bitcoin para no iniciar un ataque en contra de la empresa.	
Fuentes de Amenaza	External/Intencional	
Vulnerabilidades Relacionadas	Múltiples vulnerabilidades en Apache Tomcat (Alta) Servidor Web no soportado por vendedor	
Mitigación	Actualizar servidor de aplicaciones Tomcat a una versión soportada por el fabricante que contenga mitigación a vulnerabilidades detectadas en versiones anteriores.	
Recurso Afectado	http://www. 200.26.137.	

TECNOLOGIA AVANZADA
TECNOAV

IMPLEMENTACION SISTEMAS DE GESTION SEGURIDAD DE LA INFORMACION ISO 27001 DEL 2022



ISO/IEC 27002:2022	ISO/IEC 27002:2013
"Information security, cybersecurity and privacy protection — Information security controls"	"Information technology — Security techniques — Code of practice for information security controls"
93 Controles	114 controles
4 Categorías y 2 Anexos	14 Categorías

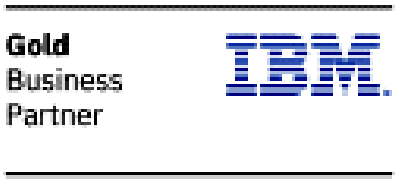
TECNOLOGIA AVANZADA
TECNOAV

IMPLEMENTACION SISTEMAS DE GESTION SEGURIDAD DE LA INFORMACION ISO 27001 DEL 2022

ISO/IEC 27002:2022	
Controles de la organización:	37 controles de gestión de la organización
Controles enfocadas a personas:	8 controles de la seguridad enfocados a los recursos humanos
Controles Físicos:	14 controles de seguridad en el entorno físico
Controles tecnológicos:	34 controles con soluciones tecnológicas de seguridad
ANEXO A:	Matriz con los 93 controles y sus atributos
ANEXO B:	Correspondencia entre los controles de la nueva versión y la versión anterior.

TECNOLOGIA AVANZADA
TECNOAV

NUESTROS PARTNERS



NUESTROS SERVICIOS

ANÁLISIS SEGURIDAD APLICACIONES

ETHICAL HACKING

ANÁLISIS DE VULNERABILIDADES

IMPLEMENTACIÓN ISO 27001:2022

GESTIÓN DE CRISIS TABLETOP EXERCISE

INFORMÁTICA FORENSE

INGENIERÍA SOCIAL

CONTINUIDAD DE NEGOCIO - BCP – DRP

ALGUNOS DE NUESTROS CLIENTES

BANCO DEL PACÍFICO
Más banco banco para ti

VISITENOS EN NUESTRO STAND PARA MAYOR INFORMACION

Denise Roca
Gerente de Software
droca@tecnoav.com
info@tecnoav.com
cel.:0999792514

TECNOLOGIA AVANZADA
TECNOAV

www.tecnoav.com

TECNOLOGIA AVANZADA
TECNOAV