XDR + SIEM +SOC

- Tecnologías en Islas, analistas L1,L2 y L3 lidiando con el ruido y la fatiga de alerta.
- Tecnologías fuera del alcance de la mayoría de las organizaciones debido al alto Capex y Opex.

LATAM CyberSOC

- DETECCIÓN proactiva de amenazas y CONTENCIÓN automática.
- La Mejor EFICACIA, EFICIENCIA Y ROI.

CYBERSOC

EM | Tecnología

Un hacker roba en un casino colándose a través de una pecera

B.T. 17 ABR. 2018 | 04:11

1 Ver comentario →

CYBERSOC

Mi cuenta

Productos Renovar Descargas Soporte Centro de recursos Blog

APT

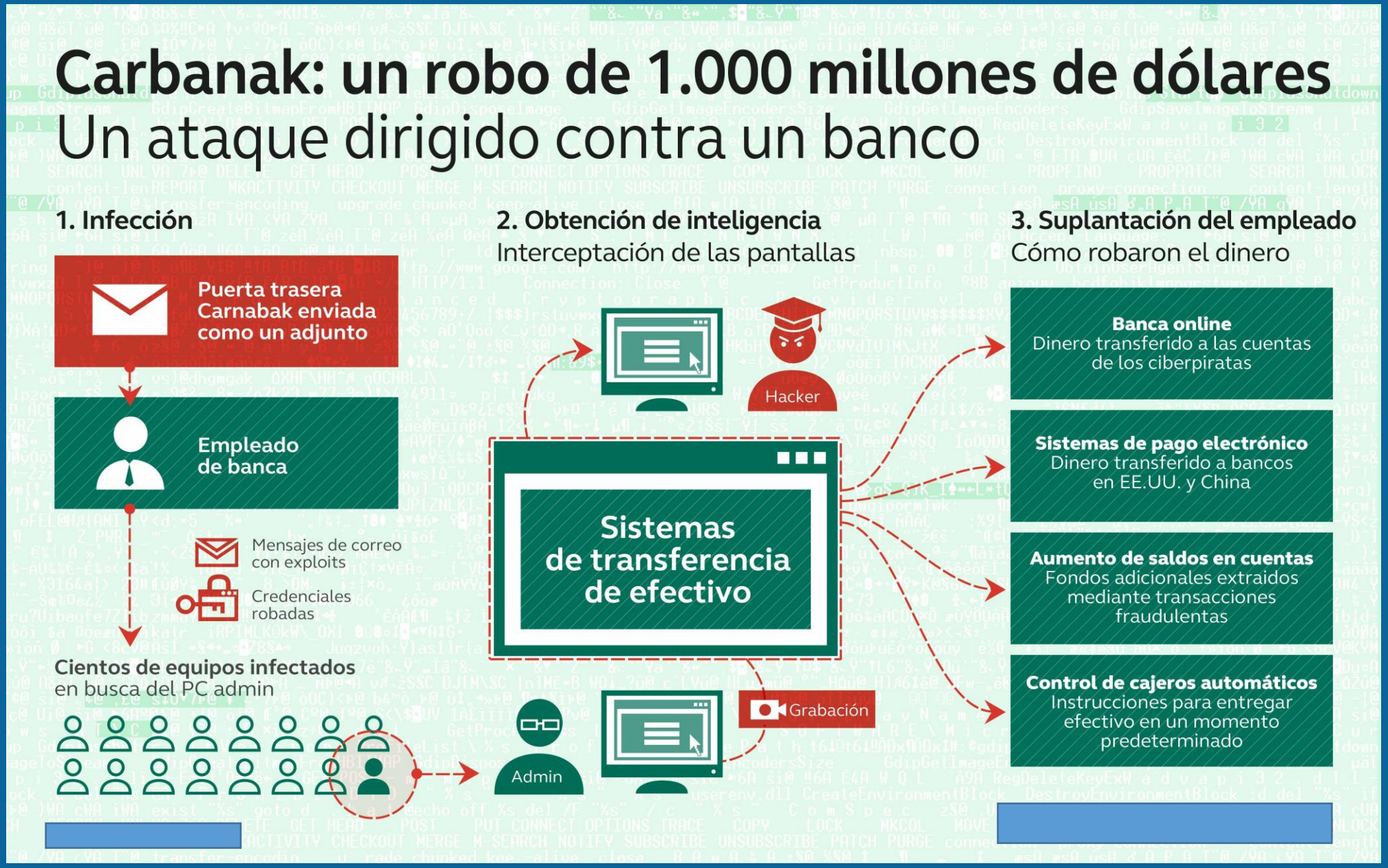
Buscar publicaciones del t

El mayor atraco del siglo: los ciberdelincuentes roban mil millones de dólares

El grupo Carbank robó en total 1 billón de dólares de docenas de bancos de todo el mundo.

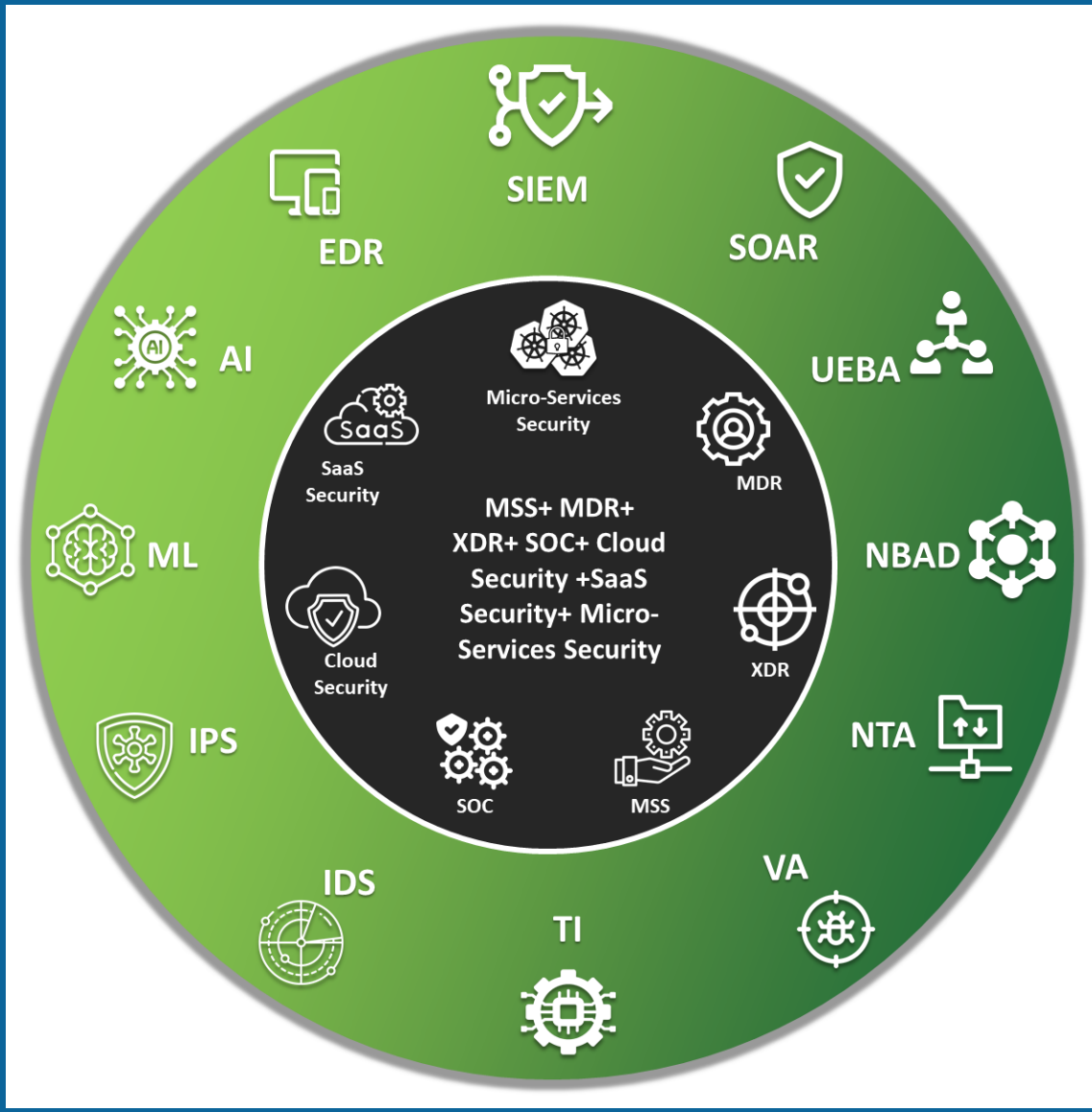
Alex Drozhzhin 16 Feb 2015

CYBERSOC

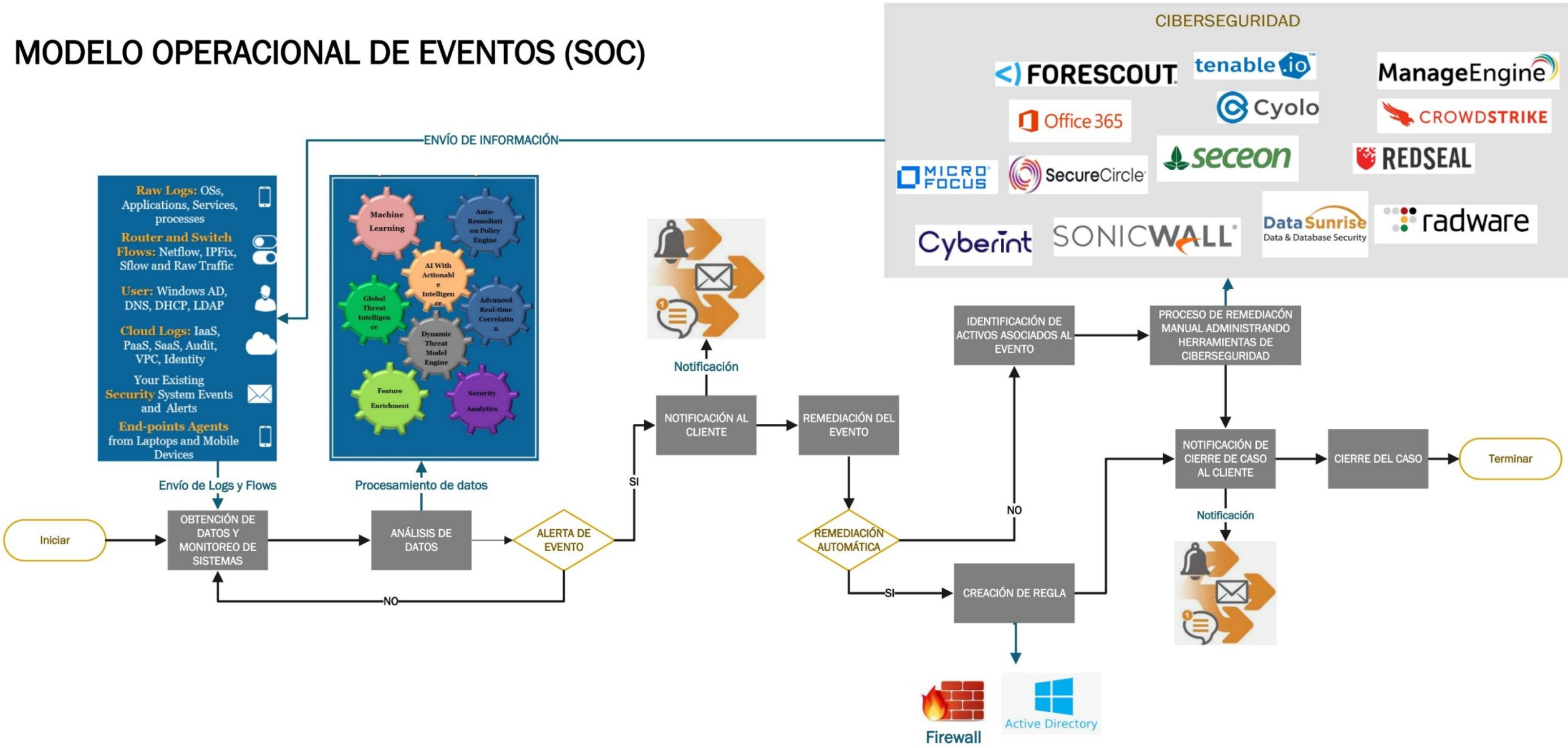

Carbanak: un robo de 1.000 millones de dólares
Un ataque dirigido contra un banco
1. Infección
Puerta trasera Carnabak enviada como un adjunto
Empleado de banca
Mensajes de correo con exploits
Credenciales robadas
Cientos de equipos infectados
en busca del PC admin
2. Obtención de inteligencia
Interceptación de las pantallas
Hacker
Sistemas de transferencia de efectivo
Admin
Grabación
3. Suplantación del empleado
Cómo robaron el dinero
Banca online
Dinero transferido a las cuentas de los ciberpiratas
Sistemas de pago electrónico
Dinero transferido a bancos en EE.UU. y China
Aumento de saldos en cuentas
Fondos adicionales extraidos mediante transacciones fraudulentas
Control de cajeros automáticos
Instrucciones para entregar efectivo en un momento predeterminado

CYBERSOC

- Servicio 24x7 para detección continua, protección y respuesta a incidentes.
- Disminuye el impacto de los ataques.
- Solución como servicio, escalable y customizable, que aporta un importante ahorro de costes.
- Integración con más de 150 Tecnologías.
- Visibilidad en tiempo real de las amenazas.
- Respuesta automática inmediata frente a posibles incidentes de seguridad.



MODELO OPERACIONAL DE EVENTOS (SOC)



CYBERSOC V-LATAM

Una plataforma de **inteligencia artificial** y aprendizaje automático basada en la arquitectura **Big / Fast Data**

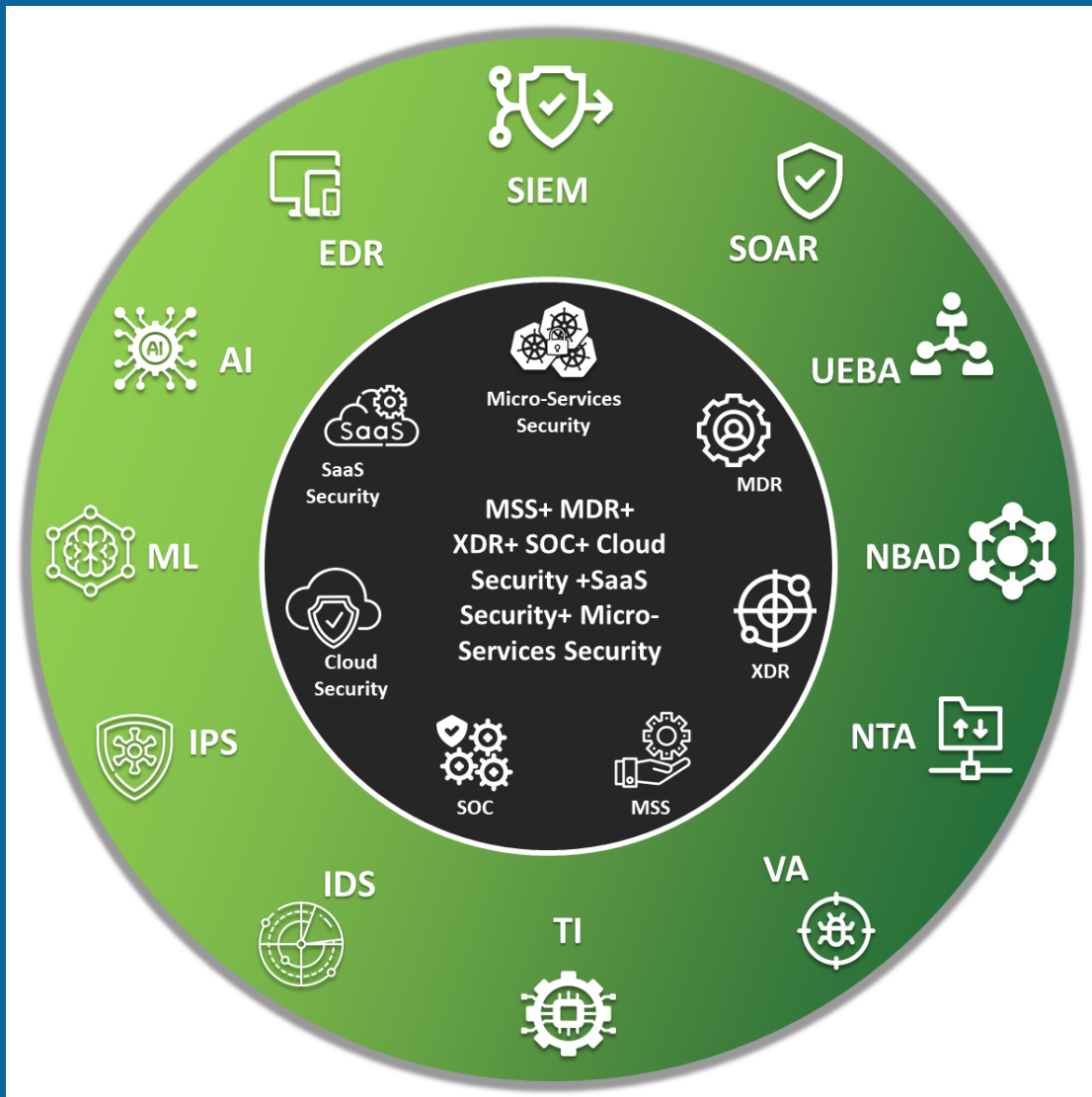
Detección y remediación de amenazas integrales integradas en una sola plataforma

Fuera de la caja - **presenta automáticamente** solo **amenazas analizadas / verificadas**, sin ajustes nunca

Aprovecha la inteligencia artificial para **detectar y detener las amenazas, sin intervención humana**

Un agente aiXDR especialmente diseñado que **rastrea** todos los activos **incluso cuando no están en la red de la empresa**

Una **solución integrada** que cubre el cumplimiento y un amplio **espectro de casos de uso**



CYBERSOC V-LATAM

(SIEM+SOAR+UEBA+NBAD/NTA+TI+IDS/IPS+ML+AI+VA+EDR: Comprehensive Cybersecurity for Digital-Era)

Reduce el tiempo medio de respuesta (MTTR) con corrección automática de amenazas

Reduce el tiempo medio de identificación (MTTI) con la detección proactiva de amenazas

Cumplimiento y supervisión continuos (análisis de seguridad)

Visibilidad completa de todos los activos, flujos, aplicaciones y sus interacciones

Implementación flexible y escalable en bare metal, en la nube o híbrido

Reduce CAPEX / OPEX ya que las licencias se basan en la cantidad de activos

Elimina la necesidad de soluciones de silos (como EDR, SIEM, UEBA, DLP, IDS, IPS, SOAR, NBAD)

V-LATAM

TECNOLOGÍA DE PUNTA EN NUESTRO CYBERSOC

Micro Service architecture based on Docker Containers

Built on Highly scalable Proven platforms and Frameworks

Extensible and Pluggable Design with standard Open Interfaces (REST,JSON..)

Flexible deployment model
Ansible, Docker, DevOps

Functional programming
Lazy loading

Lambda Data Processing Architecture
With proven Big/Fast Data patterns

Kafka can ingest up to **50B events per day**

Spark Streaming has been benchmarked to handle **150M events per second**

Elastic Search **indexes 50TB of documents per day**

Python machine learning library includes contemporary algorithms

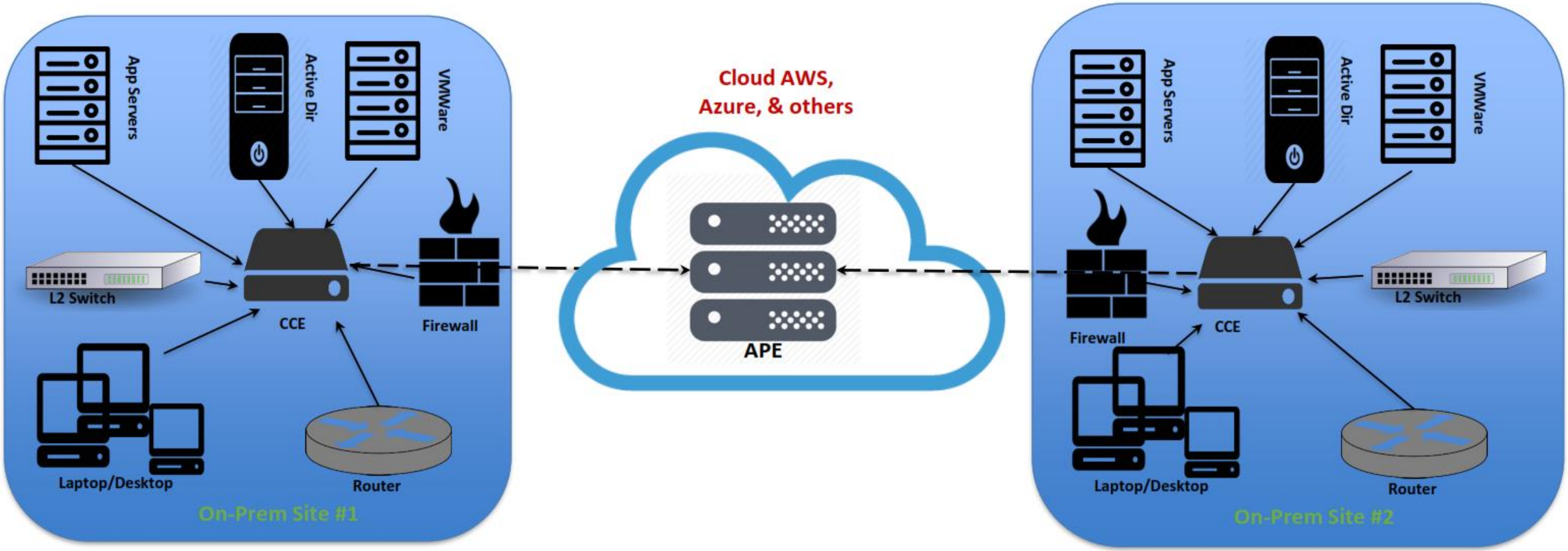
NodeJS server is proven to handle **Millions of User requests per second**

Cassandra can scale to **400K operations per second**

Pre-packaged Processes
Proven set of fully functional engines

VLATAM

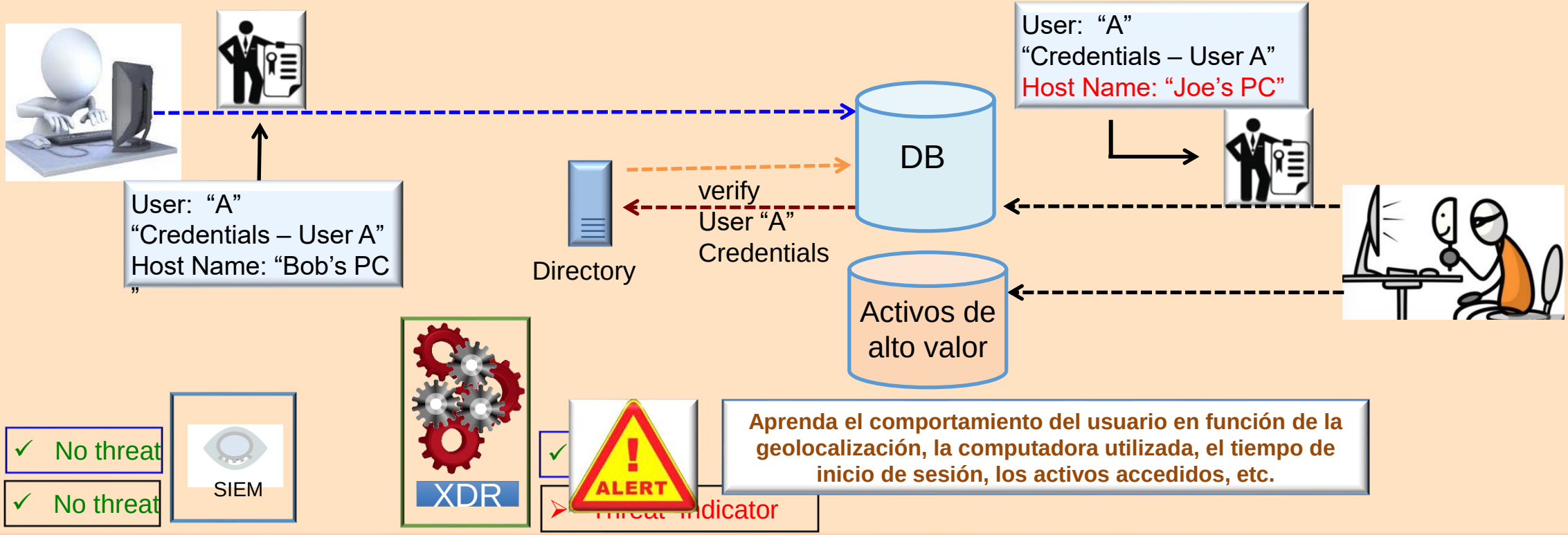
ARQUITECTURA CYBERSOC



LATAM

Use Case: Compromised Credentials

- Las credenciales comprometidas representan el 75% del robo de datos
- La mayoría de las soluciones de seguridad tradicionales son ciegas a casi todas las formas de credenciales comprometidas.
- Seceon detecta todas las formas de uso de credenciales comprometidas en tiempo real para fuentes externas o internas



CYBERSOC : Casos de Uso

(SIEM+SOAR+UEBA+NBAD/NTA+TI+IDS/IPS+ML+AI+VA+EDR: Comprehensive Cybersecurity for Digital-Era)

Una plataforma integrada que cubre un conjunto completo de casos de uso y proporciona cumplimiento continuo

Cyber Crime

- **Ransomware***
- **Malware***
- **Spyware***
- **APTs**
- **Potential Infiltration**
- **Botnet Detection**
- **Trojan Activity**

- ***All Known and Zero-Day**

Insider Threats

- **Malicious Insider**
- **Compromised Credentials**
- **UEBA**
- **Privilege Misuse**
- **Suspicious Login**

Cloud Security

- **IaaS**
  - AWS, GCP, Azure
- **SaaS**
  - O365
  - Azure AD
- **PaaS**
- **CASB**
  - API-based

Denial of Service

- **Volumetric**
- **Application Layer**
- **Protocols**
- **ICMP**
- **Amplification**
- **SYN Attack**

Strict Policy Enforcement

- **Limit access to Critical Assets**
- **Stop Unwanted Connectivity, Applications**
- **Network Segregation and Segmentations**
- **Catch multi-stage, multi-vectors malware/ransomware attacks Proactively**

VLATAM

CYBERSOC : Casos de Uso

(SIEM+SOAR+UEBA+NBAD/NTA+TI+IDS/IPS+ML+AI+VA+EDR: Comprehensive Cybersecurity for Digital-Era)

Vulnerability Exploits

- **Unknown**
- **Known OS**
- **Apps**
- **Firmware**
- **Vulnerability Assessed**

Brute Force

- **Password Spraying**
- **Dictionary Attack**
- **Credential Surfing**

Web/Email Exploits

- **Web**
  - SQL Injection
  - Cross-Site Scripting
  - Local File Inclusion
  - Directory Traversal
  - Remote File Execution
  - Cross-Site Request Forgery
- **Email**
  - Spam
  - Business Email Compromise

DNS Protection

- **DNS Tunneling**
- **DNS Fast Fluxing**

Continuous Compliance

- **HIPAA**
- **PCI-DSS**
- **NIST**
- **GDPR**
- **SOX**

Other Use Cases

- **Data/IP Exfiltration**
- **IoT/IIoT Cybersecurity**
- **OT/ICS Cybersecurity**
- **Detect IT Mistakes**
- **Detect Shadow IT**
- **NBAD**
- **IDS/IPS**

VLATAM

CYBERSOC : Casos de Uso

(SIEM+SOAR+UEBA+NBAD/NTA+TI+IDS/IPS+ML+AI+VA+EDR: Comprehensive Cybersecurity for Digital-Era)

Threat Hunting

- Explore de manera proactiva todo su entorno en busca de posibles vulnerabilidades y amenazas aprovechando la inteligencia de amenazas global y el análisis contextual y de comportamiento. Esto incluye inicios y cierres de sesión, eventos de archivos, actividad de dispositivos USB, etc..

Incident Response & Forensics

- Respuesta automatizada en tiempo real que satisface las necesidades anticipadas de la organización.
- Recopile datos relevantes para las fases de un ataque, como explotación, instalación, C&C y movimiento lateral.
- Almacene datos forenses detallados para la investigación posterior al incidente.

File Integrity Monitoring

- Detectar actividad ilícita
- Diagnosticar cambios no deseados
- Gestión de mandatos de cumplimiento

Data Loss Prevention

- Utiliza un mecanismo de detección de anomalías
- Proporciona visibilidad de los datos almacenados en todos los puntos finales (dentro y fuera de la organización)

New Elimination Options

- Poner en cuarentena la estación de trabajo
- Mata el proceso
- Restablecer la conexión de red

VLATAM

ALGUNAS DETECCIONES EN CLIENTES REALES

NUESTRA TECNOLOGÍA DETECTÓ UN SERVIDOR QUE HACÍA CONSULTAS A DOMINIOS NO PERMITIDOS

1. Seceon en conjunto con su módulo de Machine Learning detectó el comportamiento sospechoso del equipo dc el cual realiza conexiones a distintos host internos y externos (alrededor de unas 50 conexiones el día de hoy 08 de enero).

Alert Level: Major
Alert Type: Botnet Detected
Alert Message: The Host dc is participating in a DNS Outflood.
Alert Status: Open
Alert ID: 6027269010853513927

Legend: Host/User | Network | Application | Machine Learning

Export Alert Details

Threat Indicator Type: : Unusual Number Of Connections From Host To Host On Port

Time	Origin	Type	Message	Source/Profiled Device Source/Profiled IP/Host Asset Group	Target Device Target IP Asset Group	User Name
08/01/2019 12:51:23		Unusual Number Of Connections From Host To Host On Port	Unusual number of connections from dc ns1.softlayer.com on application port	dc 17 VLAN Servicios	ns1.softlayer.com Uncategorized	
08/01/2019 12:51:22		Unusual Number Of Connections From Host To Host On Port	Unusual number of connections from d o ns2.softlayer.com on application port	dc 17 VLAN Servicios	ns2.softlayer.com Uncategorized	
08/01/2019 02:49:42		Unusual Number Of Connections	Unusual number of connections from dc o 192.168.74.27 on application port 53	dc 17 VLAN Servicios	192.168.74.27 192.168.74.27 Uncategorized	

Go to page: 1 Show rows: 20 1-20of118

HEMOS DETECTADO LOGINS NO AUTORIZADOS A BASES DE DATOS

Type	Message	Source Device Source IP Asset Group	Source Data Type	Target Device Asset Group	User Name
Database Login Success	mssql_logs: ;'MSSQLSERVER 17:39:(A.LOCAL CESS 33205 dministrator Audit event: audit_schema_version:1 event_time:2021-05-12 22:39:06.4297254 sequence_number:1 action_id:LGIS succeeded:true is_column_permission:false session_id:234 server_principal_id:792 database_principal_id:0 target_server_principal_id:0 target_database_principal_id:0 object_id:0 user_defined_event_id:0 transaction_id:0 class_type:LX permission_bitmask:0000000000000000000 sequence_group_id:8C4EEC3E- session_server_principal_name: server_principal_name:msantillana server_principal_sid:0126148ca6641458de database_principal_name: target_server_principal_name: target_server_principal_sid: server_instance_name:MI database_name: schema_name: object_name: statement:-- network protocol: TCP/IP set quoted_identifier on set arithabort off set numeric_roundabort off set ansi_warnings on set ansi_padding on set ansi_nulls on set concat_null_yields_null on set cursor_close_on_commit off set implicit_transactions off set language Español set dateformat dmy set datefirst 1 set transaction isolation level read committed additional_information:00x280001200x0001 192.168.20.205	192.16 Uncategorized	seceon-events		msantillana

EVENTO A LAS 17:39

LOGIN SATISFACTORIO

USUARIO MSANTILLANA

SERVIDOR MIN

DIRECCION IP 192.168.20.205

VLATAM

TECNOLOGÍA DE PUNTA EN NUESTRO CYBERSOC

✓	Major		**Ransomware in Progress**: The host mtto-monitoreo [redacted] is suspected to be Ransomware In Progress. This host is involved in scanning network and made a new connection and SMB Port open to public has seen.	mtto-monitoreo [redacted] HOST	Uncategorized	ylomparte, ochavez, [redacted]	50%	8/7/2022 7:30:43		Open

Threat Indicator Types | Threat Indicator Details | Recommendations | Event Trending and History | Alert Actions

Alert ID: 5317773018701095979

Legend: Host/User | Network | Application | Machine Learn

Export Alert Incident Package | Export Alert Deta

Threat Indicator Types

Origin	Type	Instances	First Threat Indicator Timestamp	Last Threat Indicator Timestamp
	IP Scan	732	17/4/2022 20:04:00	8/7/2022 8:06:00
	New Connection Between Two Hosts	60	17/4/2022 20:22:49	7/7/2022 14:50:06
	Trojan Horse Traffic	10	17/4/2022 20:26:00	5/6/2022 20:38:00
	New Connection To An Application On A Host	4	21/4/2022 17:56:19	16/5/2022 13:12:59
	Unusual Number Of Outgoing Bytes	1	25/4/2022 18:33:37	25/4/2022 18:33:37
	Single Port Scan Across Network	1	8/6/2022 10:29:00	8/6/2022 10:29:00
	SMB Port Open to Public	1	8/7/2022 7:27:00	8/7/2022 7:27:00

ALGUNAS DETECCIONES EN CLIENTES REALES

Alert Profile

Severity	Origin	Type:Message	Entity:Type	Entity:Group	User Name	Confidence	Time	Assigned To	Status
Major		**Potential Web Exploit**: The host 192.168.10.29 is suspected to be under 'Potential Web Exploit' attack.	192.168.10.29: HOST	SRV DL HP	SYSTEM, iacuna_857416, Administrator, jmontalvo	60%	23/6/2022 17:49:52		Closed

Threat Indicator Types

Origin	Type	Instances	First Threat Indicator Timestamp	Last Threat Indicator Timestamp
	Web Exploit	17	23/6/2022 17:44:32	23/6/2022 17:46:07

rcode	**"192"**
reason	**"dt: Detects specific directory and path traversal"**
request	**"/plugins/PluginController.php"**
request_method	**"GET"**
rule	**"(?:(?:\/|)(\.\.\/home|\.\.\/conf|\.\.\/usr|\.\.\/proc|\.\.\/opt|\.\.\/s?bin|\.\.\/local|\.\.\/dev|\.\.\/tmp|\.\.\/kern|\.\.\/[br]oot|\.\.\/sys|\.\.\/system|\.\.\/windows|\.\.\/winnt|\.\.\/program|%[a-z_-]{3,}%)(?:\/|))"**
src_addr_space	**"private"**
src_network_tags	**"private"**

CYBERSOC – ALERTAS

Open Threat Management

All Traffic for Last 15 days ending at 2/19/2021 2:03:51 PM | Select: Last 15 days | Our Company

17 Alert(s) for Last 15 days

Legend: Host/User | Network | Application | Machine Learning

Export to Excel

Filter... | Show Only Critical Alerts | Show Only Major Alerts | Show Only Minor Alerts | Filter by Status: Open

By default, Critical and Major alerts are shown when no filters are used.

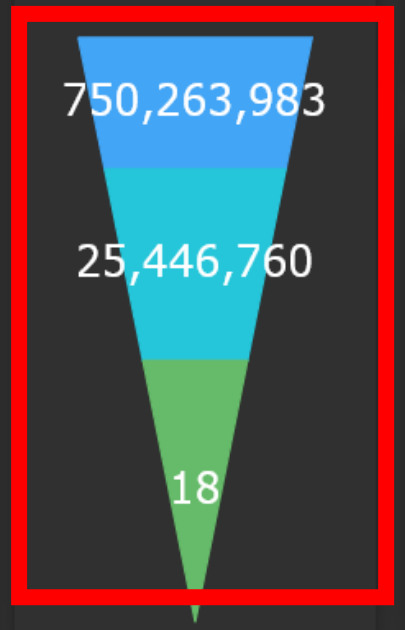
Severity	Origin	Type:Message	Entity:Type	Entity:Group	User Name	Confidence	Time	Assigned To	Status
Critical		**Policy Violation**: Policy violated due to prohibited country China, Pakistan, Russia having host 120.79.31.82, server-185-153-199-132.cloudedic.net, 91.241.19.60 and 4 others is accessed by 96.237.103.37.	96.237.103.37: HOST	Seceon-Cloud		100%	2/13/2021 4:39:07 PM	Abhishek Tripathi	Open
Critical		**Policy Violation**: Policy violated by the host 192.168.19.2. It tried to access the application Facebook Games.	192.168.19.2: HOST	Seceon-Cloud		100%	2/12/2021 5:16:06 AM		Open
Critical		**Policy Violation**: Policy violated due to prohibited country China, Russia having host 120.131.3.164, mc.yandex.ru is accessed by 192.168.19.136.	192.168.19.136: HOST	Seceon-Cloud		100%	2/8/2021 8:05:08 AM		Open
Critical		**Potential Malware Infected Host**: Threat Indicators on the host Swaraj have been observed which indicates a high risk of hacking, virus or other malicious activity.	Swaraj: HOST	Uncategorized	SWARAJ$, DELL, LOCAL SERVICE	75%	2/17/2021 11:50:09 PM		Open
Critical		**Potential Data Exfiltration**: The host 192.168.19.229 is confirmed to be involved in potential data exfiltration due to unusual large amount of data leaving organization.	192.168.19.229: HOST	Seceon-Cloud		70%	2/6/2021 5:50:09 AM		Open
Major		**File Access Monitoring**: FILE_DELETE action has been performed on file(s) C:\CCE\Arpita\putty-0.74.tar.gz, C:\CCE\Arpita\pageant.exe, C:\CCE\Arpita\images_reports.jpg and 3 others at CCEVM-19-136	CCEVM-19-136: HOST	Uncategorized	seceon	100%	2/5/2021 8:41:06 AM		Open
Major		**Potential Malware Infected Host**: Threat Indicators on the host VinayO-Laptop have been observed which indicates a significant risk of hacking, virus or other malicious activity.	VinayO-Laptop: HOST	Uncategorized	VINAYO$, I, LOCAL SERVICE, VINAYO-LAPTOP$	55%	2/14/2021 11:29:07 AM		Open

Select a period.
Last 7 Days

CYBERSOC – VILSOL LATAM

Auto Refresh: ON

Performance Pyramid



Total Applications Monitored

3,992

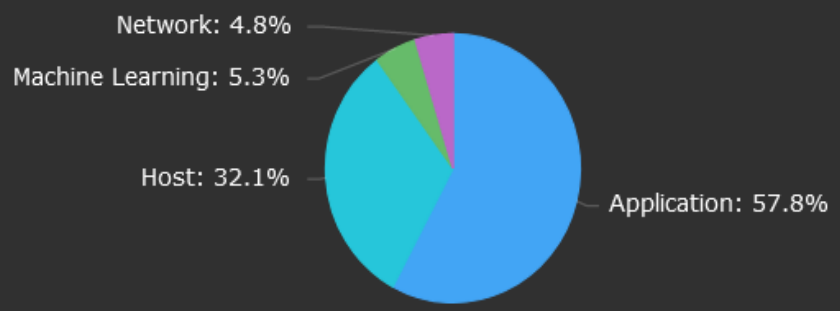
Total Private Hosts Monitored

2,114

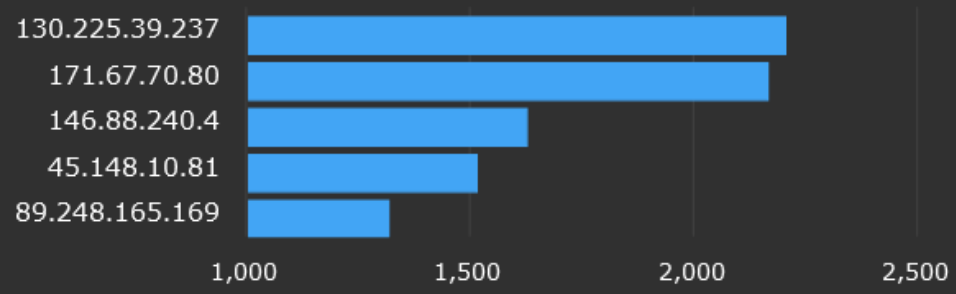
Total External Hosts Detected

33,314

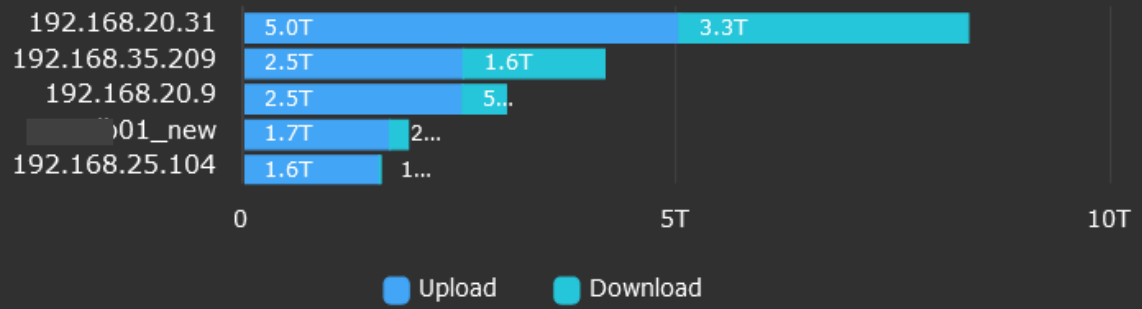
Threat Indicator Distribution by Origin



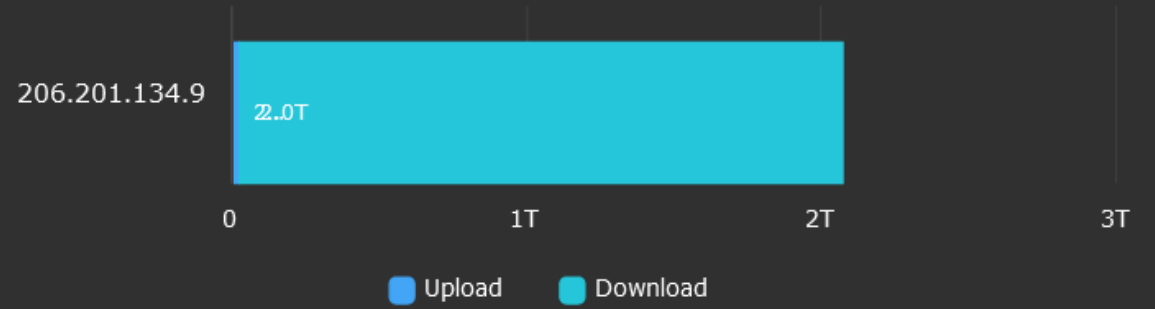
Top-5 Malicious Hosts By Flow Count



Top 5 Internal and External Hosts by Bandwidth Usage (Upload Bandwidth)



Top-5 Public Sites Accessed (Upload Bandwidth)



CYBERSOC : LISTA DE PRECIOS

Seceon aiSIEM MSSP aiSIEM = SIEM+SOAR+UEBA+NDR+TI+ML+AI		
Número de Usuarios	Cuota Mensual	Cuota Unica Anual (pagado adelantado)
< 5	$ 150.00	$ 1,500.00
< 10	$ 300.00	$ 3,000.00
< 25	$ 500.00	$ 5,000.00
< 50	$ 750.00	$ 7,500.00
< 100	$ 1,000.00	$ 10,000.00
< 200	$ 1,500.00	$ 15,000.00
< 300	$ 2,000.00	$ 20,000.00
< 400	$ 2,250.00	$ 22,500.00
< 500	$ 2,500.00	$ 25,000.00
Número de Usuarios = Número de Empleados, Contractors, Subcontractos, Invitados		
Máximo Critical Assets 25% de la cantidad de empleados está cubierto en estos precios.		

Precios son especiales para primeros 100 clientes,

Oferta válida hasta el 31 de Agosto del 2022

Se ofrece POC por 1 mes sin costo

Se require Equipo para instalar Appliance Virtual para Colectar Información

Gestión es Nube