Cibersecurity Management 2024

RIMAC

Vulnerability Management Roadmap 2024

RIMAC

Infrastructure Scanning Cycles

Cloud Infrastructure
On Premise Infrastructure
PCI DSS
Cracking Credentials
Database

Application Scan Cycle

Web application scanning and API´s

Searching for secrets in internal repositories

Search for secrets

Public secrets

Ethical Hacking

Ethical Hacking of BIA Applications

Ethical Infrastructure Hacking

Baseline Monitoring Management Roadmap 2024

Onpremise

Cloud

The Baseline Monitoring and Vulnerability Management Plan helps us identify, assess, and track cybersecurity breach remediations to prevent potential threats and attacks.

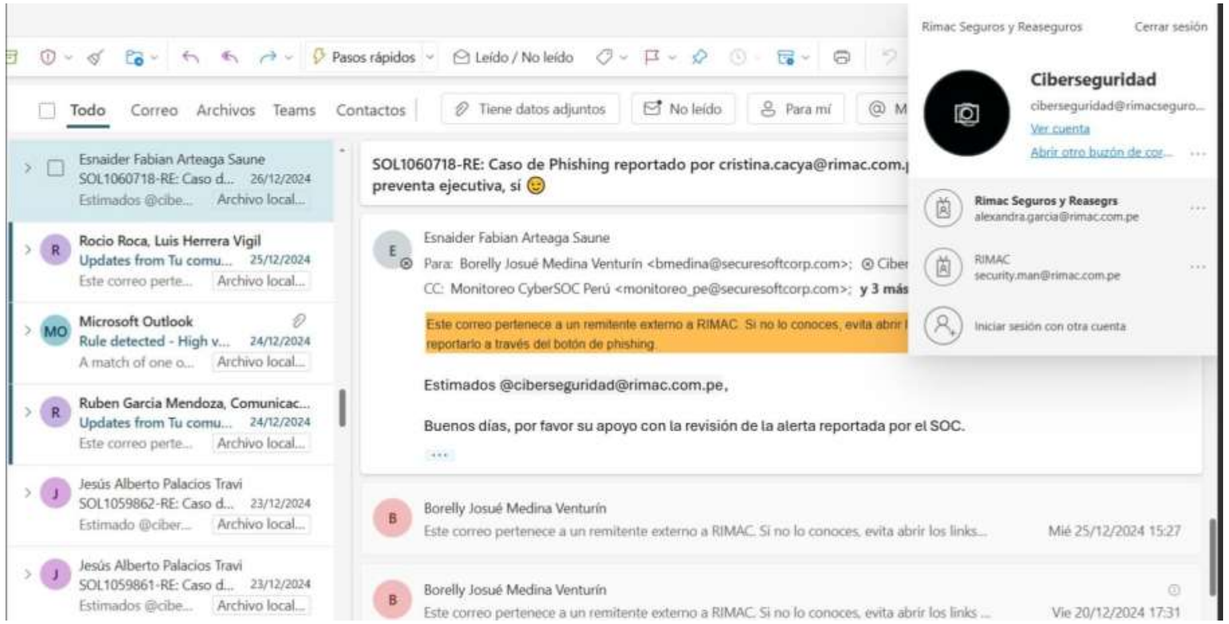
Cibersecurity drills

We also carry out cybersecurity drills to keep our employees alert and ensure that they can correctly identify different threats.

As presented in the example, a mass email is sent to all employees with a phishing simulation and those who cannot correctly identify it are sent an explanation email after that.

Cybersecurity Mailbox

At RIMAC we have an email that works as a mailbox to receive concerns and reports of cybersecurity cases in the organization. This email is ciberseguridad@rimac.com.pe



Cybersecurity Incidents Report

Upon receiving a report about a cybersecurity incident through the mailbox, the cybersecurity area conducts an investigation of the case. For example, in the case of phishing presented below, an analysis of the email is carried out to determine if it does indeed present a risk and at what level, as well as the actions to be taken.

De: Borelly Josué Medina Venturín <bmedina@securesoftcorp.com>
Enviado: miércoles, 25 de diciembre de 2024 15:27
Para: ciberseguridad@rimac.com.pe <ciberseguridad@rimac.com.pe>; CyberSOC RIMAC <cybersoc_rimac@securesoftcorp.com>
Cc: Monitoreo CyberSOC Perú <monitoreo_pe@securesoftcorp.com>; Soporte Secure Soft Perú <soporte@securesoftcorp.com>; Soporte Onsite Rimac <soporte_onsite_rimac@securesoftcorp.com>; SMARTFENSE <preport@livefense.com>
Asunto: RE: SOL1060718-RE: Caso de Phishing reportado por cristina.cacya@rimac.com.pe: Santa no te traerá un ascenso...la preventa ejecutiva, sí 😀

Estimado @CyberSOC RIMAC buen día,

Se realizó el análisis del correo en un ambiente seguro **Sandbox**

Conclusión del Análisis:

Posible campaña de spam publicitario: El correo parece ser parte de una campaña de spam publicitario que ofrece programas educativos de desarrollo profesional. El tono de detallada sobre la oferta hacen que este correo se asemeje más a un mensaje de marketing masivo que a una oferta legítima.

Acciones a Tomar - Securesoft	Realizar el bloqueo proactivo de las **IOC´s** maliciosa/sospechosa en todas las plataformas (Soporte) (previa confirmación)
Acciones a Tomar - Cliente	Revisar si los **IOC´s** pertenece a un proveedor o servicio, de ser el caso solicitar el bloqueo. (Cliente) Indicar a los usuarios finales que No deben ingresar credenciales y/o información personal en páginas no autorizadas. Evite hacer clic en enlaces o descargar archivos adjuntos de fuentes desconocidas o sospechosas. Eliminar el correo del buzón de las personas que recibieron dicho correo. Evitar el uso de las cuentas corporativas en páginas que no estén asociadas a las funciones de la empresa. NO hacer clic en hipervínculos de correos electrónicos de remitentes desconocidos. NO abrir correos si se desconoce el sender e inmediatamente remitirlo al área de ciber-seguridad para su posterior revisión.