Cazando al Cazador, más allá del SIEM

Septiembre 2023

Jorge López Franco
Country Manager – México, Stellar Cyber

Estrategias de Ciberseguridad

Fecha Modificación 11/03/2021 12:23:06

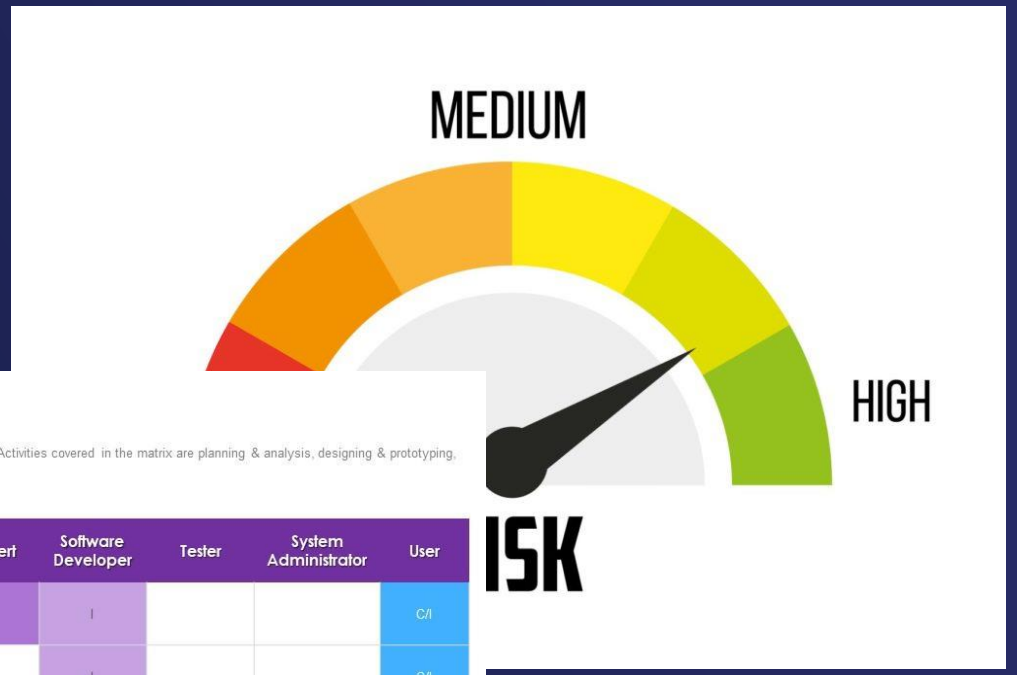
Impactos en el Negocio

Tabla de Impactos

Impacto / Tiempo	1.00 horas	4.00 horas	8.00 horas	24.00 horas	2.00 dias	1.00 semanas	2.00 semanas	3.00 semanas	4.00 semanas	Criticidad
	Muy Bajo	Muy Bajo	Medio	Medio	Alto	Muy alto	Muy alto	Muy alto	Muy alto	5
Impacto económico. Pérdida de beneficios (%)	Muy Bajo	Muy Bajo	Bajo	Bajo	Alto	Alto	Alto	Alto	Alto	26
Impacto económico. Incremento de costes y/o gastos (%)	Muy Bajo	Muy Bajo	Medio	Medio	Alto	Alto	Alto	Muy alto	Muy alto	29
Impacto comercial	Muy Bajo	Muy Bajo	Medio	Medio						
Impacto operacional	Muy Bajo	Bajo	Bajo	Bajo						
Impacto reputacional	Muy Bajo	Bajo	Bajo	Bajo						
Impacto legal (Incumplimiento de	Muy Bajo	Bajo	Medio	Medio						

RTO MT

BIA



RASCI Matrix for Assigning Responsibilities

Mentioned slide illustrates RASCI matrix that can be used for assigning responsibilities to implement ISMS process successfully. Activities covered in the matrix are planning & analysis, designing & prototyping, coding, testing, deployment and maintenance.

Activities	Analyst	UI/UX	Project Manager	IT Expert	Software Developer	Tester	System Administrator	User
Planning and Analysis	R		A	C	I			C/I
Designing and Prototyping	S	R	A		I			C/I
Coding			A		R	S/I	I	I
Review and Testing			A			R	I	C/I
Development			A		S	S	R	I
Maintenance		S	A		S	S	R	C/I

Note: - RASCI Stands for Responsible, Accountable, Support, Consulted and Informed

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

STELLAR CYBER®


STELLAR
CYBER®
¡Listo! Ya tenemos la ciberseguridad garantizada.
¿Entonces por qué sigue habiendo tantos ciberataques exitosos?

RETO ACTUAL: MUCHA INFORMACIÓN

1.5 millones de logs en 1 día

(aprox. 1500 usuarios)

STELLAR CYBER®

SITUACIÓN ACTUAL: **MUCHAS** TECNOLOGÍAS

STELLAR CYBER®

SITUACIÓN ACTUAL: LAS SECOPS NO ESTÁN CONFORMES

LA MITAD DE LAS ORGANIZACIONES CREEN QUE LAS SECOPS SE ESTÁN VOLVIENDO MÁS DIFÍCILES **

El panorama de amenazas está creciendo y cambiando rápidamente

41%

La superficie de ataque ha crecido

40%

La superficie de ataque está cambiando y evolucionando constantemente

39%

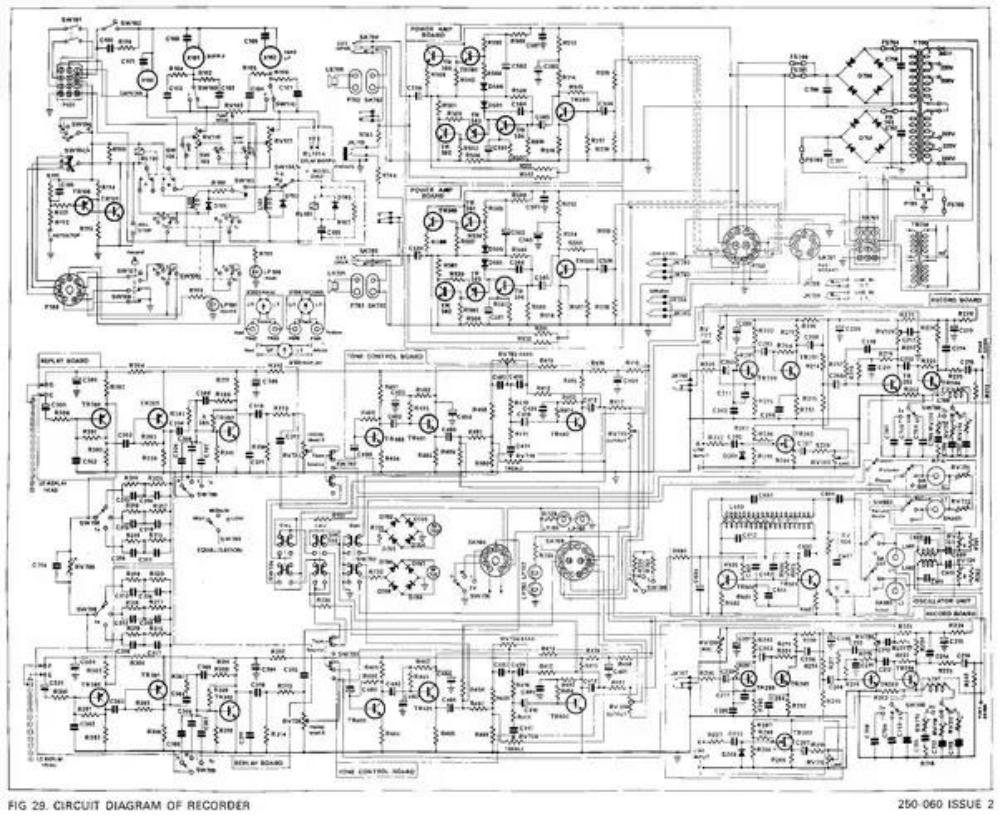
El volumen y la complejidad de las alertas de seguridad ha incrementado

37%

* Resultado modificado de la guía de mercado XDR de Gartner
** Del studio de ESG en el 2022 “SOC Modernization and the Role of XDR”

STELLAR CYBER®

Reconstruyendo un incidente (La manera tradicional)



Logs en crudo

Incidente de seguridad

STELLAR CYBER®

¿QUÉ ES UN SIEM?

SECURITY INFORMATION AND EVENT MANAGEMENT

Necesidades del cliente de:

- Detectar ataques y brechas de seguridad
- **Recolectar**
- Almacenar
- **Investigar** y
- Reportar

Unifica información desde:

- Dispositivos de seguridad
- Infraestructura de red
- Sistemas y
- Aplicaciones

También puede procesar telémetría de red

Los datos de eventos se contextualizan con información de:

- Usuarios
- Activos
- Amenazas y
- Vulnerabilidades

https://www.gartner.com/reviews/market/security-information-event-management

STELLAR CYBER®

¿QUÉ ES OPEN XDR?

EXTENDED DETECTION AND RESPONSE

En comparación a las tecnologías basadas en silos, automáticamente recolecta y correlaciona información de **múltiples fuentes de información**.

Pueden mejorar la operación de seguridad al:

- Compartir información de inteligencia de amenazas inmediatamente entre los distintos componentes
- **Combinar señales débiles para lograr señales más fuertes**
- Integrar sólo la información más importante para un triage más rápido y efectivo

Puede mejorar el staff de seguridad al:

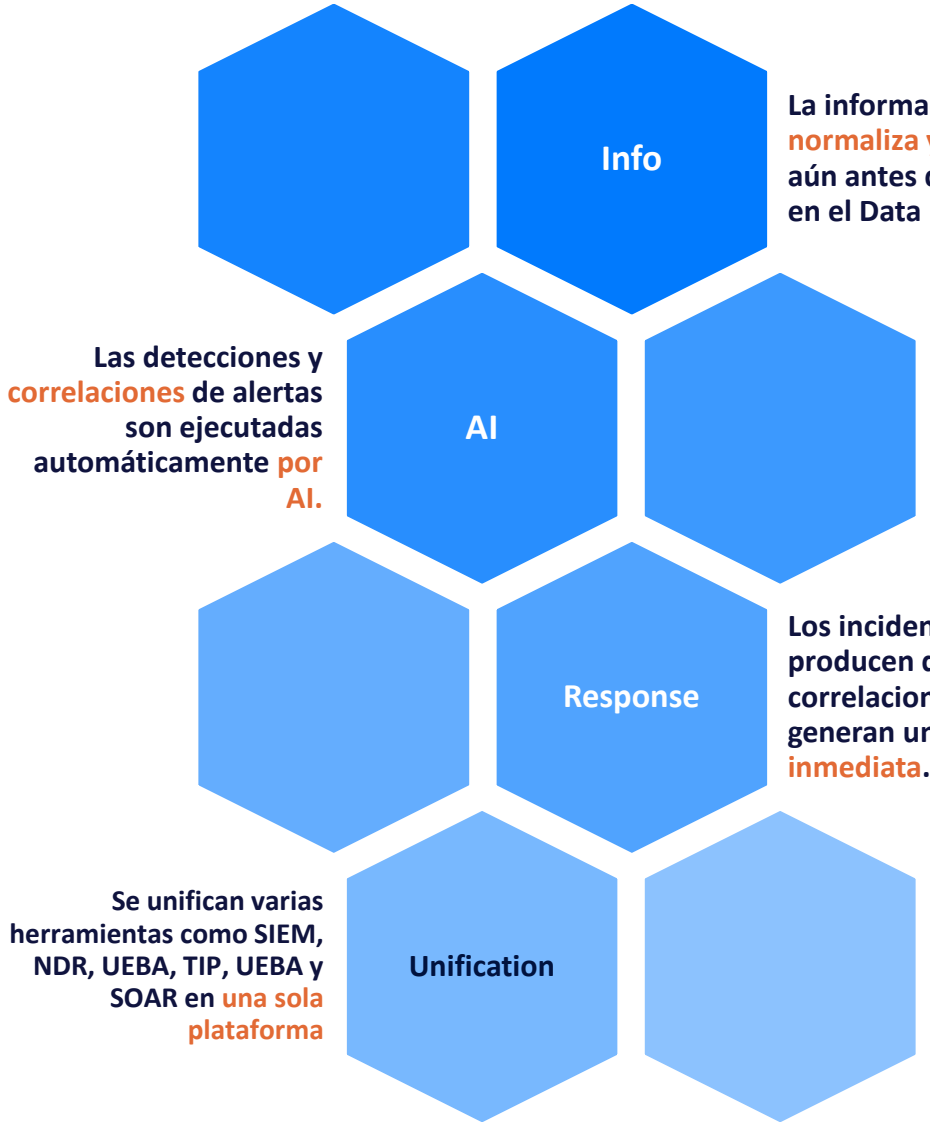
- **Condensar un gran número de alertas en incidentes**, que se pueden analizar más fácilmente
- **Integrar respuesta** a incidentes dentro de la misma consola
- Reducir tiempos de entrenamiento y habilidades del personal

https://www.gartner.com/doc/reprints?id=1-280DQ0LU&ct=211110&st=sb
Documento: “Emerging technologies: defining composable security” Gartner, Abril 2021

STELLAR CYBER®

BENEFICIOS DE OPEN XDR POR ARQUITECTURA

SIMPLIFICA LA COMPLEJIDAD DE LAS OPERACIONES DE SEGURIDAD



La información se normaliza y enriquece aún antes de guardarse en el Data Lake.

Las detecciones y correlaciones de alertas son ejecutadas automáticamente por AI.

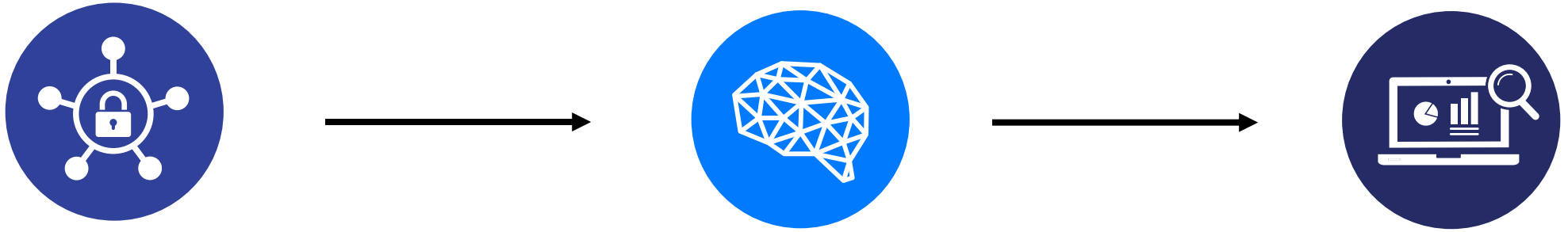
Los incidentes se producen de alertas correlacionadas que generan una respuesta inmediata.

Se unifican varias herramientas como SIEM, NDR, UEBA, TIP, UEBA y SOAR en una sola plataforma

STELLAR CYBER

BENEFICIOS DE OPEN XDR POR FUNCIÓN

SIMPLIFICA LA COMPLEJIDAD DE LAS OPERACIONES DE SEGURIDAD



Conectar facilmente todas las herramientas existentes en la plataforma de Open XDR

Identificar y **Correlacionar Automaticamente** las amenazas usando análisis inteligente de información

Automatizar Respuestas y tomar acciones definitivas rápidamente

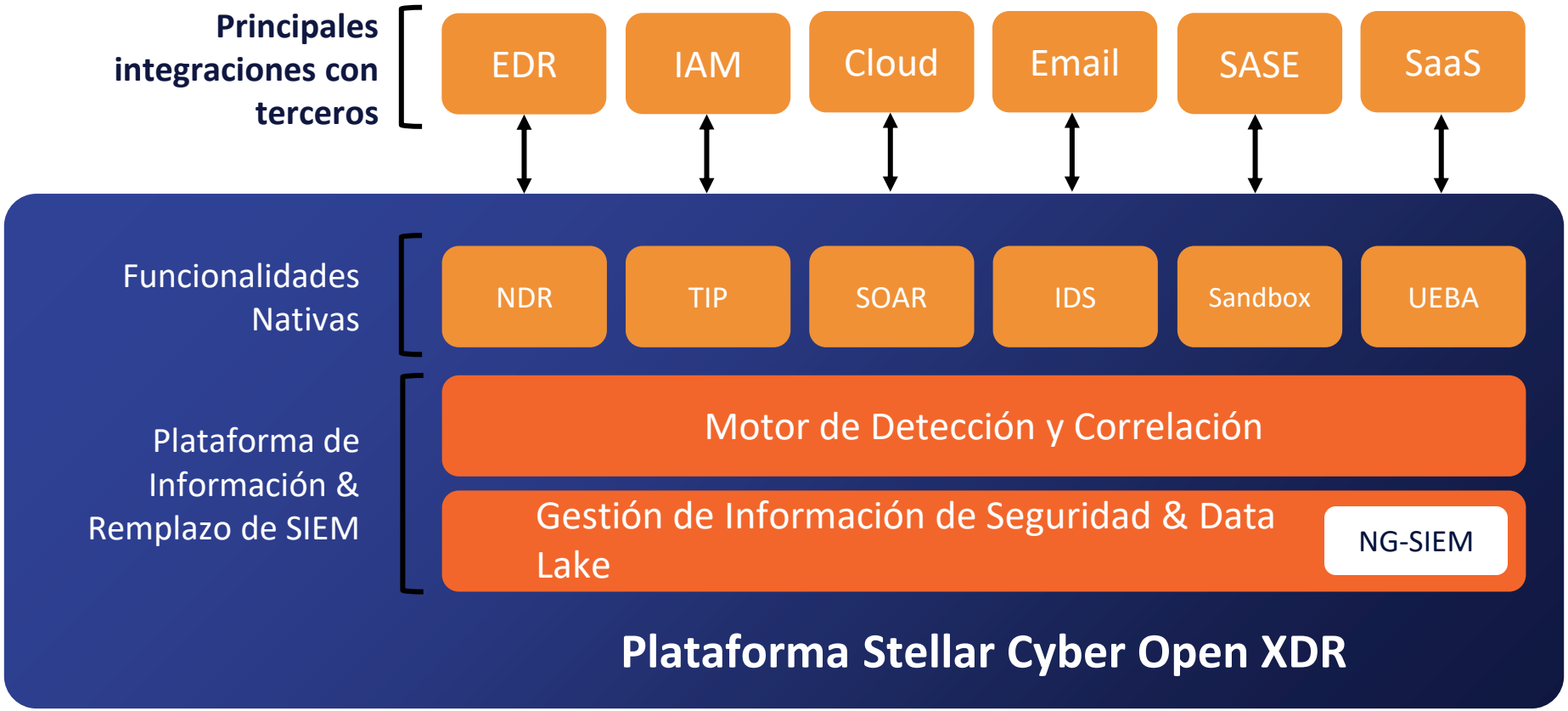
Plataforma Stellar Cyber Open XDR Principios

Automatizada

Simplificada

Unificada

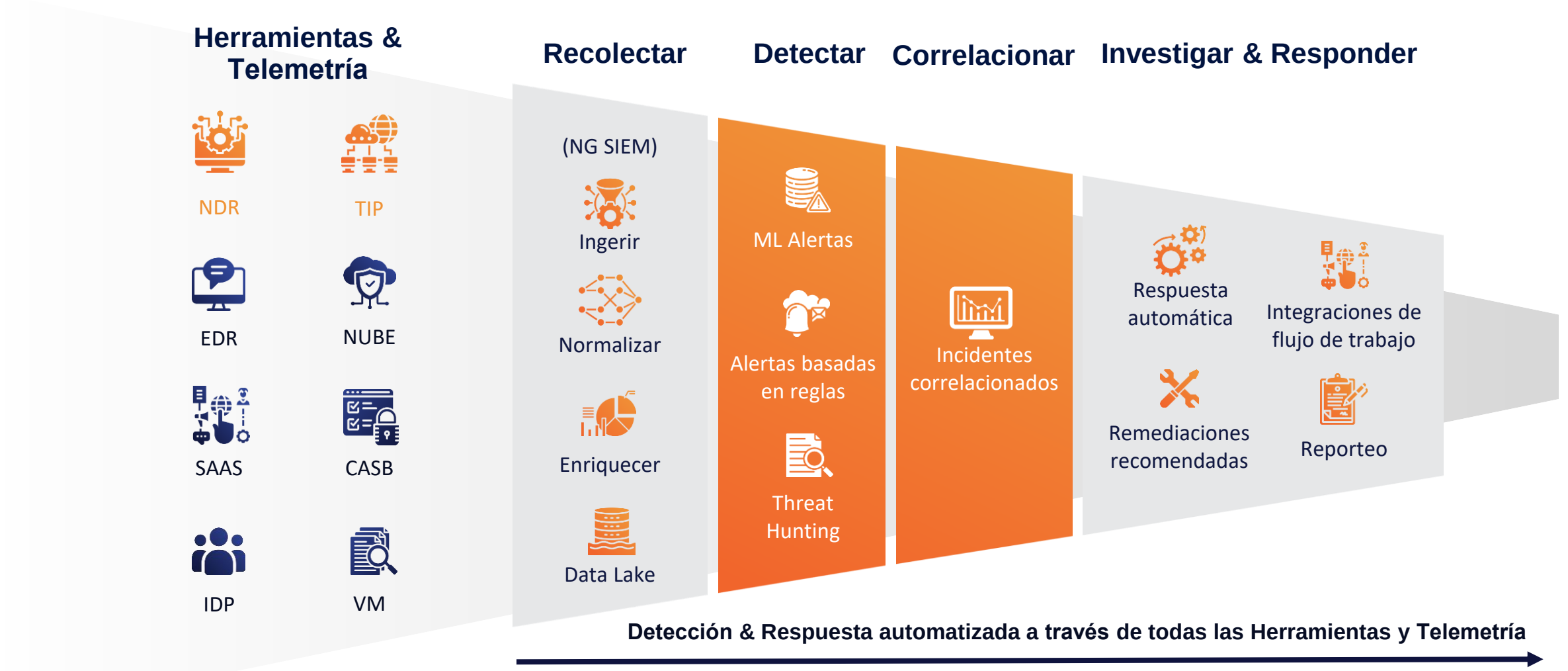
Abierta



STELLAR CYBER®

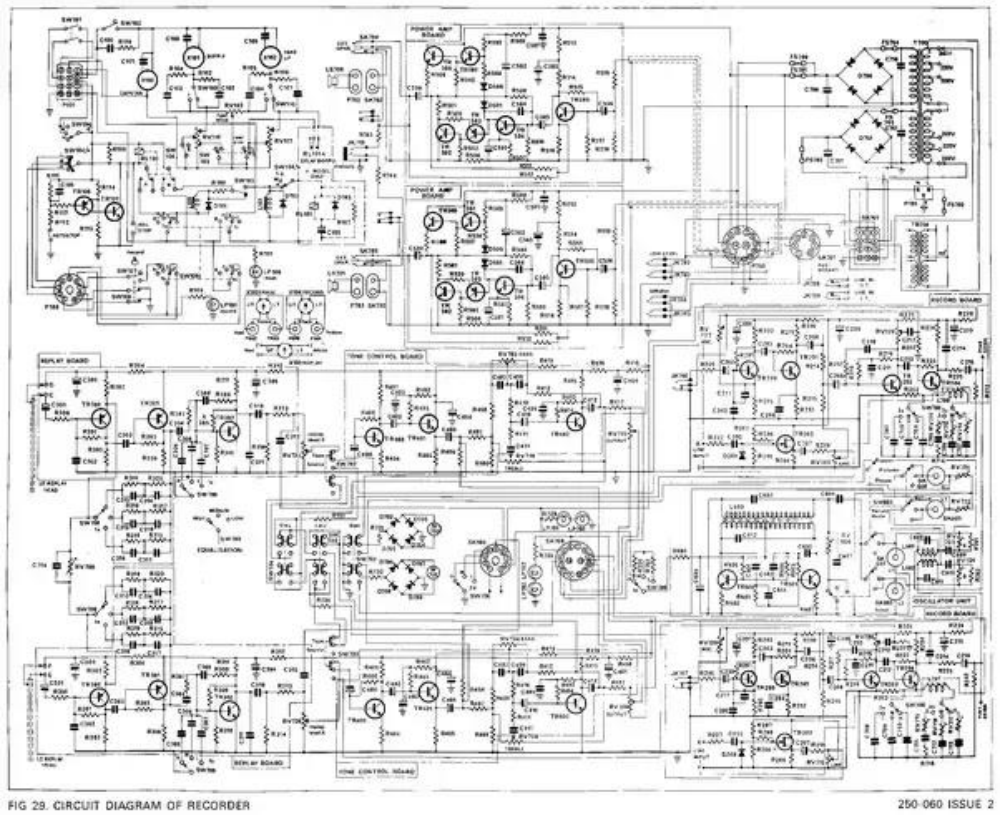
Una Plataforma y Una Licencia para Operaciones de Seguridad

Componentes Nativos en la Plataforma de Stellar Cyber's Open XDR



STELLAR CYBER®

Reconstruyendo un incidente (La manera tradicional)



Logs en crudo

Incidente de seguridad

STELLAR CYBER®

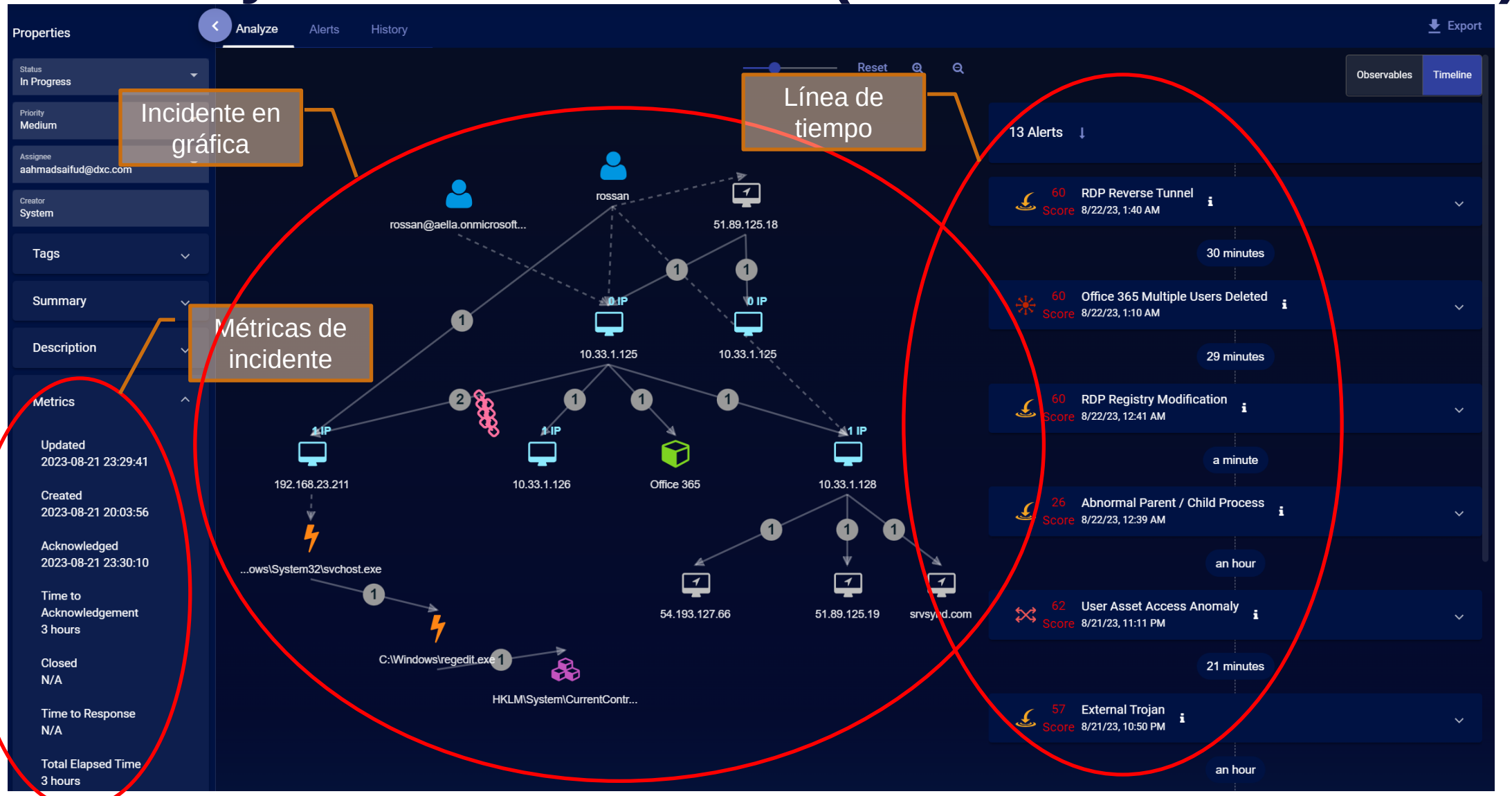
Reconstruyendo un incidente (La manera tradicional)

Alert Type	Total	Critical ↓	Stage	Tactic	Tags	
CylancePROTECT: Command and Scripting Interpreter	28,984	28,984	Persistent Foothold	Execution	CylancePROTECT	View
Command Anomaly	11,966	11,966	Persistent Foothold	Execution		View
CylancePROTECT: Process Injection	2,714	2,714	Propagation	Privilege Escalation	CylancePROTECT	View
CylancePROTECT: Exploitation for Privilege Escalation	302	302	Propagation	Privilege Escalation	CylancePROTECT	View
CylancePROTECT: OS Credential Dumping	117	117	Propagation	Internal Credential Access	CylancePROTECT	View
Outbound to TorNode	55	55	Exfiltration & Impact	Exfiltration	Custom	View
Command & Control Reputation Anomaly	32	31	Persistent Foothold	XDR Intel	Network Traffic Analysis	View
Exploited C&C Connection	31	31	Initial Attempts	External XDR NBA	Network Traffic Analysis	View
Internal Exploited Vulnerability	31	31	Exploration	Internal XDR NBA	Internal, Network Traffic A...	View
Private to Private Exploit Anomaly	5	3	Propagation	Lateral Movement	Internal, Network Traffic A...	View
Google Workspace User Suspended	3	3	Initial Attempts	External XDR UBA	External	View
Mimikatz Credential Dump	2	2	Propagation	Internal Credential Access	Internal	View
External Brute-Forced Successful User Login	2	2	Initial Attempts	External Credential Access	External	View
Google Workspace Alert: XDR Anomaly	13	1	Propagation	Internal XDR UBA	Google Workspace Alert	View
Mimikatz DCSync	1	1	Propagation	Internal Credential Access	Internal, Active Directory	View
Google Workspace Alert: Phishing	1	1	Initial Attempts	Initial Access	Google Workspace Alert	View
CrowdStrike: Command and Scripting Interpreter	1	1	Persistent Foothold	Execution		View

Logs en crudo

STELLAR CYBER®

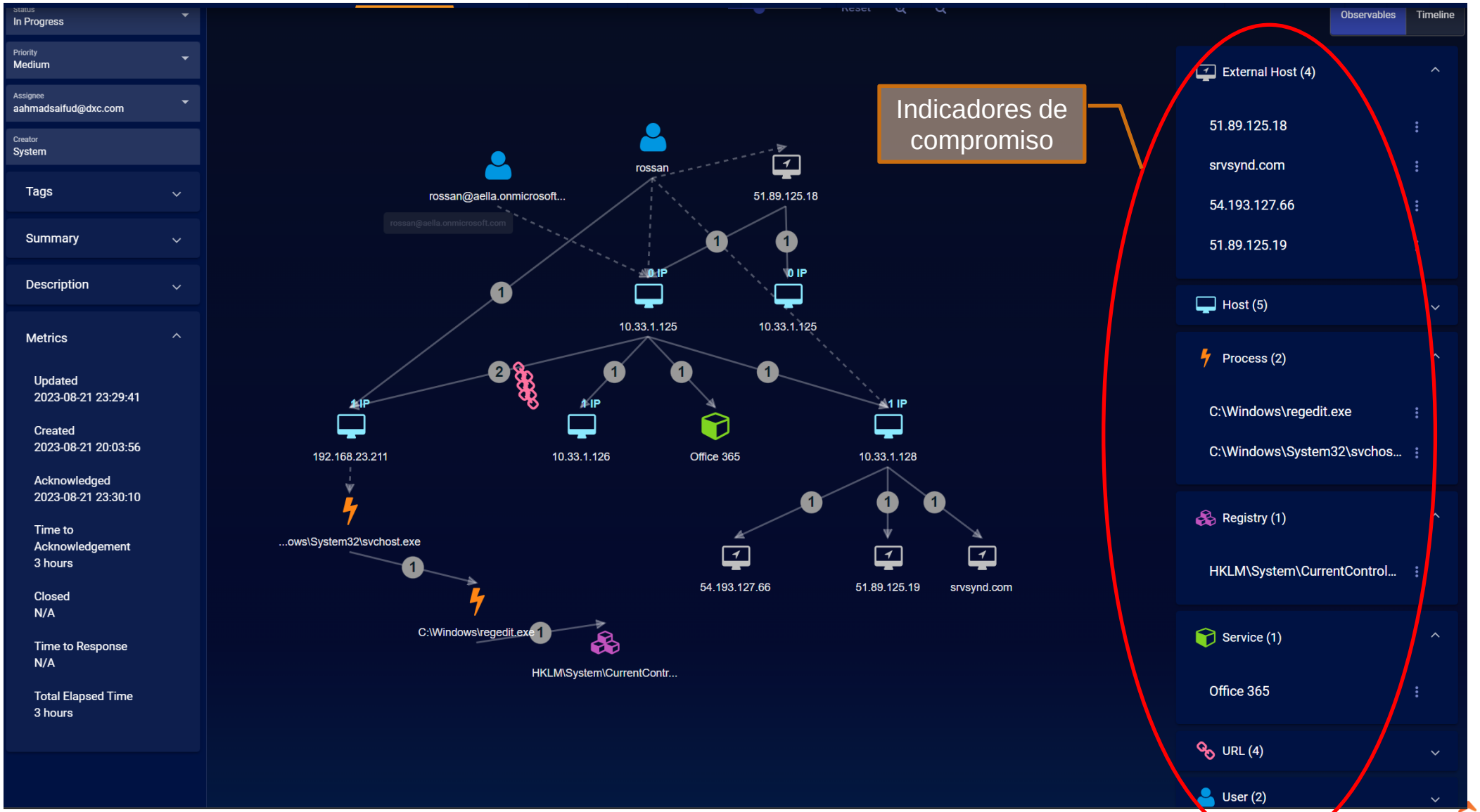
Reconstruyendo un incidente (La manera tradicional)



Incidente de seguridad

STELLAR CYBER®

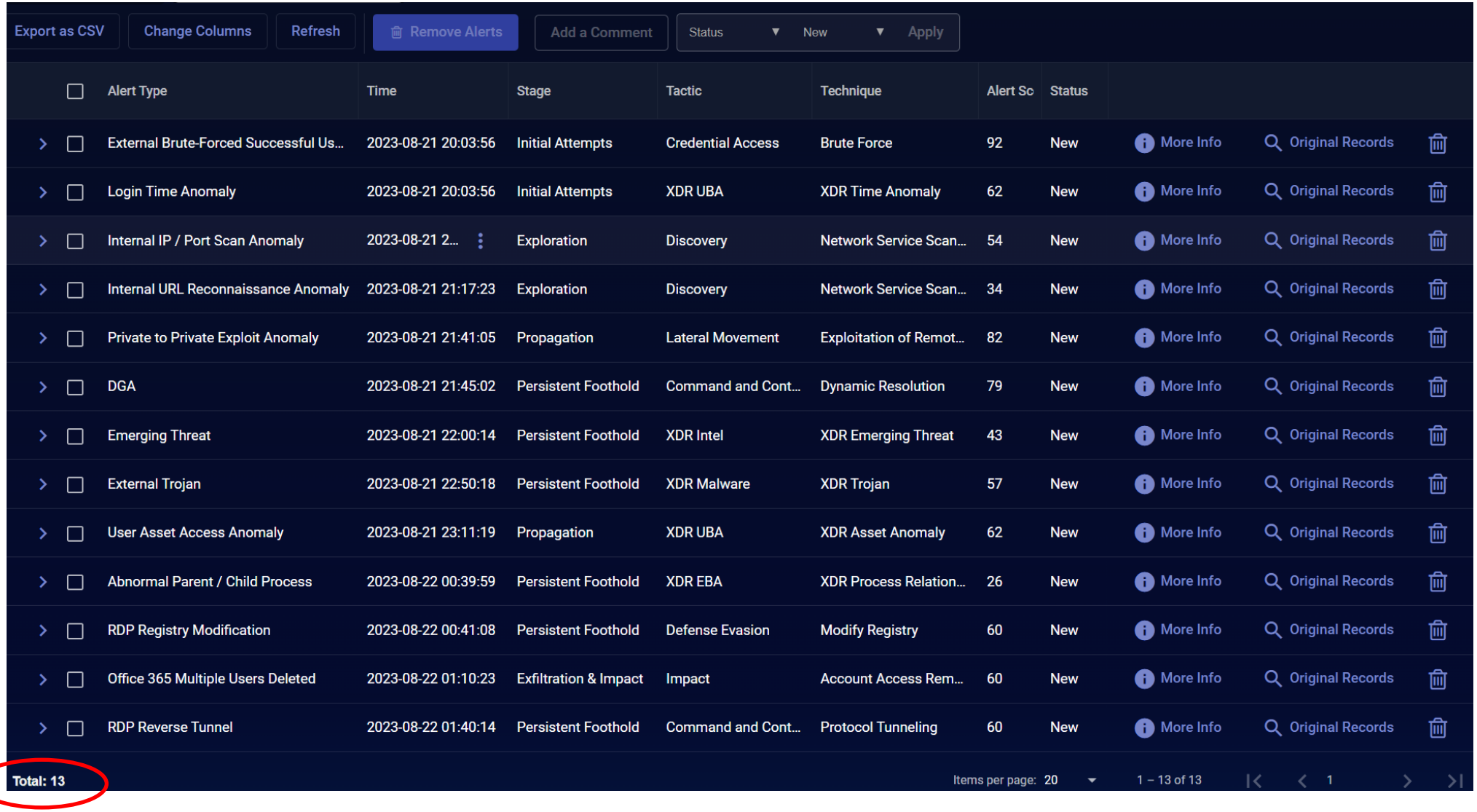
Reconstruyendo un incidente (La manera tradicional)



Incidente de seguridad

STELLAR CYBER®

Reconstruyendo un incidente (La manera tradicional)



Incidente de seguridad

STELLAR CYBER®

Stellar Cyber Open XDR – Ventajas únicas

Multinivel y multiusuario.	**Licencia única:** TODAS las funciones incluidas.	**Plataforma única:** unificada y automatizada
Detecciones y correlación **automatizadas**	**Las integraciones** más completas del mercado	Nube pública, local (HW o virtual) o **SaaS**
Plataforma abierta: más de 500 integraciones existentes	**Fácil** de implementar, fácil de usar	Sistema de **aprendizaje** personalizado (LMS)

STELLAR CYBER®

Stellar Cyber Empodera las Operaciones de Seguridad

- Equipo Global, con una base de clientes y partners
- Alrededor de ~7000 clientes globalmente
- Alianzas con tecnologías líderes en el mercado

Enfoque abierto garantizando inversiones

Gartner

Stellar Cyber se destaca en proyectos XDR

OMDIA
Brought to you by Informa Tech

Stellar Cyber mejora la eficacia, la eficiencia y la productividad del SOC

ESG
Enterprise Strategy Group

Stellar Cyber es seleccionada como una de las 20 mejores plataformas de análisis de seguridad

FORRESTER®

Stellar Cyber ofrece protección generalizada con su plataforma XDR

451 Research®

Las 10 Empresas de Seguridad más Calientes de XDR que debes seguir

THE CHANNEL CO.
CRN

Solución de XDR más innovador 2023

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2023

Ganador de Cloud Security 2022

TMC Cloud Computing EXCELLENCE AWARD 2022

Premio Baby Black Unicorn 2022

BABY BLACK UNICORN AWARDS 2022 FINALIST

Editor's Choice XDR 2022

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2022

Mejor solución de Ciberseguridad 2022

Líder de Mercado Nube Futuriom 40 2022

2022 FUTURIOM 40 CLOUD MARKET LEADER

STELLAR CYBER®

Clientes Enterprise

Enterprise

EBSCO
FUJISOFT
RCO
HANNEL
SK networks
ELIZONDO
ansa McAL
suva
malath
ICASA
GFI
exabytes
viettel
ORTIGAS REAL ESTATE.com

Servicios Financieros

CredAvenue
BRI
CoopBank
MIRAE ASSET
CREDICOMER
enfusion
LOTTE CARD
exela Banking Services
UBA
Superintendencia de Bancos Guatemala, C. A.
AGRIBANK

Educación

University of Zurich
Juilliard
University of Northern Colorado
Boise State University
University of Crete
University of San Francisco
The University of Chicago
Universiti Malaya
University of Denver
Universidad de Guadalajara
BMCC
Bend Lapine Schools

Gobierno

TM Telekom Malaysia
California Department of Aging
BMKG
BUNDESPOLIZEI
CNR Centro Nacional de Registros
KAC
HDN Handreamnet
BRUGG
NSSF
SITA
대한민국국회
djp
KEMENTERIAN KESEHATAN REPUBLIK INDONESIA
Grupo Aeroportuario del Pacífico
DICT

Manufactura

gepp
KRAKATAU STEEL
SL
Plastipak
STRÜBY
ARTHUR WEBER
ARCACONTINENTAL
SUMITOMO CHEMICAL
UNITED GRINDING
a·dec
Makita USA
5-hour ENERGY
DENSO
Southland

Servicios

EVNGENCO 3
California
NGCP
K water
VEOLIA
HPS
Ranhill

STELLAR CYBER®

STELLAR CYBER®

¡GRACIAS!

Para preguntas, por favor mande un correo a jlopez@stellarcyber.ai

es.stellarcyber.ai >>