

El rol de la auditoría interna en la gestión de incidentes de ciberseguridad

Andrés Casas

Jornada
2022

 **ISACA.**
Costa Rica Chapter

 Instituto de
Auditores Internos
de Costa Rica



Andrés Casas

 andres.casas@brakk.us



Agenda

- El hostil mundo de los ciber-ataques
- Conceptos clave
- Ciclo de vida de la gestión de incidentes

Agenda

- **EL HOSTIL MUNDO DE LOS CIBER-ATAQUES**
- Conceptos clave
- Ciclo de vida de la gestión de incidentes





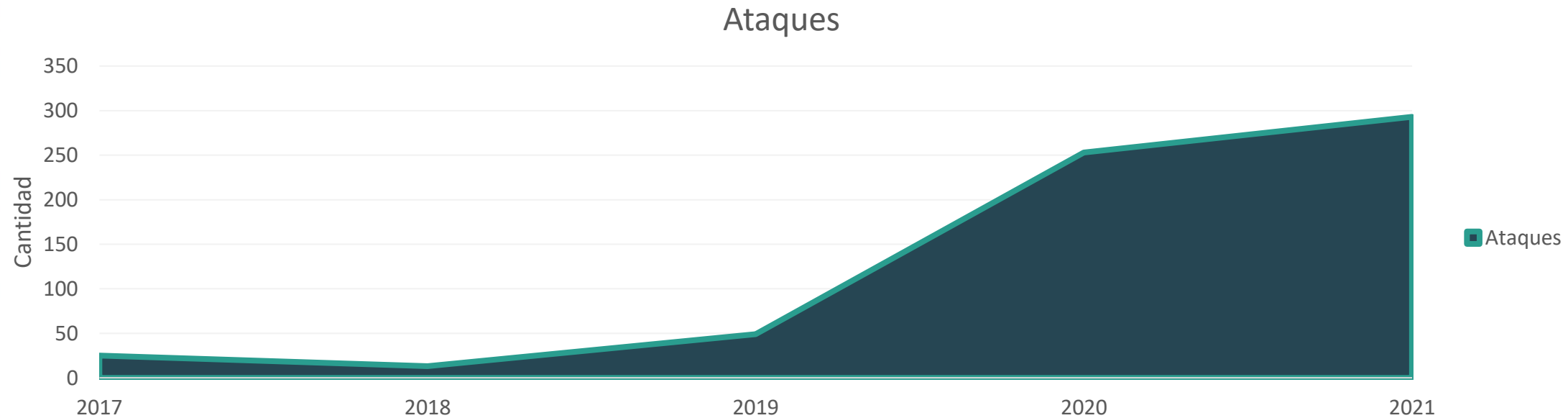
USD\$ 400,000,000,000

Jornada
2022



USD\$ 6,000,000,000,000

Incremento de ataques ransomware



Fuente: Five Lessons Learned from Over 600 Ransomware Attacks, RiskRecon MasterCard

¿Cuál es su mayor preocupación por el crimen cibernético?

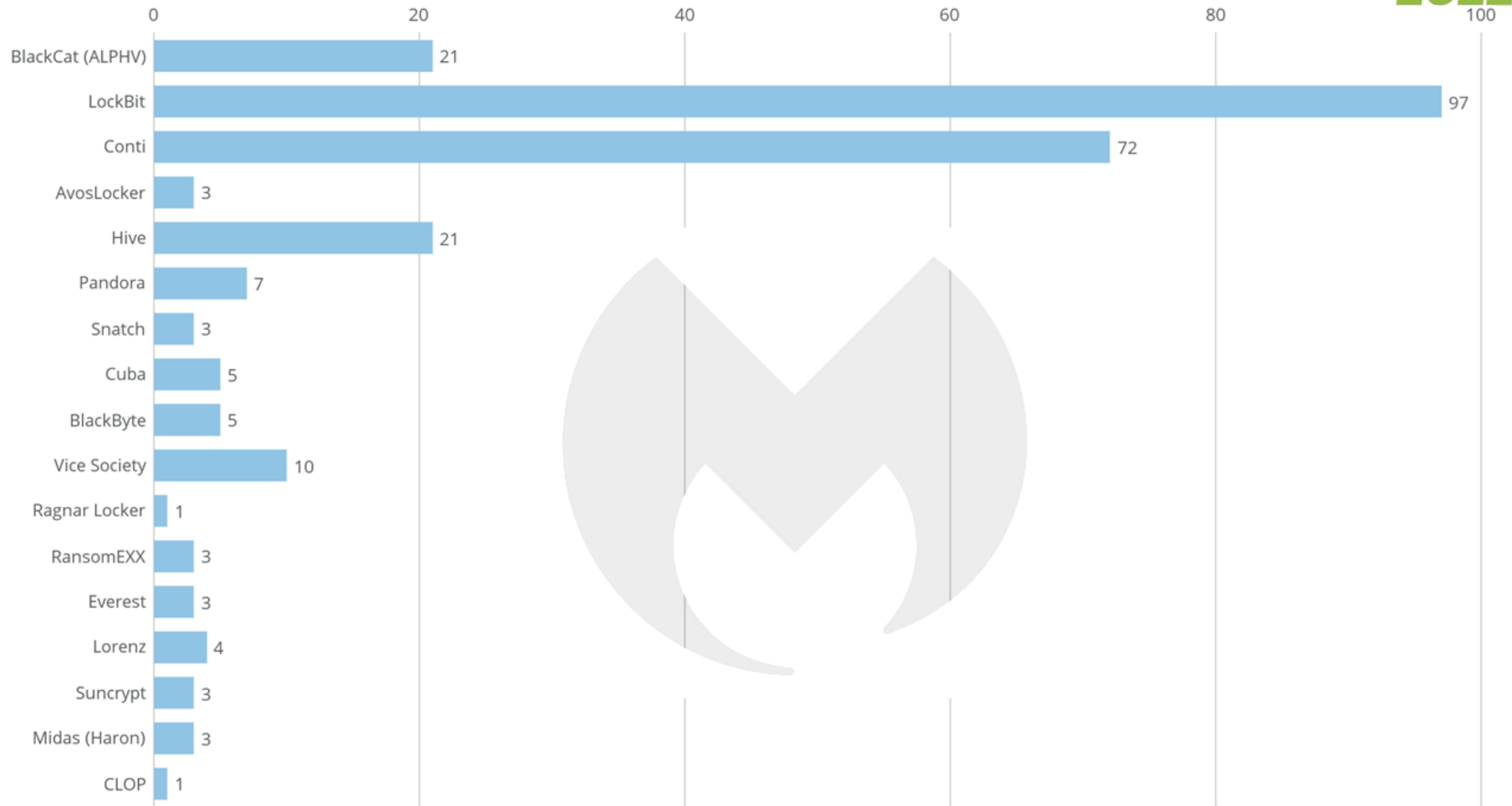
Jornada
2022

El FBI presentó informes de casi \$ 2.4 mil millones en pérdidas de víctimas por estafas BEC en 2021. Eso fue 49 veces más que el rendimiento del ransomware reportado al FBI (\$ 49.2 millones), y más de un tercio del total de delitos cibernéticos (\$ 6.9 mil millones).

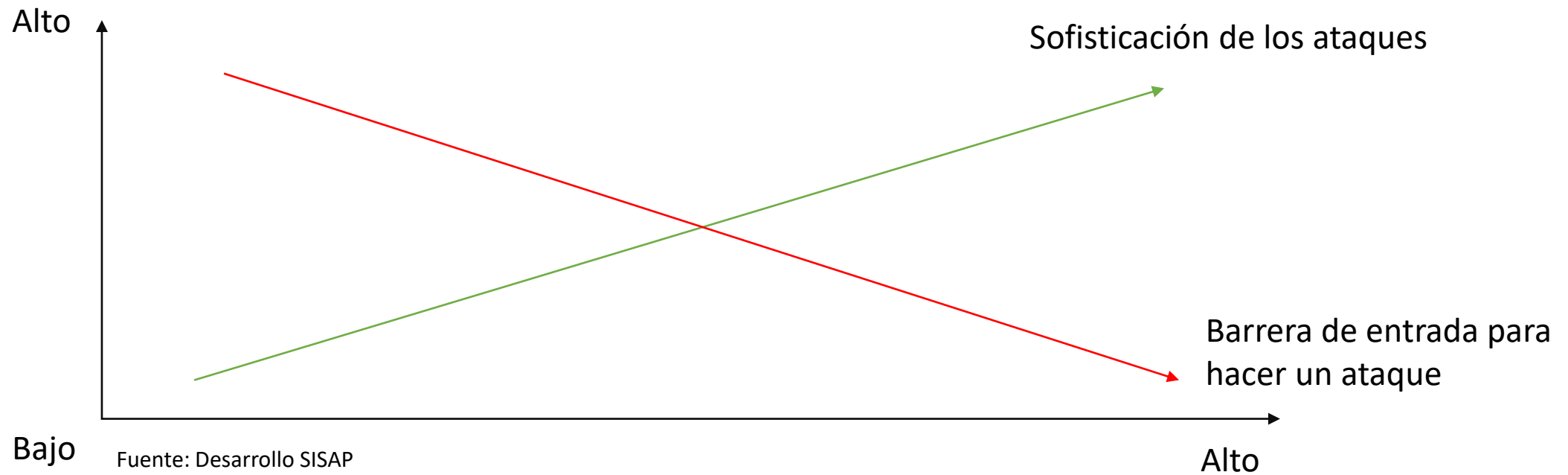
Fuente: Internet Crime report https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Ataques de ransomware por banda

Jornada
2022



Ingreso al mercado

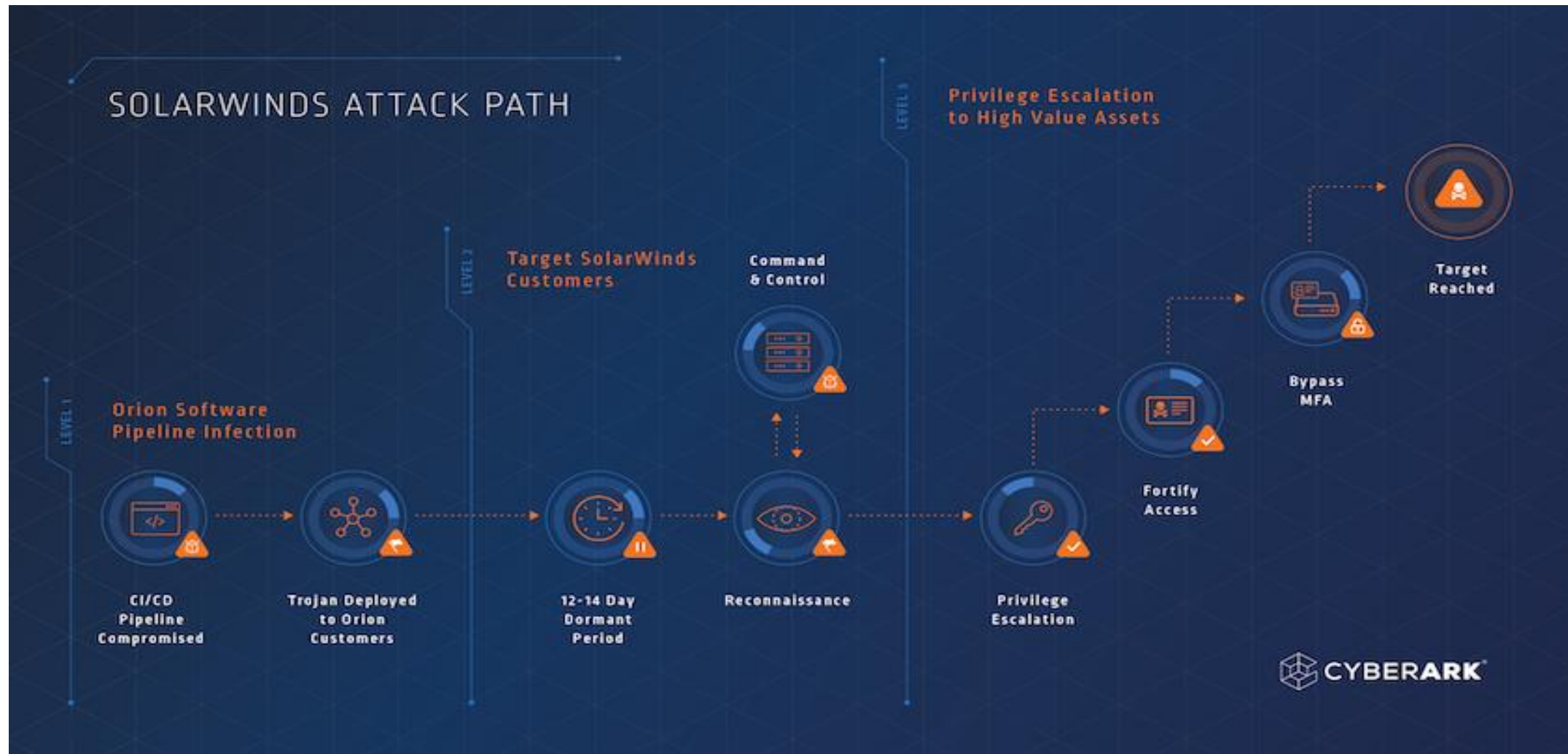


Ingreso al mercado

Jornada
2022

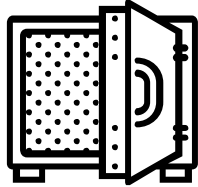


Caso SolarWinds



Agenda

- El hostil mundo de los ciber-ataques
- **CONCEPTOS CLAVE**
- Ciclo de vida de la gestión de incidentes



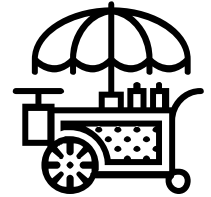
Confidencialidad

Garantizar la privacidad de los datos.



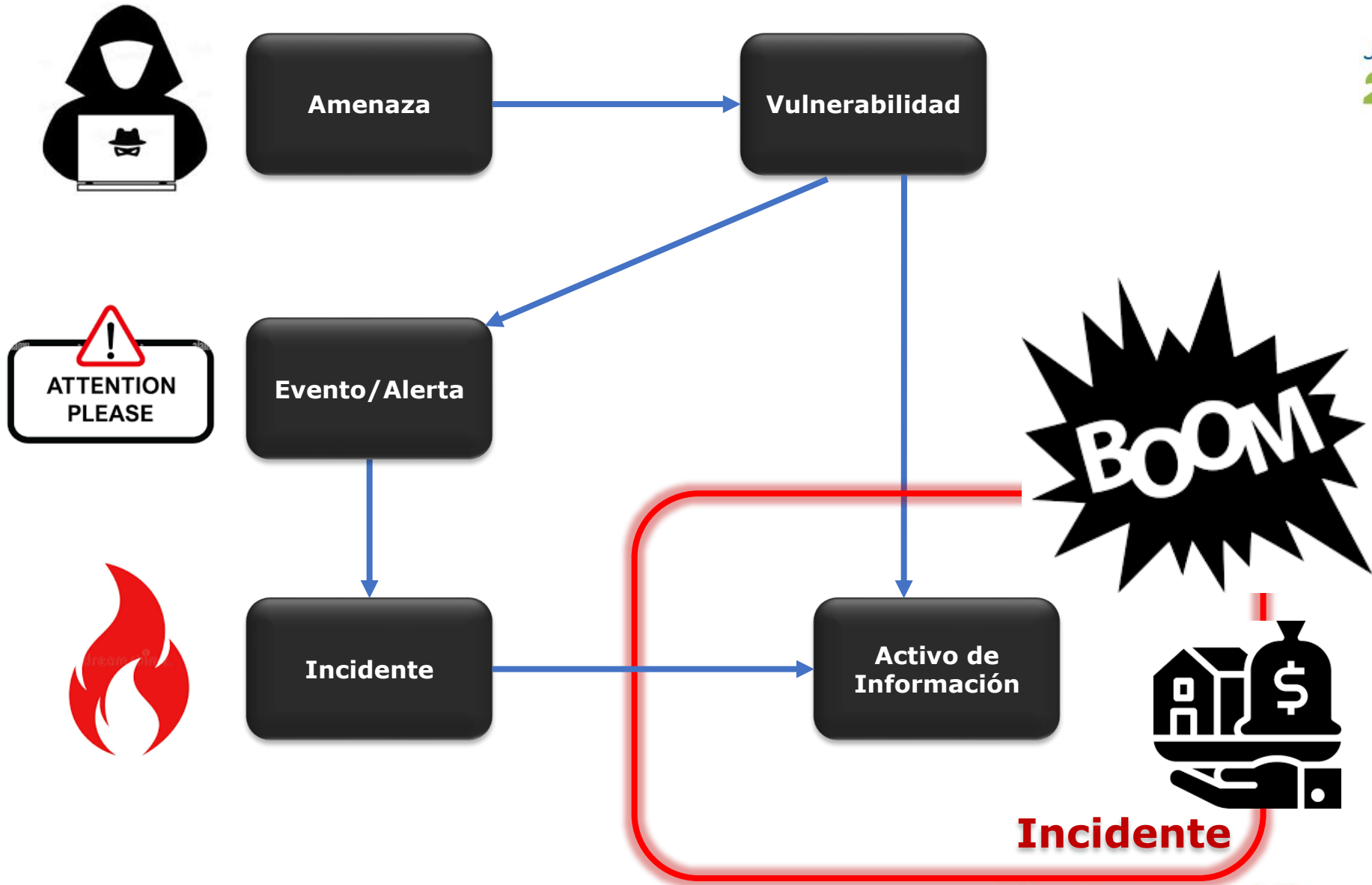
Integridad

Garantizar que la información sea precisa y confiable.



Disponibilidad

Garantizar que la información esté disponible a las personas autorizadas.



Fuente: ISO 27035 – Técnicas de seguridad Gestión de incidentes de seguridad de la información

Amenazas

Causa **potencial** de un **incidente no deseado**, el cual puede ocasionar daño a un sistema o a una organización.

Vulnerabilidad

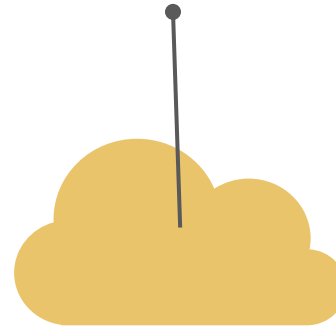
Debilidad de un activo o de un **control** que puede ser explotada por una o más **amenazas**.

Crterios

Jornada
2022

COBIT 2019

Marco: Objetivos de gobierno y gestión



ISO 27035

Técnicas de seguridad
Gestión de incidentes
de seguridad de la
información

NIST CSF

Cyber Security
Framework



NIST.SP.800

Incident Handling
Guide



Cyber Fusion Center

Jornada
2022

Next-generation SOC

Vulnerability
management



Threat intelligence



Threat
response

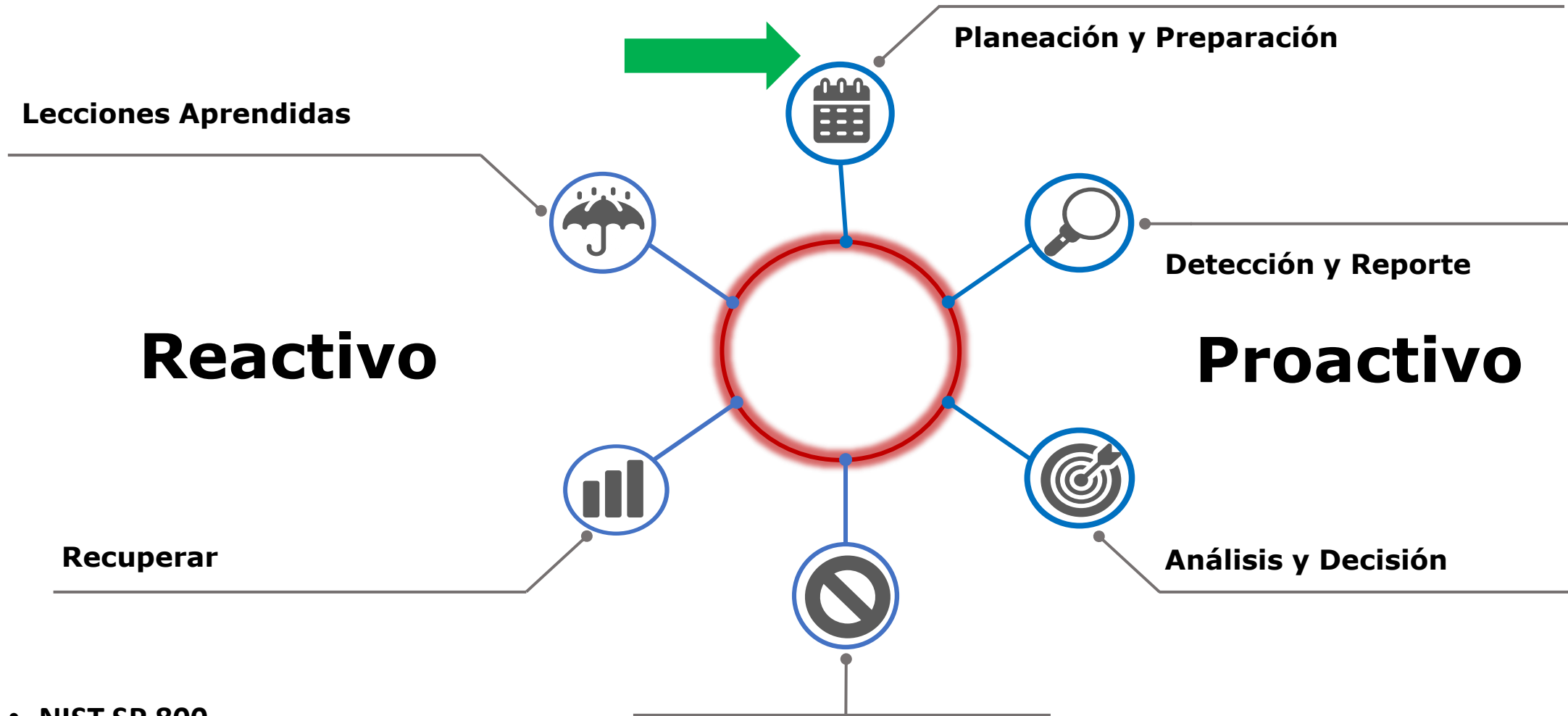
Threat detection

Agenda

- El hostil mundo de los ciber-ataques
- Conceptos clave
- **CICLO DE VIDA DE LA GESTIÓN DE INCIDENTES**

Ciclo de vida

Jornada
2022



- NIST SP 800
- ISO 27035

Contener y Erradicar

Ciclo de vida - Planeación y preparación

Jornada
2022

01

Alinear la estrategia del negocio con los objetivos de seguridad Para la gestión de incidentes.

Definir políticas y procedimientos de seguridad.

02

03

Ejecutar un análisis de riesgos de seguridad.

Establecer un plan de gestión de incidentes de seguridad.

04

05

Definir los equipos de respuesta a incidentes.

Ciclo de vida - Planeación y preparación

Jornada
2022

06

Establecer relaciones y conexiones.

Definir el soporte técnico y otros.

07

08

Definir el soporte técnico y otros.

Pruebas.

09

Ciclo de vida - Planeación y preparación

Jornada
2022

06

Establecer relaciones y conexiones.

Definir el soporte técnico y otros.

07

08

Definir el soporte técnico y otros.

Pruebas.

09

Ciclo de vida - Planeación y preparación

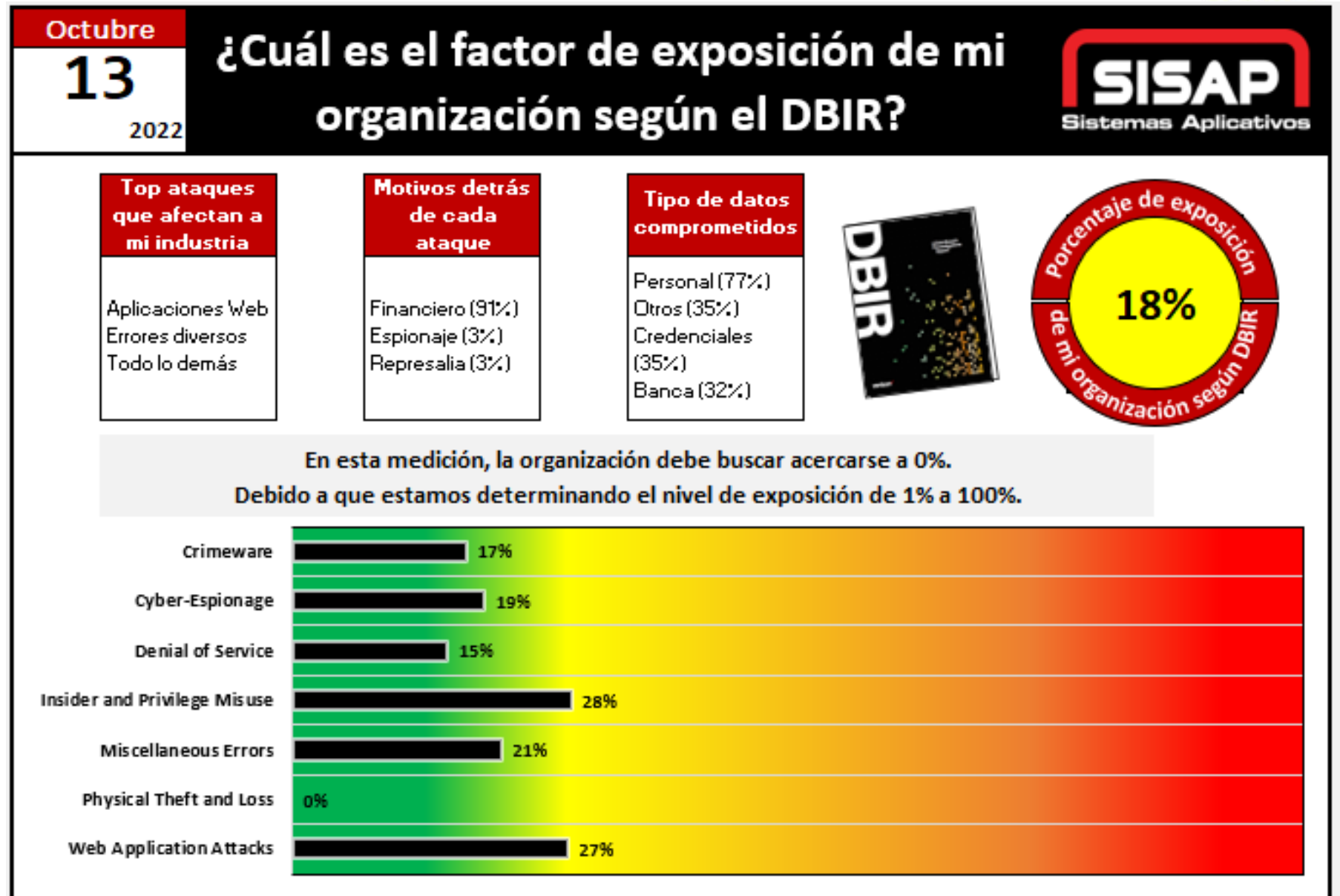
Jornada
2022

Cada organización debería documentar una política para la gestión de eventos, incidentes o vulnerabilidades de seguridad, como parte de su política holística para la gestión de seguridad de la información. Algunos de sus componentes clave son:

- Debe ser documentada a alto nivel.
- Debe establecer el propósito, objetivos y alcance de la política.
- Debe establecer la importancia de la gestión de incidentes para la organización.
- Debe establecer qué se considera como un incidente de seguridad para la organización.
- Debe incluir una descripción de las categorías de incidentes de seguridad.
- Debe definir las responsabilidades de las partes interesadas.
- Debe establecer las autoridades y líneas de reporte y comunicación.
- Debe establecer cualquier iniciativa de concientización y capacitación que requiera el personal.
- **Debe estar aprobada por la alta gerencia.**

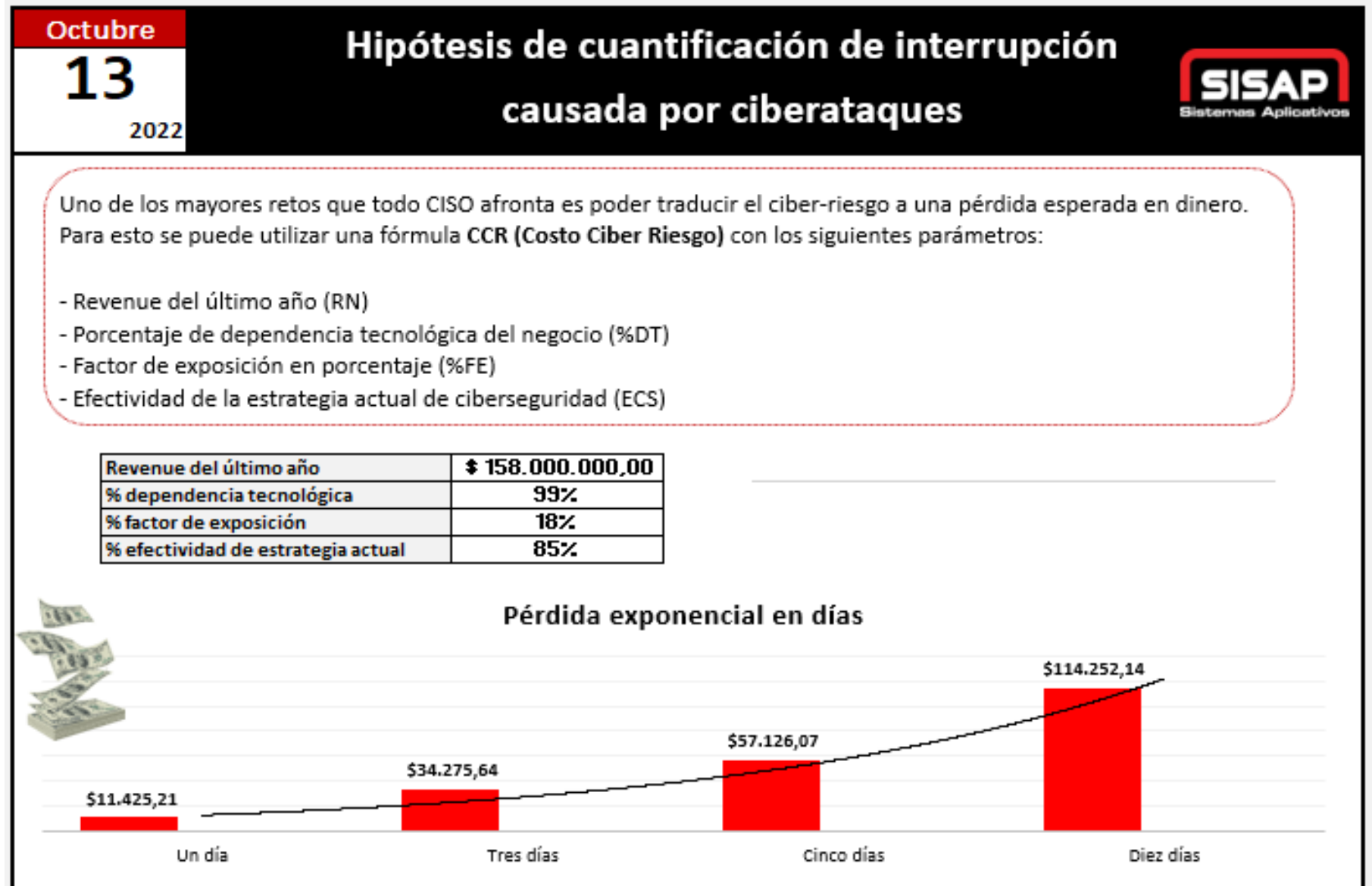
Ciclo de vida – Gestión de riesgos

Jornada
2022



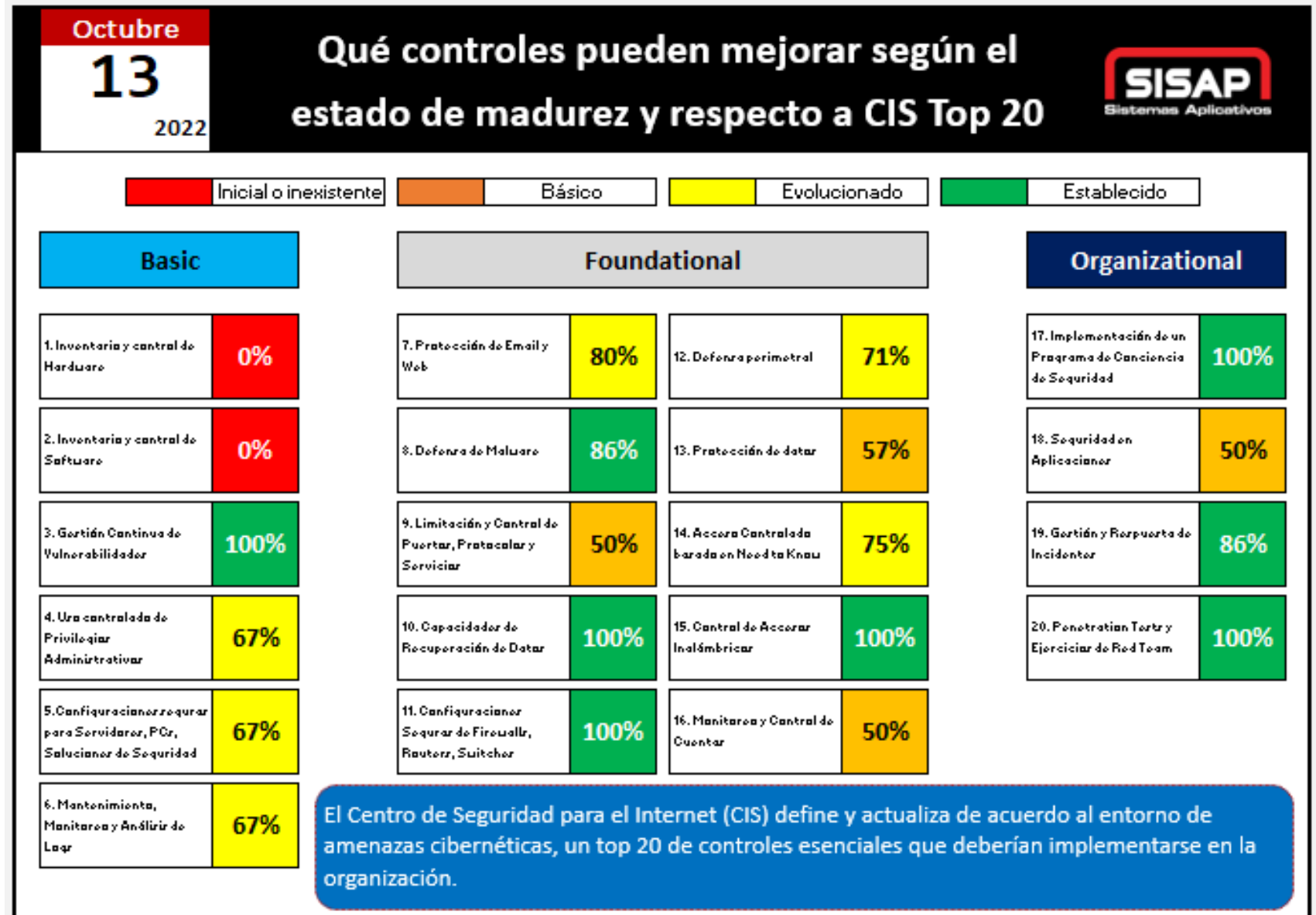
Ciclo de vida – Gestión de riesgos

Jornada
2022



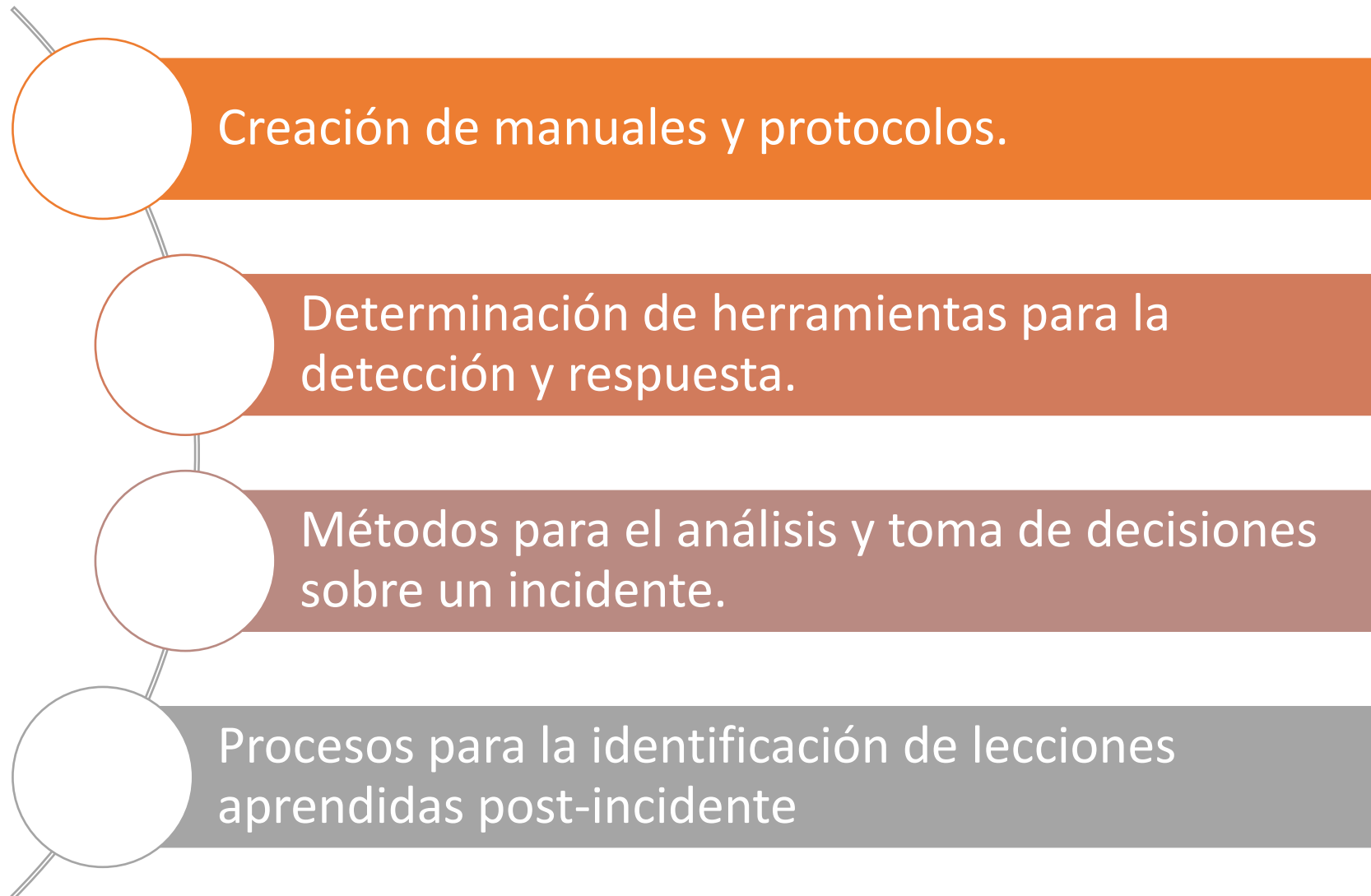
Ciclo de vida – Gestión de riesgos

Jornada
2022



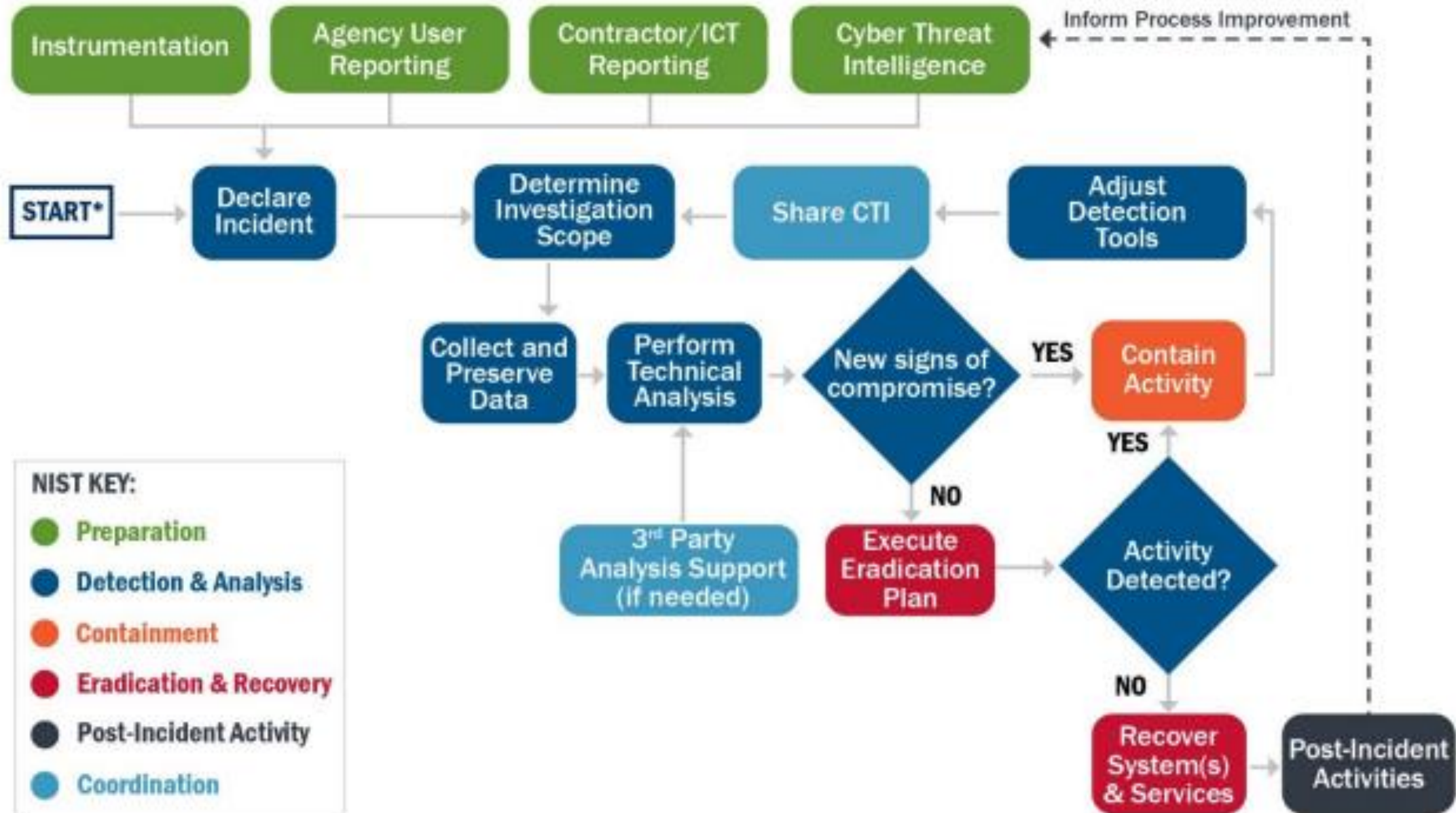
Ciclo de vida – Plan de gestión de incidentes

Jornada
2022

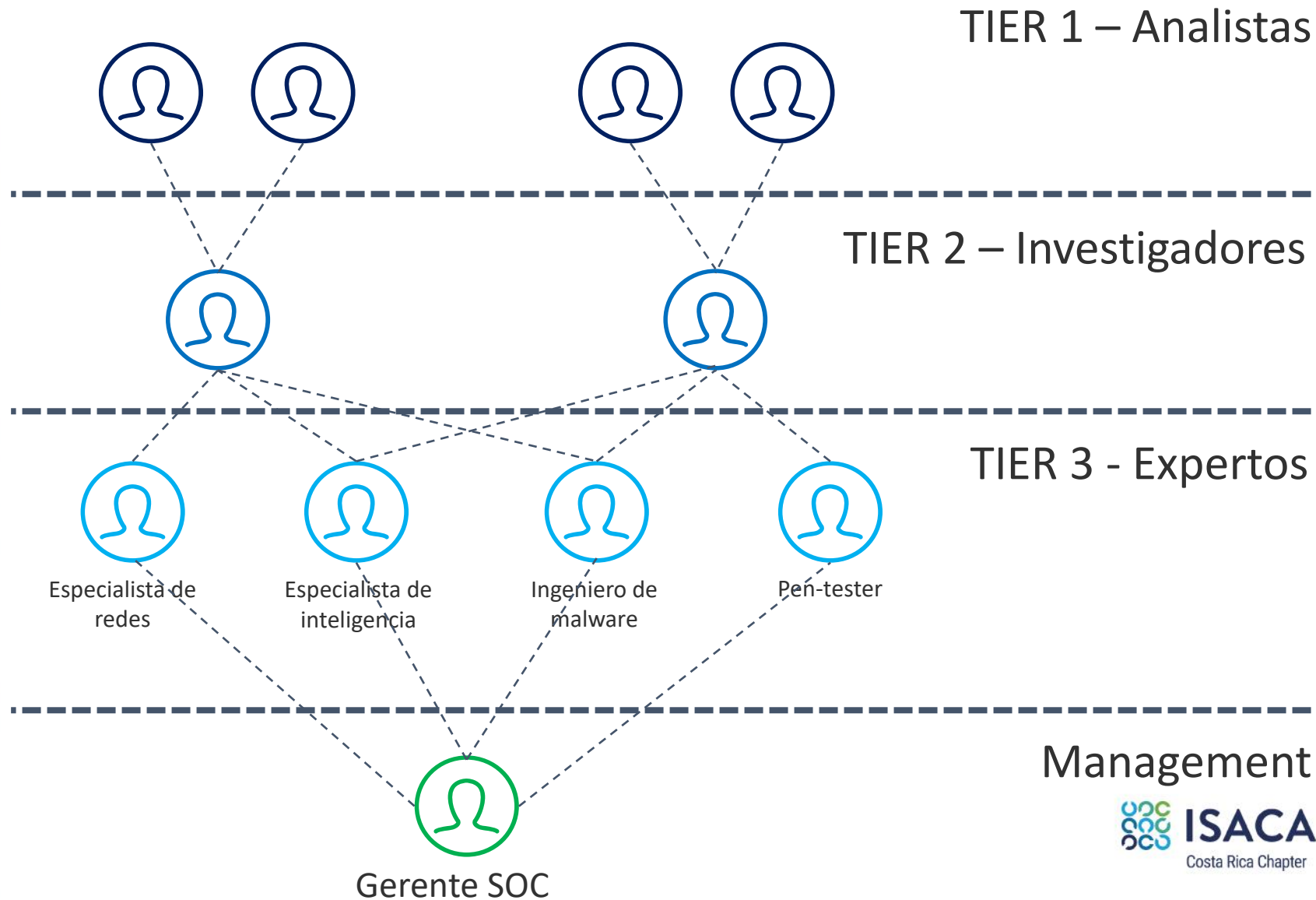


Ciclo de vida – Proceso

Jornada



Ciclo de vida – Equipo de respuesta



Management

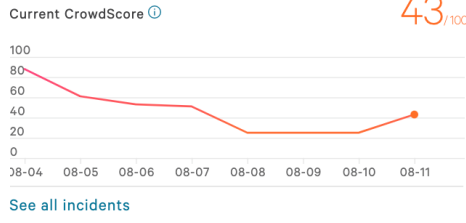
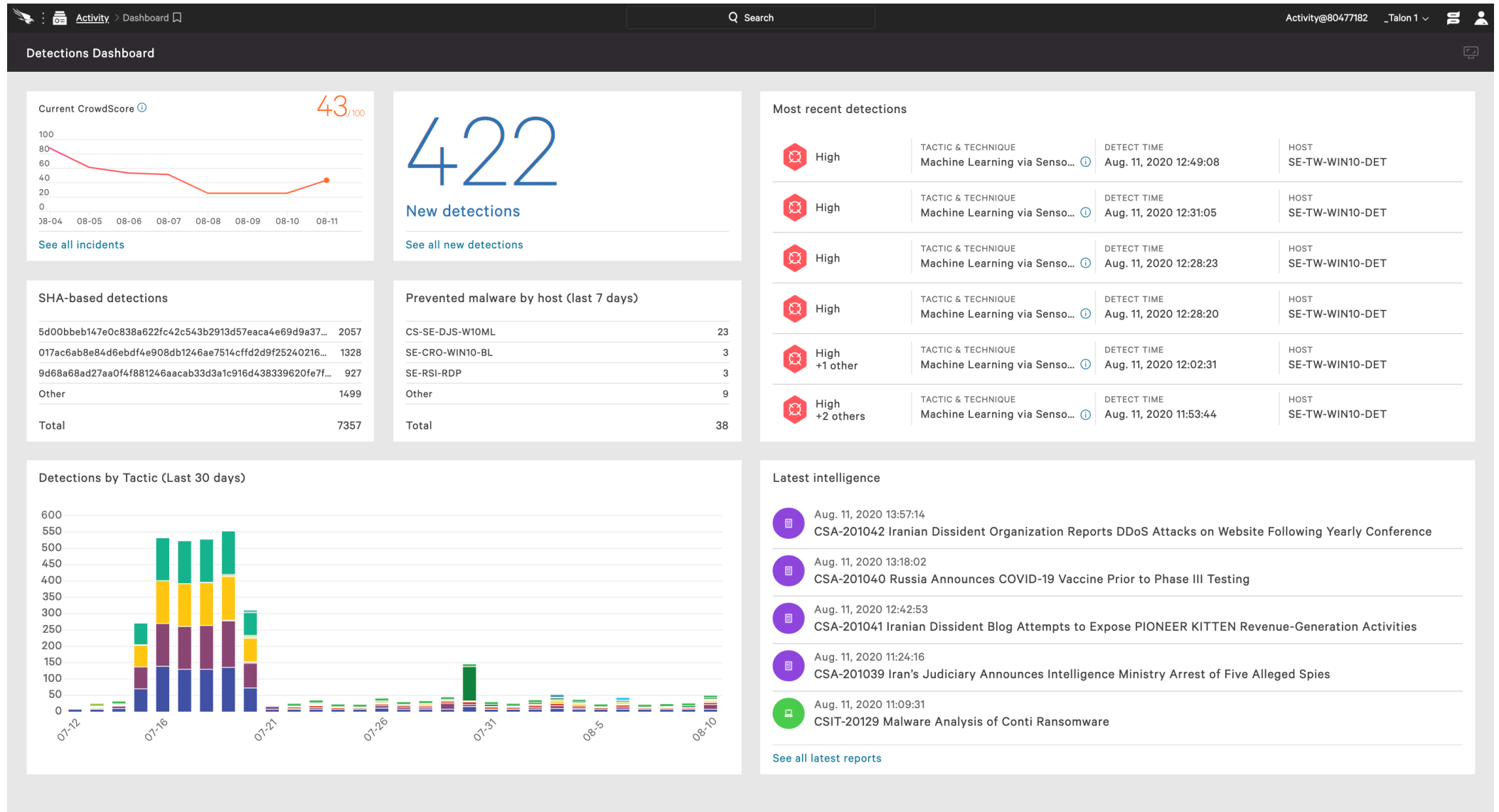
Ciclo de vida – Detección y reporte

Jornada
2022

¿Cómo detectar un incidente de seguridad? ¿Cuáles son las fuentes?

- Plataforma SIEM.
- Usuarios finales.
- Equipos de seguridad perimetral (Firewall, IPS, IDS, WAF, etc).
- Clientes.
- Sub-unidades de TIC.
- NOCs (Network Operation Center).
- Organizaciones de investigación.
- SOCs (Security Operation Center).
- Proveedores de servicio.
- CERTs externos o internacionales.
- Unidades de negocio o departamentos internos.
- Medios de comunicación.
- Sitios Web.

Ciclo de vida – Detección y reporte



422
New detections

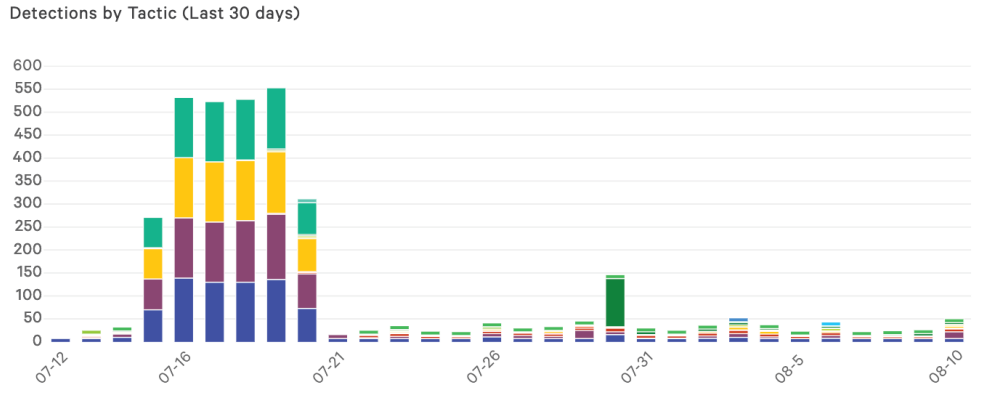
See all new detections

SHA-based detections

5d00bbeb147e0c838a622fc42c543b2913d57eaca4e69d9a37...	2057
017ac6ab8e84d6ebdf4e908db1246ae7514cfd2d9f25240216...	1328
9d68a68ad27aa0f4f881246aacab33d3a1c916d438339620fe7f...	927
Other	1499
Total	7357

Prevented malware by host (last 7 days)

CS-SE-DJS-W10ML	23
SE-CRO-WIN10-BL	3
SE-RSI-RDP	3
Other	9
Total	38



Most recent detections

High	TACTIC & TECHNIQUE Machine Learning via Senso...	DETECT TIME Aug. 11, 2020 12:49:08	HOST SE-TW-WIN10-DET
High	TACTIC & TECHNIQUE Machine Learning via Senso...	DETECT TIME Aug. 11, 2020 12:31:05	HOST SE-TW-WIN10-DET
High	TACTIC & TECHNIQUE Machine Learning via Senso...	DETECT TIME Aug. 11, 2020 12:28:23	HOST SE-TW-WIN10-DET
High	TACTIC & TECHNIQUE Machine Learning via Senso...	DETECT TIME Aug. 11, 2020 12:28:20	HOST SE-TW-WIN10-DET
High +1 other	TACTIC & TECHNIQUE Machine Learning via Senso...	DETECT TIME Aug. 11, 2020 12:02:31	HOST SE-TW-WIN10-DET
High +2 others	TACTIC & TECHNIQUE Machine Learning via Senso...	DETECT TIME Aug. 11, 2020 11:53:44	HOST SE-TW-WIN10-DET

- Latest intelligence
- Aug. 11, 2020 13:57:14
CSA-201042 Iranian Dissident Organization Reports DDoS Attacks on Website Following Yearly Conference
 - Aug. 11, 2020 13:18:02
CSA-201040 Russia Announces COVID-19 Vaccine Prior to Phase III Testing
 - Aug. 11, 2020 12:42:53
CSA-201041 Iranian Dissident Blog Attempts to Expose PIONEER KITTEN Revenue-Generation Activities
 - Aug. 11, 2020 11:24:16
CSA-201039 Iran's Judiciary Announces Intelligence Ministry Arrest of Five Alleged Spies
 - Aug. 11, 2020 11:09:31
CSIT-20129 Malware Analysis of Conti Ransomware
- See all latest reports

Ciclo de vida – Detección y reporte

Jornada
2022

Unsuccessful inbound RDP connection from

[REDACTED]

 Hunt for related events

Event info

Event	Unsuccessful inbound RDP connection from [REDACTED]
Event time	4/30/2022, 11:17:48.892 AM
Action type	InboundRdpConnection

Ciclo de vida – Detección y reporte

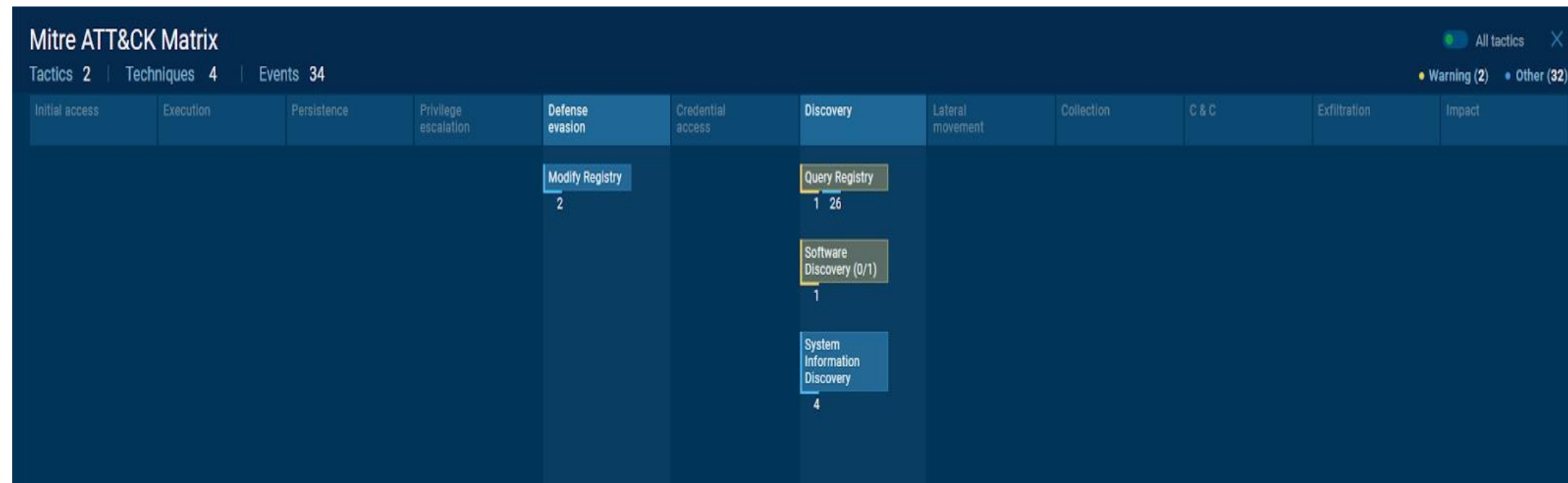
The screenshot shows an Internet Explorer browser window with the address bar displaying `http://js.mykings.top:280/helloworld.msi%20/q`. The main content area displays the error message "This page can't be displayed" with a list of troubleshooting steps: "Make sure the web address http://js.mykings.top:280 is correct.", "Look for the page with your search engine.", and "Refresh the page in a few minutes." Below the list is a button labeled "Fix connection problems".

Below the browser window, the Wireshark interface is visible, showing a list of network traffic events. The "Threats" tab is selected, displaying a list of detected threats. The table below summarizes the visible data:

Timeshift	Class	PID	Process name	Message
230 ms	A Network Trojan was detected	-	-	AV TROJAN Observed DNS Query to Suspicious Domain (js[.]mykings[.]top)
230 ms	Potentially Bad Traffic	-	-	ET DNS Query to a *.top domain - Likely Hostile
607 ms	A Network Trojan was detected	-	-	AV TROJAN Observed DNS Query to Suspicious Domain (js[.]mykings[.]top)
1215 ms	A Network Trojan was detected	-	-	AV TROJAN Observed DNS Query to Suspicious Domain (js[.]mykings[.]top)
1606 ms	A Network Trojan was detected	-	-	AV TROJAN Observed DNS Query to Suspicious Domain (js[.]mykings[.]top)
2215 ms	A Network Trojan was detected	-	-	AV TROJAN Observed DNS Query to Suspicious Domain (js[.]mykings[.]top)
2606 ms	A Network Trojan was detected	-	-	AV TROJAN Observed DNS Query to Suspicious Domain (js[.]mykings[.]top)
4215 ms	A Network Trojan was detected	-	-	AV TROJAN Observed DNS Query to Suspicious Domain (js[.]mykings[.]top)
4606 ms	A Network Trojan was detected	-	-	AV TROJAN Observed DNS Query to Suspicious Domain (js[.]mykings[.]top)
8606 ms	A Network Trojan was detected	-	-	AV TROJAN Observed DNS Query to Suspicious Domain (js[.]mykings[.]top)

Ciclo de vida – Detección y reporte

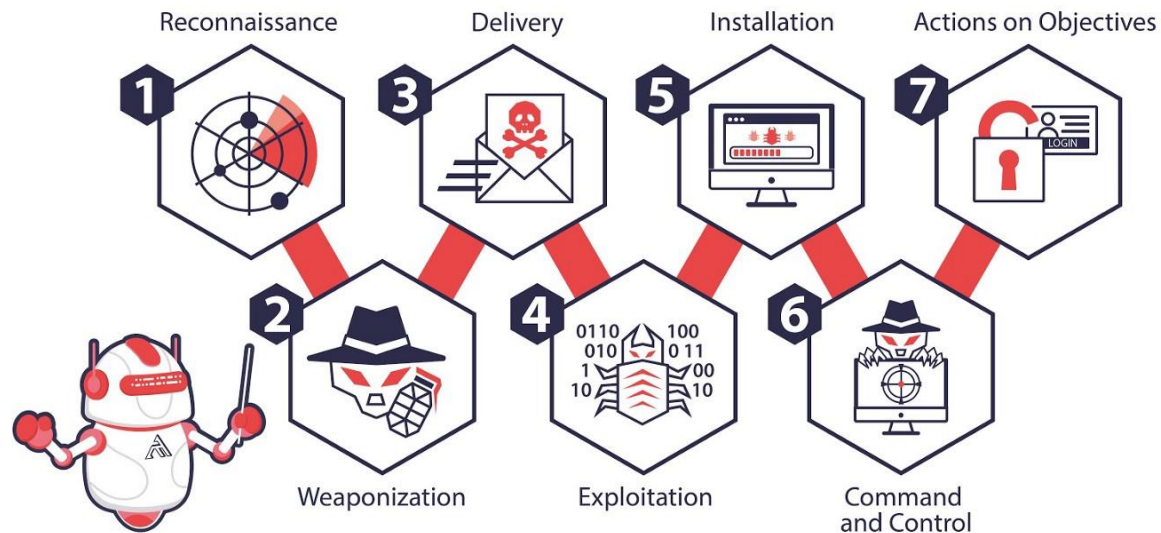
Jornada
2022



Ciclo de vida – Detección y reporte

Jornada
2022

THE CYBER KILL CHAIN



MITRE
ATT&CK™

Ciclo de vida – Detección y reporte

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Authentication Package	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	Bypass User Account Control	Component Firmware	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	DLL Search Order Hijacking	Component Object Model Hijacking	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Email Collection	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Dylib Hijacking	Control Panel Items	Hooking	Input Capture	Remote File Copy	Input Capture	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Dylib Hijacking	DCShadow	Input Prompt	Permission Groups Discovery	Remote Services	Man in the Browser	Screen Capture	Multi-hop Proxy
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Deobfuscate/Decode Files or Information	Kerberoasting	Process Discovery	Replication Through Removable Media	Video Capture	Standard Application Layer Protocol	Multi-Stage Channels
	Local Job Scheduling	Create Account	File System Permissions Weakness	Disabling Security Tools	Keychain	Query Registry	Shared Webroot		Standard Cryptographic Protocol	Multiband Communication
	LSASS Driver	DLL Search Order Hijacking	Hooking	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	Remote System Discovery	SSH Hijacking		Uncommonly Used Port	Multilayer Encryption
	Mshta	Dylib Hijacking	Image File Execution Options Injection	DLL Side-Loading	Network Sniffing	Security Software Discovery	Taint Shared Content		Web Service	Port Knocking
	PowerShell	External Remote Services	Launch Daemon	Exploitation for Defense Evasion	Password Filter DLL	System Information Discovery	Third-party Software			Remote Access Tools
	Regsvcs/Regasm	Image File Execution Options Injection	New Service	Extra Window Memory Injection	Private Keys	System Network Configuration Discovery	Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness	Path Interception	File Deletion	Replication Through Removable Media	System Network Connections Discovery	Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Plist Modification	File System Logical Offsets	Securityd Memory	System Owner/User Discovery				Standard Cryptographic Protocol
	Scheduled Task	Hooking	Port Monitors	Gatekeeper Bypass	Two-Factor Authentication Interception	System Service Discovery				Standard Non-Application Layer Protocol
	Scripting	Hypervisor	Process Injection	Hidden Files and Directories		System Time Discovery				Uncommonly Used Port
	Service Execution	Image File Execution Options Injection	Scheduled Task	Hidden Users						
	Signed Binary Proxy Execution	Image File Execution Options Injection	Service Registry Weakness	Hidden Window						
	Signed Script Proxy Execution	Kernel Modules and Extensions	Weakness	HISTCONTROL						
	Source	Launch Agent	Setuid and Setgid	Image File Execution Options Injection						
	Space after Filename	Launch Daemon	SID-History Injection	Indicator Blocking						
	Third-party Software	Launch Daemon	Indicator Blocking							
	Trap	Launchctl								
	Trusted Developer									

Ciclo de vida – Detección y reporte

Jornada
2022



Ciclo de vida – Detección y reporte

Jornada
2022

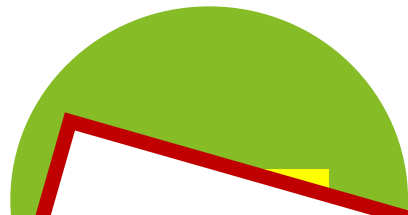
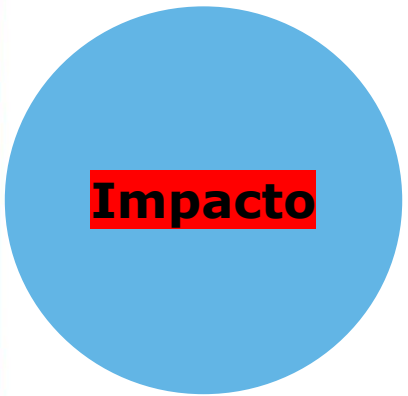
Para la mayoría de las organizaciones, el **mayor reto** en el proceso de respuesta a incidentes de seguridad es **detectar y evaluar los posibles incidentes**, así como determinar **lo que sea que haya pasado**, el tipo, la extensión y la magnitud del problema.

Ciclo de vida – Análisis y decisión

¿Cómo clasificar un Incidente?

Impacto

VS



Impacto			Urgencia		
Nivel	Descripción Cualitativa	Grado de Escala	Nivel	Descripción Cualitativa	Grado de Escala
Bajo	<ul style="list-style-type: none"> No representa mayor impacto en la operación de los servicios críticos del negocio. Afectación leve en el rendimiento de las aplicaciones críticas. Existen soluciones alternativas. El impacto es transparente para los clientes. No representa un impacto significativo sobre la operación del negocio, en función de la cantidad de usuarios afectados y del tipo de servicios. 	1	Leve	<ul style="list-style-type: none"> Representa la incorporación de ciertas mejoras a nivel de aplicación, automatización de procesos o nuevas configuraciones. Requiere de previa planificación. El incidente puede ser fácilmente controlado, aislado y resuelto. 	1
		2	Moderada	<ul style="list-style-type: none"> Requiere atención a fin de resolver problemas recurrentes o fallas detectadas. La atención debe ser planificada con anticipación y notificada a las unidades de negocio respectivas. El incidente se encuentra parcialmente controlado. 	2
		3		<ul style="list-style-type: none"> Requiere atención en el menor tiempo posible con el fin de prevenir un posible impacto en la operación del negocio. El incidente debe ser notificado a la Dirección Institucional. El incidente requiere esfuerzos significativos para ser controlado, aislado y resuelto. 	3
Muy Alto	<ul style="list-style-type: none"> Discontinúa la operación del negocio, afectando a un gran número de usuarios de manera altamente significativa. Afectación grave en el rendimiento de las aplicaciones críticas. Afecta a muchos clientes. Se requiere el involucramiento del equipo de respuesta a incidentes. 	4	Urgente	<ul style="list-style-type: none"> Requiere atención de manera inmediata a fin de prevenir un posible y severo impacto sobre la operación del negocio. El incidente debe ser presentado ante la Dirección Institucional y tratado de acuerdo con la 	4

Obsoleto

Mapa de Calor Cuantitativo

Urgencia	Valor	1	2	3	4
Urgente	4	4	8	12	16
Significativa	3	3	6	9	12
Moderada	2	2	4	6	8
Leve	1	1	2	3	4

Ciclo de vida – Análisis y decisión

Jornada
2022

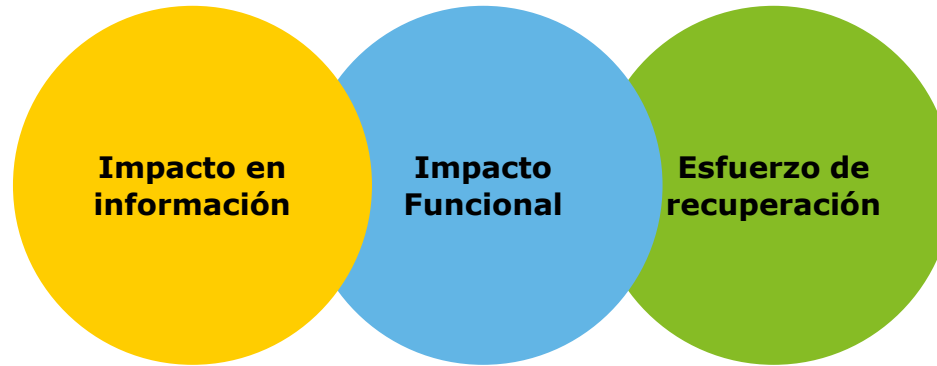
Triage

Se le conoce como el arte de clasificar, categorizar y priorizar eventos de seguridad; con el fin de determinar cuáles serán las acciones contención y respuesta a ejecutar.



Ciclo de vida – Análisis y decisión

Jornada
2022



Nivel	Valor Cuantitativo	Valor Cualitativo	Descripción
Ninguno	0		Sin efectos potenciales de acceso no autorizado, exfiltración, alteración, modificación,...

Nivel	Valor Cuantitativo	Valor Cualitativo	Descripción
Bajo	Ninguno	0	Sin efectos potenciales en la capacidad de entregar servicios críticos a los usuarios o clientes de la organización.
Medio	Bajo	1	Efecto potencial leve en la capacidad de entregar servicios críticos a los usuarios o clientes de la organización. La organización podría entregar los servicios críticos, pero con pérdida de eficiencia.
Alto	Medio	2	Efecto potencial moderado en la capacidad de entregar servicios críticos a los usuarios o clientes de la organización. La organización podría perder la capacidad de entregar servicios críticos a un sub-conjunto de usuarios o por un lapso determinado de tiempo.
Irrecuperable	Alto	3	Efecto potencial severo en la capacidad de entregar servicios críticos a los usuarios o clientes de la organización. La organización podría perder la capacidad de entregar servicios críticos a un sub-conjunto de usuarios o por un lapso determinado de tiempo.

Nivel	Valor Cuantitativo	Valor Cualitativo	Descripción
Irrecuperable	Ninguno	0	No requiere ningún esfuerzo.
	Regular	1	El tiempo para la recuperación es predecible con los recursos existentes.
	Adicional	2	El tiempo de recuperación es predecible con recursos adicionales a los actuales.
	Extendido	3	El tiempo de recuperación es impredecible, recursos adicionales y apoyo externo podrían ser necesario.



Ciclo de vida – Ejercicio grupal

Jornada
2022

Durante las últimas 24 horas, muchos empleados han llamado a la mesa de soporte de seguridad para consultar sobre la validez de un correo que recibieron proveniente de “SkyFinancial S.A”.

El correo indica que se dio una posible filtración de datos financieros y que se requiere acceder a sitio web mediante un link para crear una nueva contraseña, después de proveer su contraseña actual para validar la identidad del usuario y los datos de la cuenta.

- 1- ¿Indique cuál activo de información se vio afectado?**
- 2- ¿Indique cuál fue una posible vulnerabilidad explotada?**
- 3- Clasifique, categorice y priorice el caso.**
- 4- ¿Indique qué impacto potencial tuvo este incidente?**

Ciclo de vida – Contención y erradicación

Jornada
2022

El objetivo principal de esta fase es **limitar el alcance y la magnitud del incidente**, es decir, evitar que el incidente se expanda y empeore.

No es posible erradicar un problema de seguridad que ha comprometido la organización si no se conoce qué pasó.

Ciclo de vida – Contención y erradicación Jornada 2022



Contención

- Respuesta inmediata para minimizar el impacto.
- Vigilancia al atacante o incidente.
- Preservación de la evidencia.
- Mantener la cadena de custodia (De ser necesario).
- Identificar la fuente del incidente (No al atacante).



Erradicación

- Aplicar estrategias y protocolos de erradicación.
- Escalamiento.
- Eliminar rastro del incidente.
- Activar el DRP o BCP (De ser necesario).
- Comunicación interna/externa.

“El enfoque principal al responder ante un incidente debería ser la minimización de impactos adversos al negocio, mientras que la identificación del atacante debería ser considerada como un **objetivo secundario**”.



Ciclo de vida – Contención y erradicación

Jornada
2022



Restablecer
Respaldos



Cambio
masivo de
contraseñas



Aislar equipos
infectados

Ciclo de vida – Ejercicio grupal

Jornada
2022

Su servidor “Core financiero” fue comprometido, su archivo de contraseñas, dirección IP y la información del sistema operativo podría haber sido compartida en un foro de ciber-delincuentes en la Dark Web. Su servidor ha sido repetidamente atacado durante las siguientes 2 semanas y se han detectado comportamientos sospechosos en su red.

- 1- ¿Indique cómo contendría el ataque?**
- 2- ¿Indique cómo mejoraría sus defensas?**
- 3- ¿Indique su proceder para determinar la causa?**
- 4- ¿Indique su proceder para erradicar la causa?**

Ciclo de vida – Recuperación

Jornada
2022



Ciclo de vida – Lecciones aprendidas

Jornada
2022

La documentación de lecciones aprendidas permite:

- Determinar exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.
- Mantener los documentados los procedimientos realizados.
- Determinar si se tomaron medidas o acciones que podrían haber impedido la recuperación.
- Identificar que debería hacerse la próxima vez que ocurra un incidente similar.
- Determinar acciones correctivas que pueden prevenir incidentes similares en el futuro.
- Identificar herramientas, recursos o mejoras al proceso que son necesarias para detectar, analizar y mitigar los incidentes en el futuro.

Palabras de clausura

Jornada
2022

01

El monitoreo de red es la peor pesadilla de un atacante, prepárese cada segundo cuenta

02

Una buena seguridad tiene que ver con la resiliencia, no con ser a prueba de balas

03

Habilitar la preservación de la evidencia en todas sus herramientas le ahorrará mucho tiempo a su organización

Palabras de clausura

Jornada
2022

04

Conozca a su adversario para detener los ataques modernos

05

Elimine las configuraciones erróneas y deshabilite los servicios no seguros

06

Construir una cultura de ciberseguridad