

TIVIT

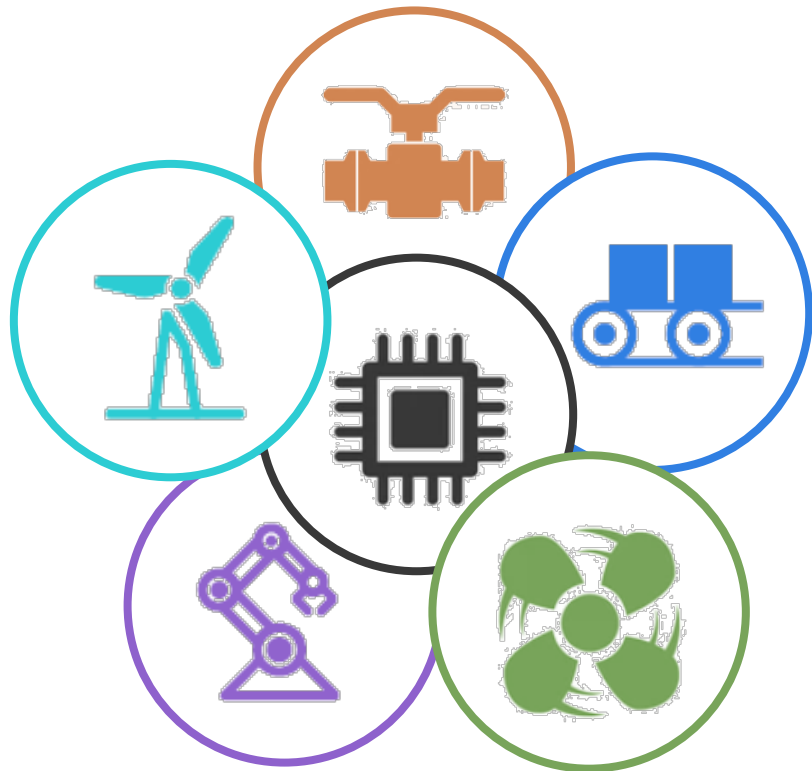
Superación Complejidades:

Desafíos y tendencias de la industria de OT

Thiago Tanaka
Cyber Security Director

Mauricio Galvez
Business Development Manager





La mayoría de los sistemas de control industrial carecen de seguridad por diseño.



La superficie de ataque para los activos cibernéticos se está expandiendo a medida que disminuye la dependencia de la protección de espacios aéreos con las iniciativas de transformación digital que impulsan la convergencia de la red de TI y TO.



Requisitos de acceso remoto para terceros y empleados que causan riesgos adicionales.



Aumento de la adopción de nuevas tecnologías, como 5G, IoT y la nube.



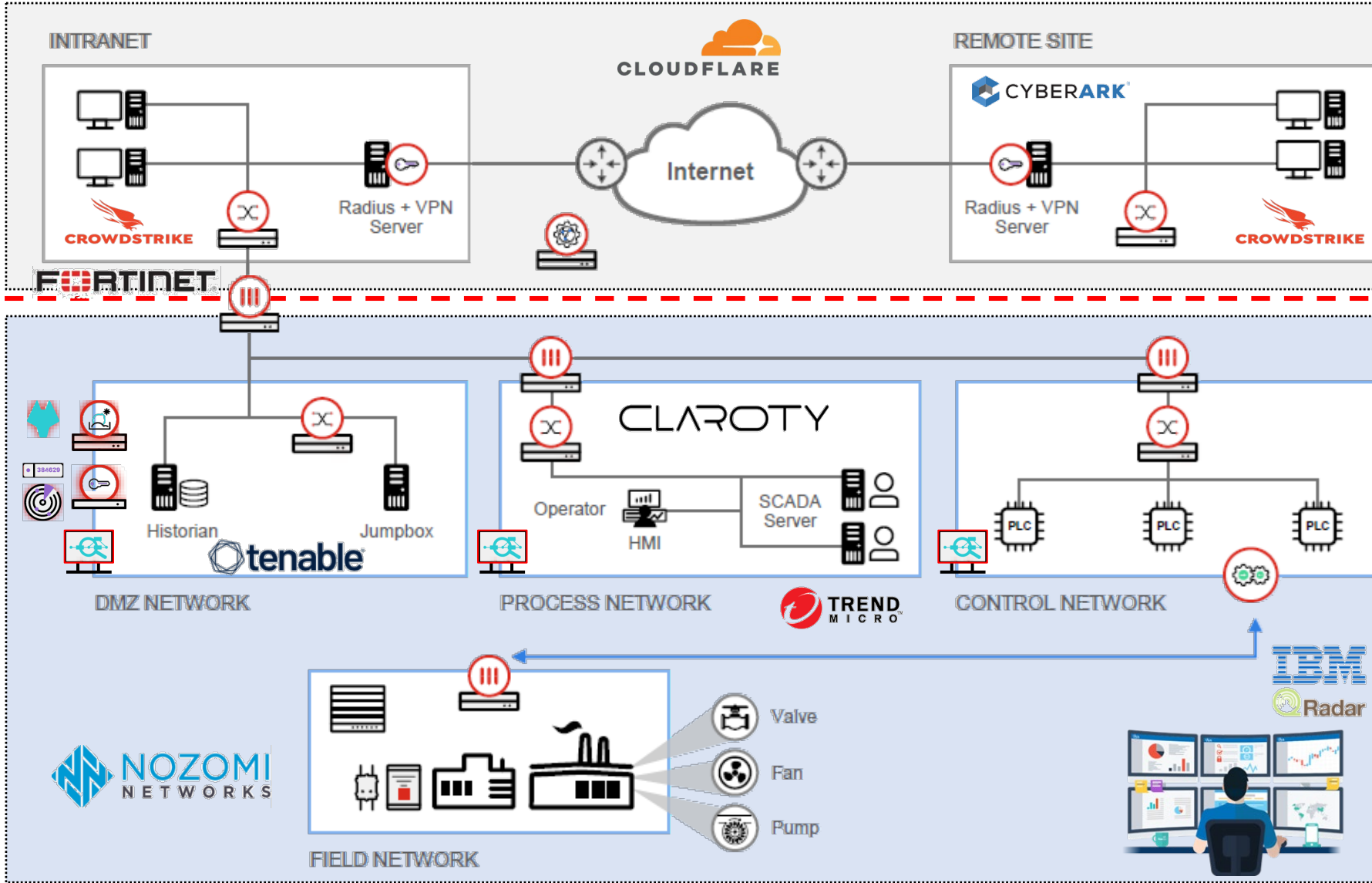
La confianza de los propietarios de activos en los OEM y los SIs expone los sistemas críticos a riesgos adicionales.

Como abordar los controles críticos Integrando OT y TI

TIVIT

Red IT

Red OT



Nuestros partners en soluciones OT

TIVIT

FORTINET

 **CYBERARK**

IBM
Radars


SentinelOne

 **NOZOMI**
NETWORKS

 **Mission**
Secure

 **tenable**

CLAROTY

 **FORESCOUT**

 **tenable**

 **TREND**
MICRO


CROWDSTRIKE


CLOUDFLARE

DRAGOS

 **paloalto**
NETWORKS

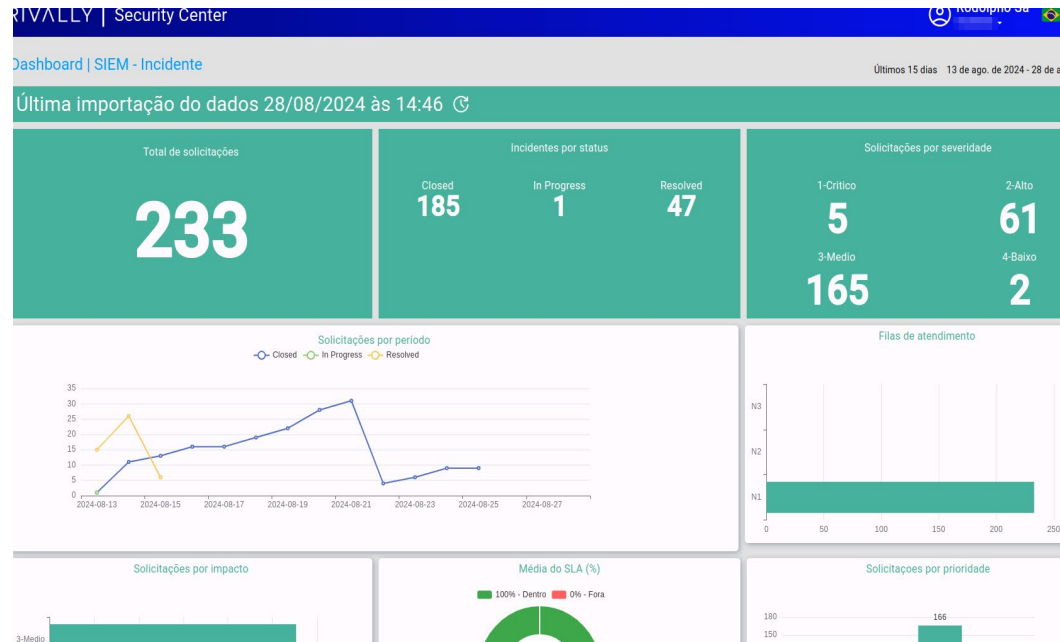


TIVIT | Security Center

TIVIT – CyberDefense – Security Center



Sistemas integrados de seguridad cibernética/ Potenciando una base de IA para optimizar la toma de decisiones tecnológicas.

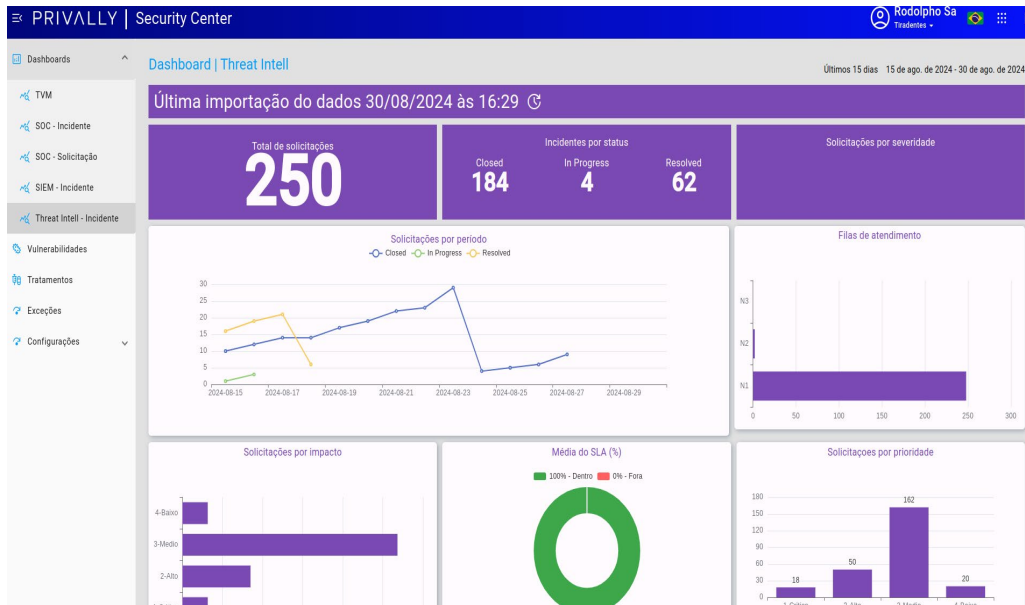


IA – Portal de incidentes generados por el **SIEM**

TIVIT – CyberDefense – Security Center



Sistemas integrados de seguridad cibernética/ Potenciando una base de IA para optimizar la toma de decisiones tecnológicas.



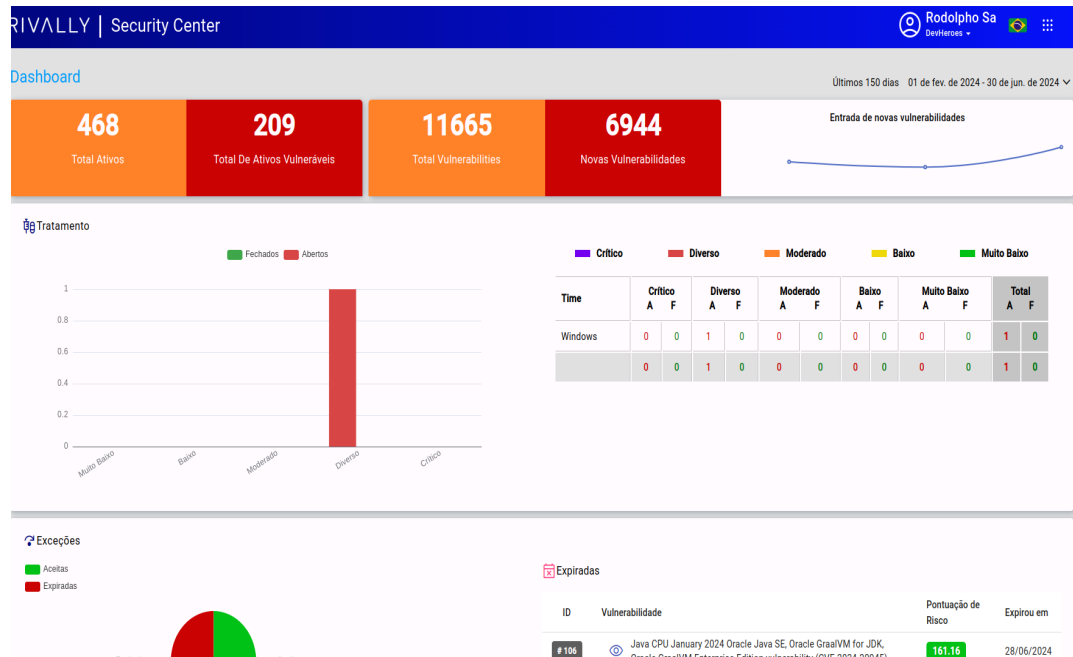
IA – Threat intelligence,

Monitorio de marca, Deep Web, Dark Web

TIVIT – CyberDefense – Security Center



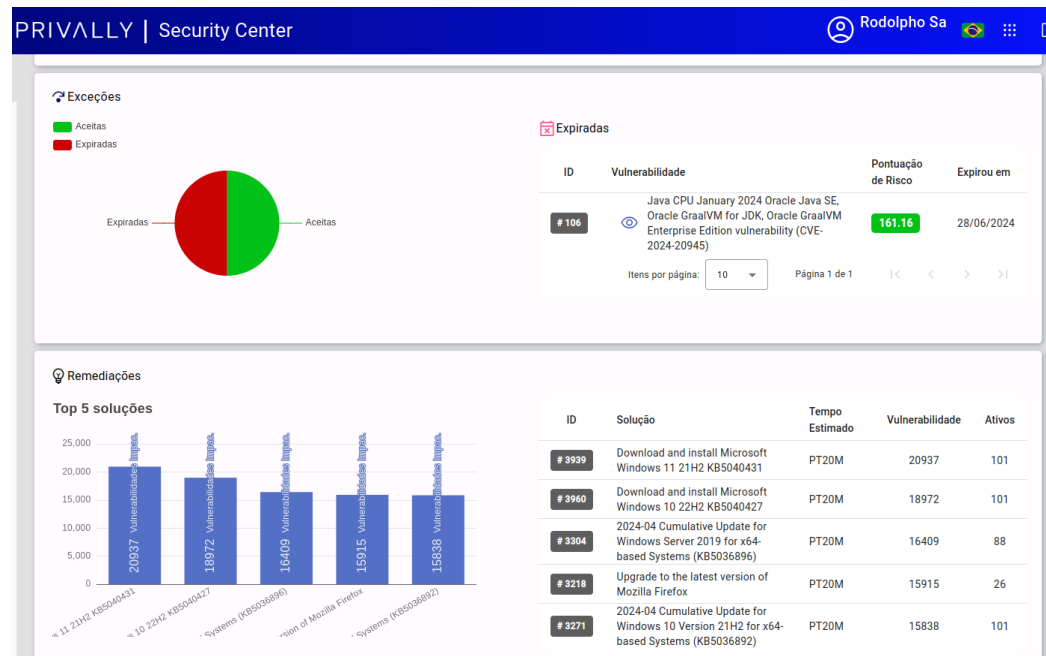
Sistemas integrados de seguridad cibernética/ Potenciando una base de IA para optimizar la toma de decisiones tecnológicas.



– Dashboard con totalizadores y tratamientos de **TVM**

TIVIT – CyberDefense – Security Center

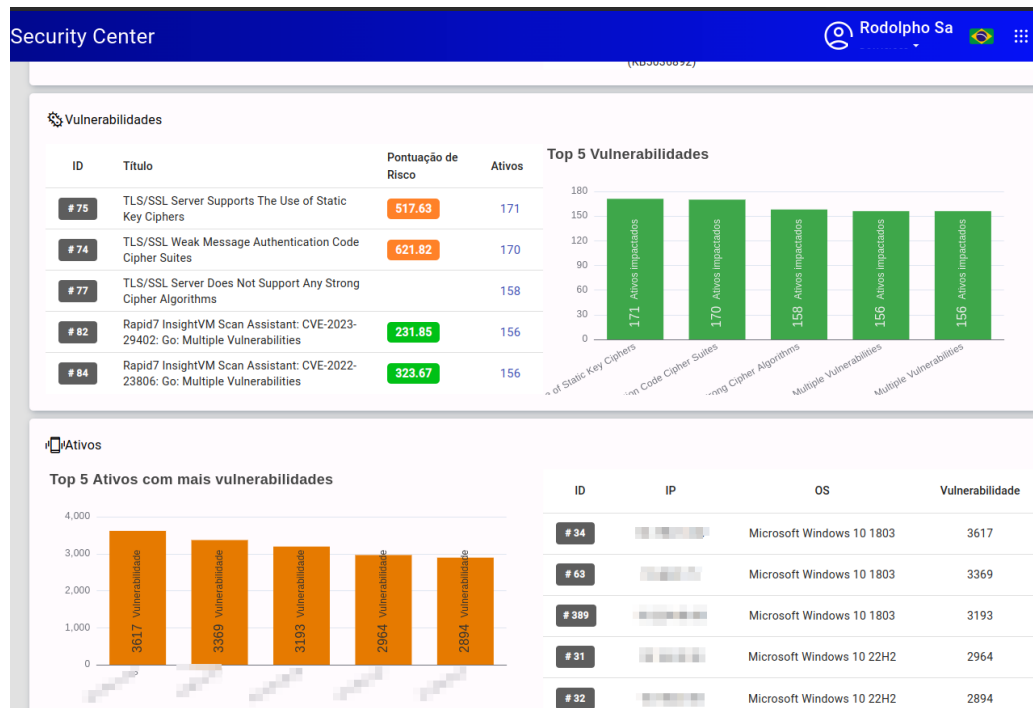
Sistemas integrados de seguridad cibernética/ Potenciando una base de IA para optimizar la toma de decisiones tecnológicas.



– Riesgo aceptados X Expirados
– TOP 5 **Soluciones** que remedian un mayor número de vulnerabilidades

TIVIT – CyberDefense – Security Center

Sistemas integrados de seguridad cibernética/ Potenciando una base de IA para optimizar la toma de decisiones tecnológicas..



– TOP 5

- La mayoría presenta vulnerabilidades
- Activos con el mayor número de vulnerabilidades

Sistemas integrados de seguridad cibernética/ Potenciando una base de IA para optimizar la toma de decisiones tecnológicas.

Vulnerabilidade N° 75
TLS/SSL Server Supports The Use of Static Key Ciphers

ID: ssl-static-key-ciphers **Severidade: Moderado**

Pontuação de Risco: 517.63 **Publicado em:** 31/01/2015 - 21:00

Categorias
Network

CVES
Nenhum CVE encontrado

Detalhe da Vulnerabilidade
The server is configured to support ciphers known as static key ciphers. These ciphers don't support "Forward Secrecy". In the new specification for HTTP/2, these ciphers have been blacklisted.

Soluções

ID	Título	Pontuação de Risco	Severidade	Ações
# 3222	Disable TLS/SSL support for static key cipher suites	configuration	PT1H	

Itens por página: 10 Página 1 de 1

Fechar **Ativos Impactados** **Incidentes** **Abrir Tratamento**

Vulnerabilidade N° 75 **Solução N° 3222**
TLS/SSL Server Supports The Disable TLS/SSL support for static key cipher suites

ID: ssl-static-key-ciphers ID: ssl-disable-static-key-ciphers **Tipo:** configuration

Pontuação de Risco: 517.63 **Tempo Estimado:** PT1H **Aplica em:**

Categorias
Network

CVES
Nenhum CVE encontrado

Detalhe da Vulnerabilidade
The server is configured to support static key cipher suites. For Microsoft IIS web servers, see [Microsoft Knowledgebase article](#) for instructions on configuring cipher suites. To achieve a higher level of security, [one may refer to authoritative sources/guides](#) as well as server vendor documentation to apply an informed cipher configuration.

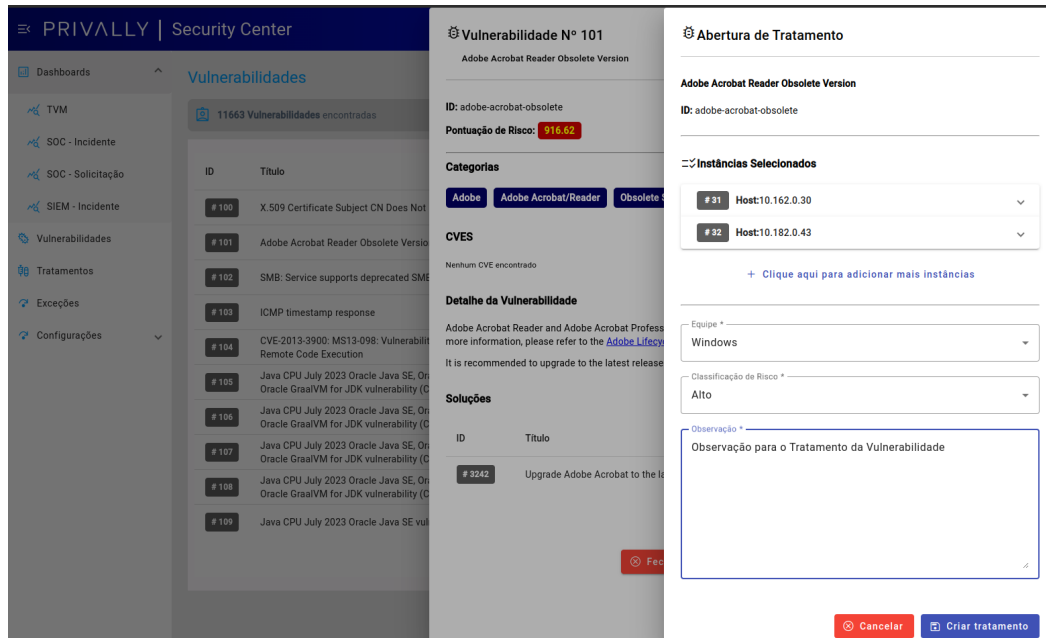
Soluções

ID	Título
# 3222	Disable TLS/SSL support for static key cipher suites

Fechar

– Detallar la vulnerabilidad con la orientación de **solución**

Sistemas integrados de seguridad cibernética/ Potenciando una base de IA para optimizar la toma de decisiones tecnológicas.



The screenshot displays the TIVIT Security Center interface. On the left, a sidebar shows navigation options like 'Dashboards', 'Vulnerabilidades', and 'Tratamentos'. The main area is divided into three panels:

- Vulnerabilidade N° 101:** Shows details for 'Adobe Acrobat Reader Obsolete Version' with a risk score of 916.62. It lists categories (Adobe, Adobe Acrobat/Reader, Obsoleto) and provides a link to 'Detalhe da Vulnerabilidade'.
- Abertura de Tratamento:** A form to create a treatment for the selected vulnerability. It includes fields for 'Equipos' (set to 'Windows') and 'Classificação de Risco' (set to 'Alto'). A text area for 'Observação' is also present.
- Instâncias Selecionadas:** A list of two selected instances: #31 (Host:10.162.0.30) and #32 (Host:10.162.0.43).

Buttons for 'Cancelar' and 'Criar tratamento' are visible at the bottom of the treatment form.

– Apertura del tratamiento

simplificada:

- Define los activos
- Dirige el equipo
- Reclasificar o recalificar

TIVIT – CyberDefense – Security Center



Sistemas integrados de seguridad cibernética/ Potenciando una base de IA para optimizar la toma de decisiones tecnológicas.

PRIVALLY | Security Center Alexandre Gasparino

Dashboards Tratamentos 8 Tratamentos encontrados

ID	Vulnerabilidade	Risk Score	Class. de Risco	Time	Status	Criado por	Criado em	Ativos	Ações
#101	Java CPU January 2024 Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition vulnerability (CVE-2024-20945)	161.16	Moderado	Backup	Cancelado		26/04/2024		
#102	Self-signed TLS/SSL certificate	249.42	Alto	Linux	Aberto		09/05/2024		
#103	TLS Server Supports TLS version 1.1	522.27	Moderado	Linux	Finalizado		09/05/2024		
#104	TLS Server Supports TLS version 1.1	522.27	Muito Baixo	Aplicações	Aberto		10/05/2024		
#106	Self-signed TLS/SSL certificate	249.42	Critico	Aplicações	Aberto		10/05/2024		
#107	TLS Server Supports TLS version 1.1	522.27	Moderado	Backup	Aberto		04/06/2024		
#109	TLS Server Supports TLS version 1.0	536.93	Critico	Windows	Aberto		26/06/2024		
#110	Java CPU January 2024 Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition vulnerability (CVE-2024-20919)	161.16	Muito Baixo	Linux	Finalizado		26/06/2024		

Itens por página: 10 Página 1 de 1

Tratamento Nº 102 Aberto

Informações da Vulnerabilidade

ID: ssl-self-signed-certificate
Risk Score: 249.42
Severidade: Moderado
Publicado em: 1995-01-01T00:00:00Z
Categorias: Network
Nenhuma CVE informada

The server's TLS/SSL certificate is self-signed. Self-signed certificates cannot be trusted by default, especially because TLS/SSL man-in-the-middle attacks typically use self-signed certificates to eavesdrop on TLS/SSL connections.

Informações do tratamento

Observações:
Sem observações

Time: Linux
Classificação de Risco: Alto
Responsável pelo tratamento: Data Prevista para conclusão:

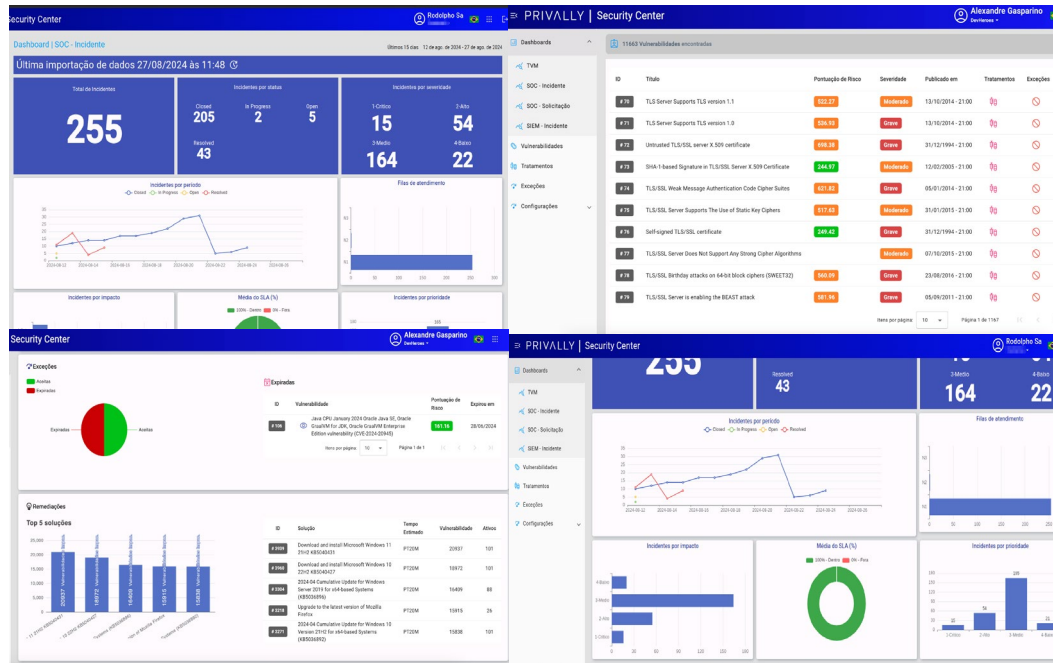
Cadastrar andamento
Parecer da classificação de risco:

IA – Gestão de Risgos de activos,
tratamiento, monitoramento con
inteligencia para operaciones de
CyberSeguridad

TIVIT – CyberDefense – Security Center



Sistemas integrados de seguridad cibernética/ Potenciando una base de IA para optimizar la toma de decisiones tecnológicas.



IA –Vision **integrada** de las tecnologías cibernéticas, alimentando la IA, generando ganancia **Operativa, Gestión y Gobernanza/Seguridad**

Seguridad en la nube

SASE | DLP | CASB | SD-WAN | FWaaS | SWG | ZTNA | RBI
 CNAPP | CSPM | CWPP | SeguridadCI/CD | CIEM

Seguridad perimetral

NGFW | IPS/IDS | WSG | Puerta de enlace de correo electrónico

Servicios de seguridad gestionados - MSS

TVM | MDR | MSS
 Threat Intelligence | CSIRT
 IoT e OT Security
 Cloud Protection
 People as a Service

Seguridad de la red

NGFW | NDR | Firewall DNS
 Microsegmentação | NAC
 DDoS Aplicação e Volumétrico

Seguridad desde el diseño - DevSecOps

SAST | DAST | Code Review
 App Penetration | Security Arch
 Security Flow | Security Cycle

Seguridad de endpoints

EPP | EDR | XDR | DLP | MDM
 Gestión de parches

**TIVIT
 DEFENSE**

**Tecnología,
 Procesos y
 Personas**

RedTeam

Hacking Ético | Análise Forense
 IRR | Hardening | Phishing

Monitoreo continuo y detección avanzada de amenazas

SIEM | NDR | VUELO | MDR | XDR
 Detección | Investigación | Caza de amenazas
 Notificación | Respuestas

Soluciones avanzadas

HSM | Criptografía
 Anonimización y seudonimización
 Descubrimiento de datos | Encriptación transparente
 Tokenización con enmascaramiento dinámico
 Recompensa por errores
 Fraude

Aplicaciones de seguridad

TVM | WAF | SAST | DAST | DSPM
 Honeypot | Deception

Gestión de identidades y accesos

IAM | IGA | PAM | CIAM | MFA

Gobernanza, Riesgo y Cumplimiento

Análisis de brechas | Assessment de Segurança
 PCI-DSS | NIST | ISO27001 | HIPAA | ISO27701 | LGPD
 Concienciación sobre la seguridad
 Centro Privado | Centro de seguridad



TIVIT

CONECTANDO TECNOLOGIA
PARA UM MUNDO MELHOR

 /tivit_oficial

 /tivotoficial

 /company/tivit

 /tivotoficial

