SECAAS: SECURITY AS A SERVICE

CLOUD COMPUTING: SERVICIOS Y APLICACIONES

CURSO 2016/2017

ÍNDICE

- Definición
- Servicios ofrecidos
- Ventajas y riesgos
- Principales desafíos
- Proveedores de SECaaS
- Referencias

DEFINICIÓN

SECaaS es un modelo de Cloud Computing basado en SaaS y especializado en dar servicios de seguridad informática a traves de internet.

SERVICIOS OFRECIDOS (I)

Segun la CSA (Cloud Service Alliance) existen las siguientes categorias de servicios:

- **Gestión de identidades y accesos (IAM)**: firma electrónica, web-SSO (Single Sign-on), gestión y provisión de tokens de autenticación...
- **Prevención de perdida de datos (DLP)**: encriptación de datos transparente, gestión de políticas de acceso...
- **Seguridad web**: filtrado web, anti-virus, monitorización web, anti-phishing, análisis de vulnerabilidades web...
- **Seguridad de correo electrónico**: filtros de spam, encriptación de emails, escaneo de los contenidos...

SERVICIOS OFRECIDOS (II)

- **Evaluación de la seguridad:** auditorias de servicios cloud basadas en estanards, tests de penetración, valoración de riesgos de seguridad...
- **Gestión de intrusiones**: usando patrones de reconocimiento para detectar y reaccionar a eventos inusuales, sistemas en tiempo real para detectar o preveer una intrusión, inspección de paquetes...
- **Gestión de información de seguridad y eventos (SIEM)**: Análisis de logs con sistemas en tiempo real para la creación de informes y alerta ante indicendes de seguridad

SERVICIOS OFRECIDOS (III)

- **Encriptación**: VPN, encripcación de comunicaciones, firmas digitales, integridad y validación de mensajes...
- **Continuidad de negocio y recuperación ante desastres**: medidas diseñadas para asegurar que el servicio se mantenga en caso de fallos, cloud backup, data center alternativo, replicación de datos...
- **Seguridad de redes**: firewall, proteccion DDoS, integración con los hiper visores...

VENTAJAS Y RIESGOS (I)

Como todo servicio cloud estos servicios presentan unas ventajas sobre su equivalente tradicional:

- **Menores costes**: al facturarse por tiempo y recursos usados realmente.
- **Actualizaciones automaticas de software y definiciones de virus**: ya que son realizadas por proveedor y llegan automaticamente a todos los clientes, algo muy importante en el mundo de la seguridad.
- **Delegación de la seguridad**: lo que permite a las empresas centrarse en ofrecer sus productos.

VENTAJAS Y RIESGOS (II)

A pesar de estas atractivas ventajas el uso de estos servicios tambien conlleva sus riesgos

- **Efecto dominó**: en caso de que se descubra una vulnerabilidad en un servicio esto puede llevar a un efecto dominó debido a la amplia escala de los entornos cloud.
- **Naturaleza compartida**: existen muchos clientes que quieren soluciones personalizadas y esto no es habitual en servicios SaaS.
- **Soluciones generales**: el usar soluciones centralizadas reduce la capacidad de los clientes de personalizar estas y puede forzar a los clientes a adaptarse para adecuarse a sus servicios SECaaS.

PRINCIPALES DESAFÍOS

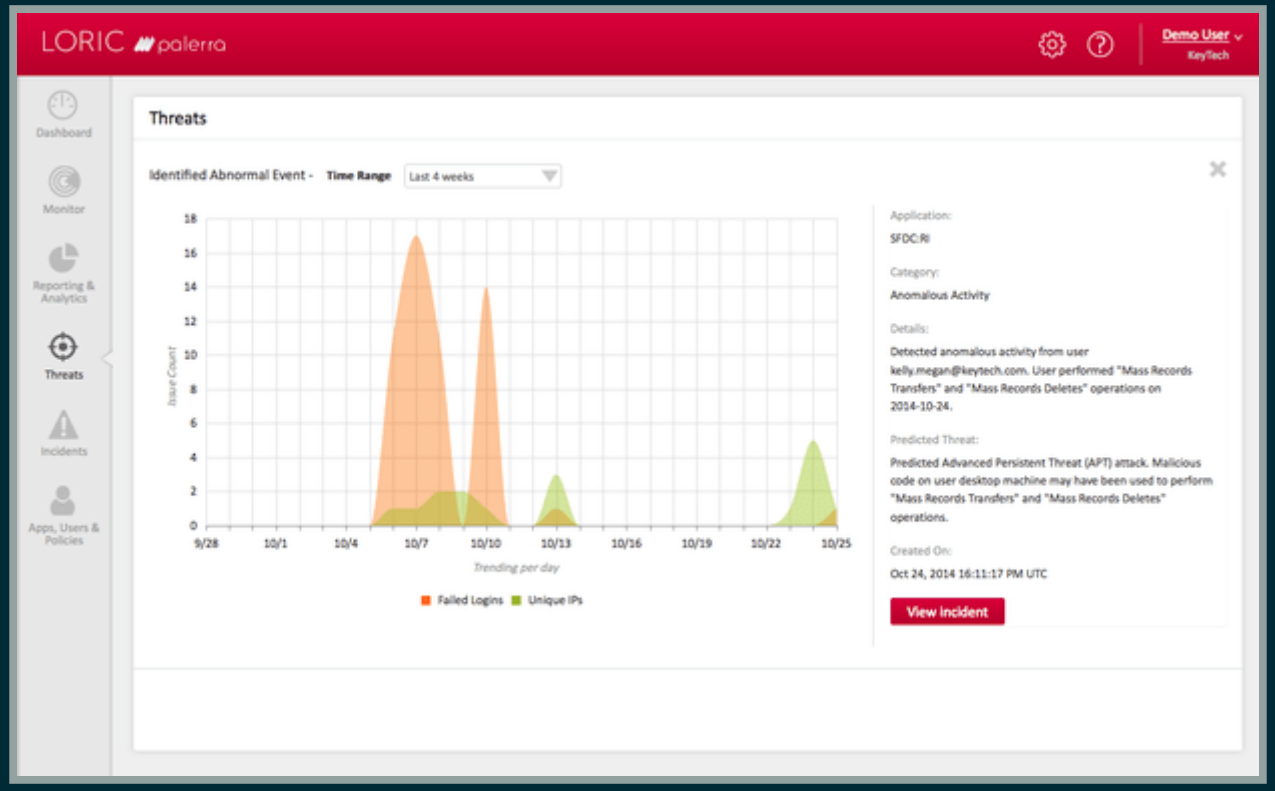
Crear un framework o estandar internacionalmente aceptado que incluya unas especificaciones mínimas.

Mantener una reputación de mayor fiabilidad respecto a las soluciones estandar no cloud.

PROVEEDORES DE SECAAS (I)

Palerra: Empresa conocida por ofrecer software de tipo cloud access security brokerage, suites integradas de seguridad en el entorno SECaaS.

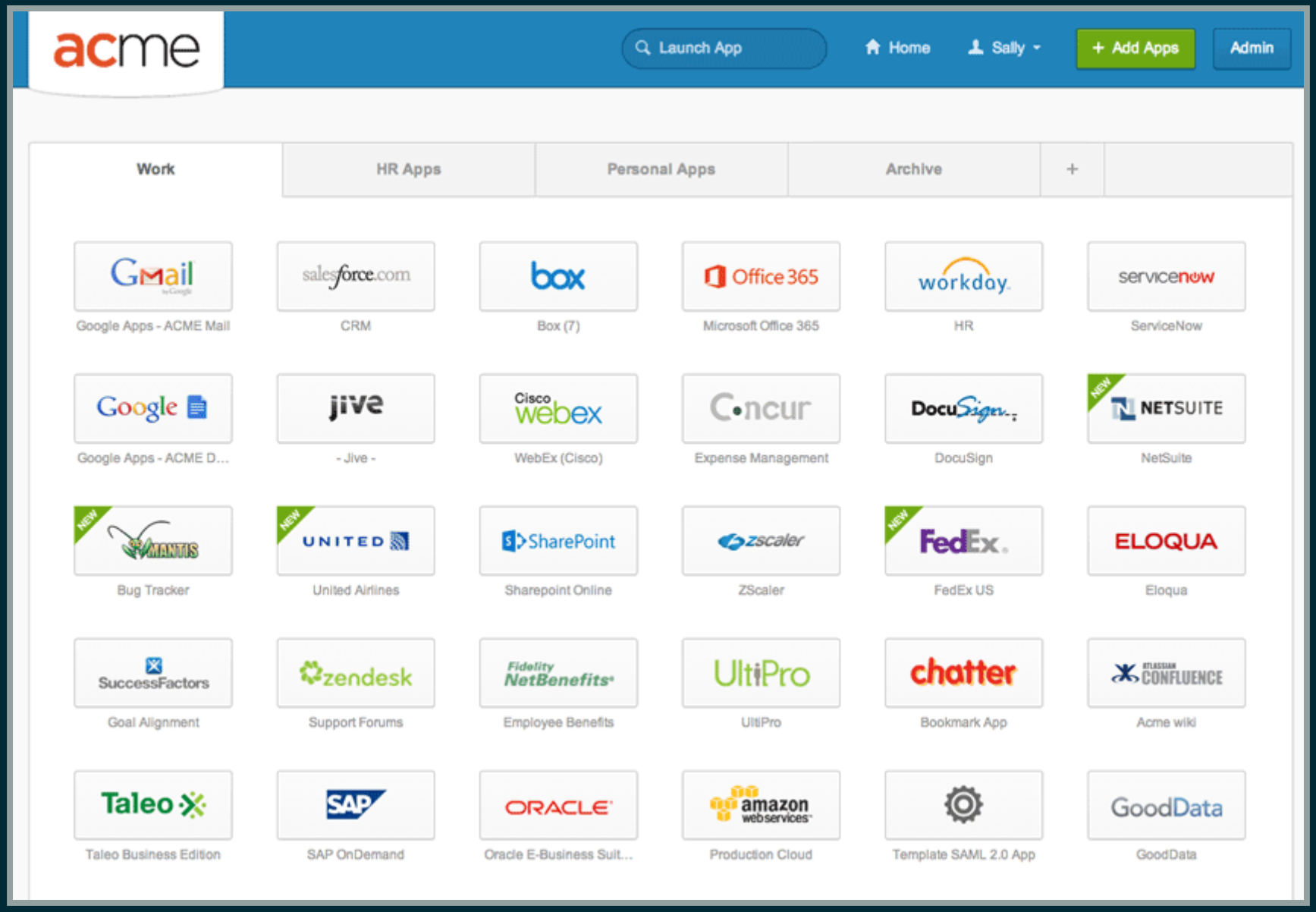
Su solución permite la detección de intrusos, el análisis predictivo, gestión de la configuración y respuesa a incidentes. Está integrada en numerosos servicios de nube como AWS, Salesforce o Github.


LORIC palerra
Demo User
KeyTech
Dashboard
Monitor
Reporting & Analytics
Threats
Incidents
Apps, Users & Policies
Threats
Identified Abnormal Event -
Time Range
Last 4 weeks
Issue Count
18
16
14
12
10
8
6
4
2
0
9/28
10/1
10/4
10/7
10/10
10/13
10/16
10/19
10/22
10/25
Trending per day
Failed Logins
Unique IPs
Application:
SFDC:RI
Category:
Anomalous Activity
Details:
Detected anomalous activity from user kelly.megan@keytech.com. User performed "Mass Records Transfers" and "Mass Records Deletes" operations on 2014-10-24.
Predicted Threat:
Predicted Advanced Persistent Threat (APT) attack. Malicious code on user desktop machine may have been used to perform "Mass Records Transfers" and "Mass Records Deletes" operations.
Created On:
Oct 24, 2014 16:11:17 PM UTC
View Incident

PROVEEDORES DE SECAAS (II)

Okta: Se centra en la gestión de identidad y acceso (IAM), destaca su producto Single Sign-on que permite a sus usuarios acceder a todas sus aplicaciones cloud o web con solo unos credendenciales de usuario. Además de esto permite la integración con AD/LDAP.

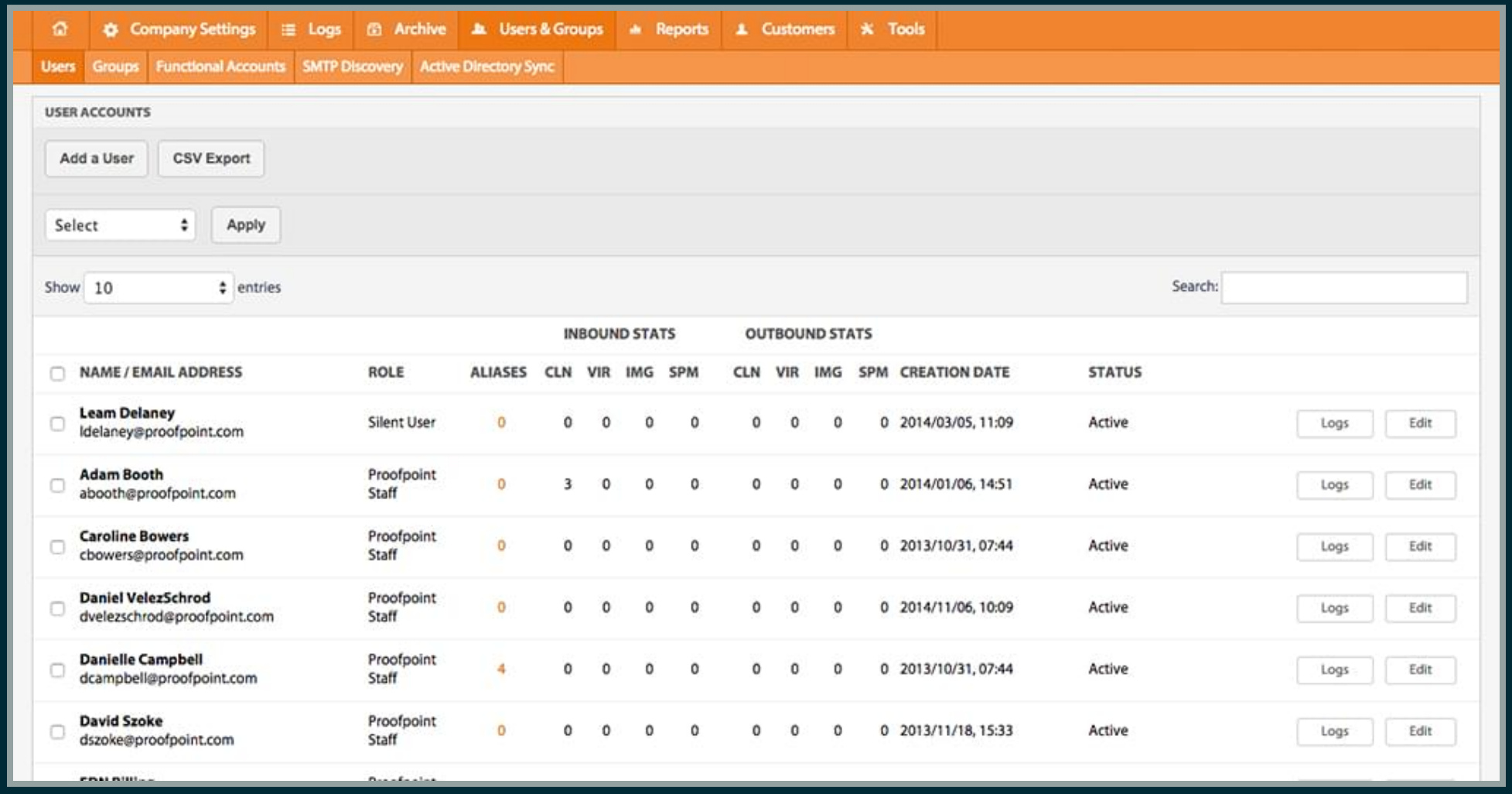
Su precio es de 2 $ al mes por usuario.


acme
Launch App
Home
Sally
+ Add Apps
Admin
Work
HR Apps
Personal Apps
Archive
+
Google Apps - ACME Mail
CRM
Box (7)
Microsoft Office 365
HR
ServiceNow
Google Apps - ACME D...
- Jive -
WebEx (Cisco)
Expense Management
DocuSign
NetSuite
Bug Tracker
United Airlines
Sharepoint Online
ZScaler
FedEx US
Eloqua
Goal Alignment
Support Forums
Employee Benefits
UltiPro
Bookmark App
Acme wiki
Taleo Business Edition
SAP OnDemand
Oracle E-Business Suit...
Production Cloud
Template SAML 2.0 App
GoodData

PROVEEDORES DE SECAAS (III)

Proofpoint: Basa su negocio en ofrecer proteccion email, afirman proteger contra malware, spam o phishing. En su SLA garantizan bloquear el 99,999% del spam y el 100% de la detección de malware. Utilizan detección basadas en firmas.

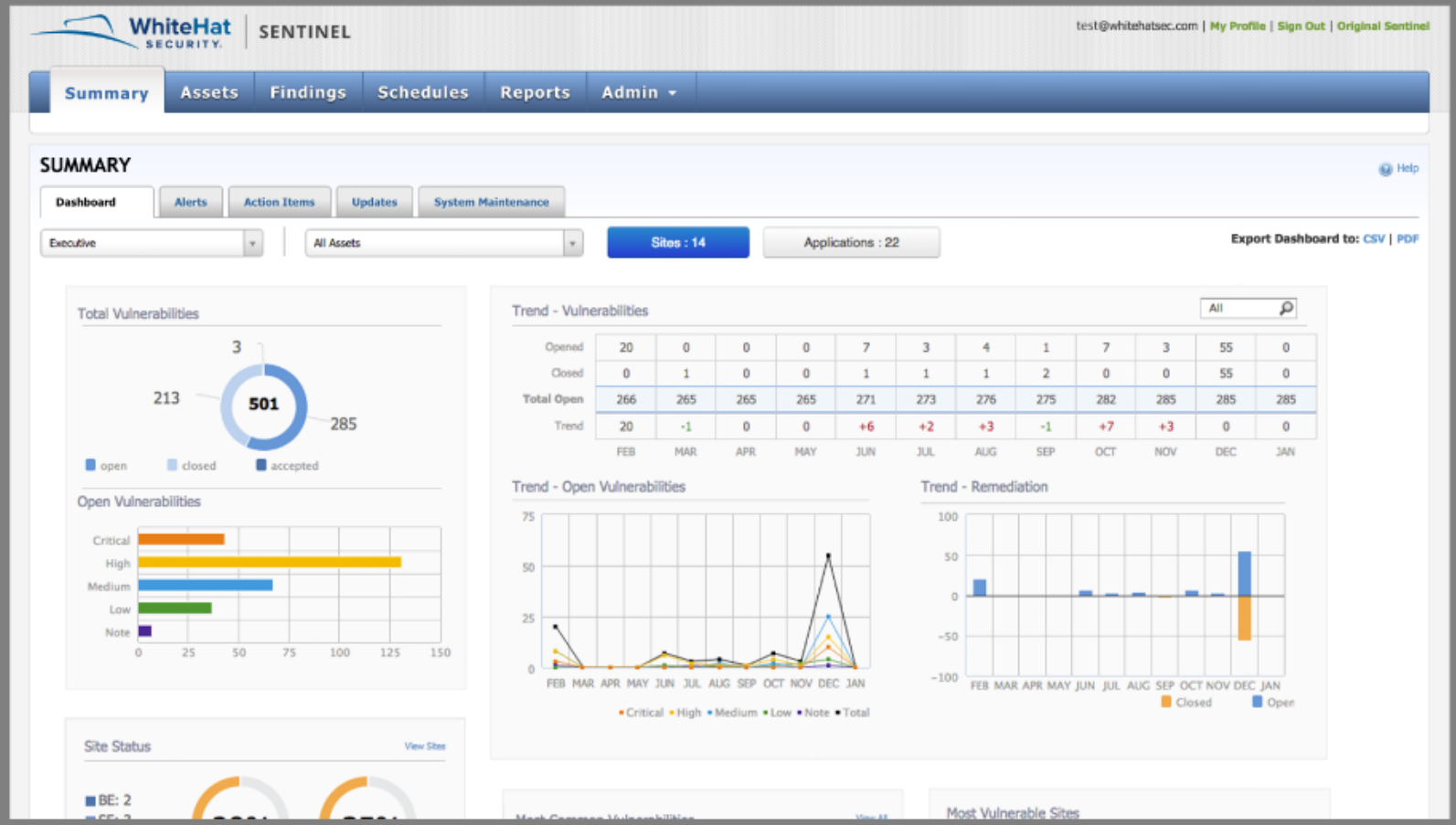
Su software permite la creación de informes, politicas personalizadas, grupos de usuarios, seguridad en redes sociales...


Company Settings
Logs
Archive
Users & Groups
Reports
Customers
Tools
Users
Groups
Functional Accounts
SMTP Discovery
Active Directory Sync
USER ACCOUNTS
Add a User
CSV Export
Select
Apply
Show 10 entries
Search:
INBOUND STATS
OUTBOUND STATS
NAME / EMAIL ADDRESS
ROLE
ALIASES
CLN VIR IMG SPM
CLN VIR IMG SPM
CREATION DATE
STATUS
Leam Delaney
ldelaney@proofpoint.com
Silent User
0 0 0 0 0 0 0 0 0 2014/03/05, 11:09 Active Logs Edit
Adam Booth
abooth@proofpoint.com
Proofpoint Staff
0 3 0 0 0 0 0 0 0 2014/01/06, 14:51 Active Logs Edit
Caroline Bowers
cbowers@proofpoint.com
Proofpoint Staff
0 0 0 0 0 0 0 0 0 2013/10/31, 07:44 Active Logs Edit
Daniel VelezSchrod
dvelezschrod@proofpoint.com
Proofpoint Staff
0 0 0 0 0 0 0 0 0 2014/11/06, 10:09 Active Logs Edit
Danielle Campbell
dcampbell@proofpoint.com
Proofpoint Staff
4 0 0 0 0 0 0 0 0 2013/10/31, 07:44 Active Logs Edit
David Szoke
dszoke@proofpoint.com
Proofpoint Staff
0 0 0 0 0 0 0 0 0 2013/11/18, 15:33 Active Logs Edit

PROVEEDORES DE SECAAS (IV)

WhiteHat Security: Esta empresa se centra en la seguridad web y de aplicación, ofrecen servicios SaaS para realizar test de seguridad dinámicos o estáticos.

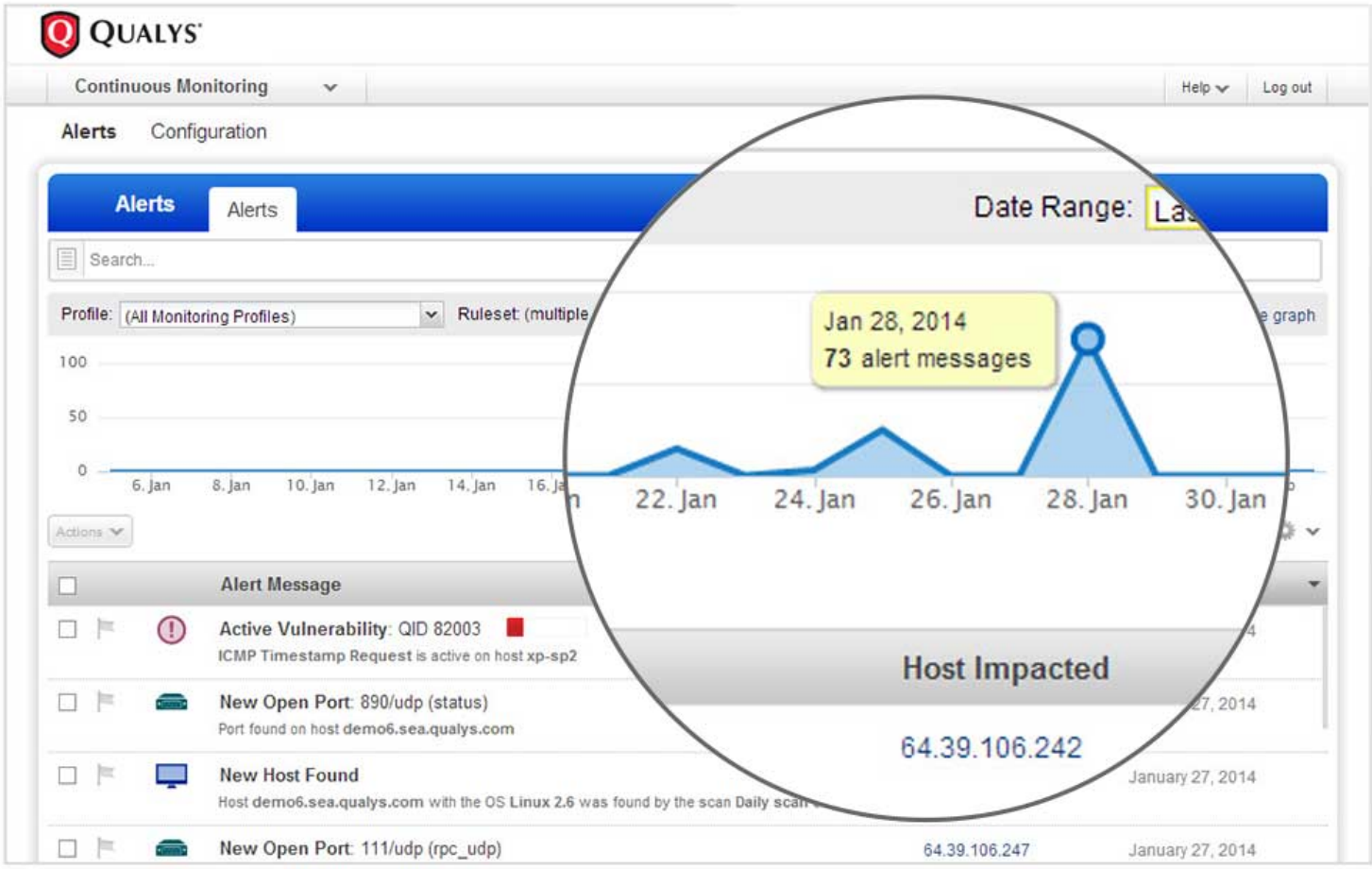
Además ofrecen consultoría personalizada para ayudar a resolver las vulnerabilidades encontradas con su herramienta.


WhiteHat SECURITY | SENTINEL
test@whitehatsec.com | My Profile | Sign Out | Original Sentinel
Summary
Assets
Findings
Schedules
Reports
Admin
SUMMARY
Help
Dashboard
Alerts
Action Items
Updates
System Maintenance
Executive
All Assets
Sites : 14
Applications : 22
Export Dashboard to: CSV | PDF
Total Vulnerabilities
3
213
501
285
open
closed
accepted
Open Vulnerabilities
Critical
High
Medium
Low
Note
0
25
50
75
100
125
150
Trend - Vulnerabilities
All
Opened 20 0 0 0 7 3 4 1 7 3 55 0
Closed 0 1 0 0 1 1 1 2 0 0 55 0
Total Open 266 265 265 265 271 273 276 275 282 285 285 285
Trend 20 -1 0 0 +6 +2 +3 -1 +7 +3 0 0
FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC JAN
Trend - Open Vulnerabilities
75
50
25
0
FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC JAN
Critical
High
Medium
Low
Note
Total
Trend - Remediation
100
50
0
-50
-100
FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC JAN
Closed
Open
Site Status
View Sites
BE: 2
Most Vulnerable Sites

PROVEEDORES DE SECAAS (V)

Qualys: este proveedor ofrece una suite integrada para la seguridad de redes. Respecto a las areas funcionales permite la monitorización continua, gestión de vulnerabilidades, escaneo web, firewall software para aplicaciones web, escaneo y monitoreo de dispositivos conectados...

Para llevar a cabo estas funciones se sirve de sensores fisicos y agentes ligeros.


QUALYS
Continuous Monitoring
Help
Log out
Alerts
Configuration
Alerts
Alerts
Date Range:
Search...
Profile: (All Monitoring Profiles)
Ruleset: (multiple
graph
Jan 28, 2014
73 alert messages
100
50
0
6. Jan
8. Jan
10. Jan
12. Jan
14. Jan
22. Jan
24. Jan
26. Jan
28. Jan
30. Jan
Actions
Alert Message
Active Vulnerability: QID 82003
ICMP Timestamp Request is active on host xp-sp2
Host Impacted
New Open Port: 890/udp (status)
Port found on host demo6.sea.qualys.com
64.39.106.242
New Host Found
Host demo6.sea.qualys.com with the OS Linux 2.6 was found by the scan Daily scan
January 27, 2014
New Open Port: 111/udp (rpc_udp)
64.39.106.247
January 27, 2014

REFERENCIAS

- Techopedia, Security as a Service (SecaaS or SaaS)
- SVT Cloud, SECaaS o Seguridad como Servicio: no solo para las grandes empresas
- CSA (Cloud Security Alliance) (2011), Defined Categories of Service
- Aleks Peterson (2016), Top 5 Security-as-a-Service Providers
- Tripwire (2016), 3 Reasons Why Your Organization Should Consider Security as a Service (SECaaS)
- CCSK Guide (2011), Security as a Service (SecaaS)
- Wikipedia (2017), Security as a service

GRACIAS POR VUESTRA ATENCIÓN
¿ALGUNA PREGUNTA?