

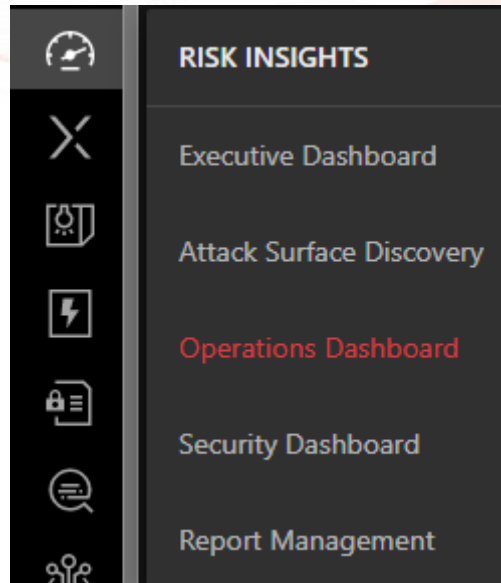


Risk Reduction Measures

Vision One

Departamento de Soporte Técnico
EDSI Trend Argentina

Paso 1: Nos tenemos que dirigir a Risk Insights>Operation Dashboard.



Paso 2: Dentro del módulo Operation Dashboard debemos dirigirnos al final de la página, donde nos encontraremos con Risk Reduction Measure. Esta función se encuentra en Preview pero nos da la información para realizar la remediación de nuestros riesgos.

RISK REDUCTION MEASURES ⓘ Last assessment: 2023-04-18 11:13:14 ⓘ [Alt-Risk Users/Devices](#)

From Medium risk 41 To Low risk Less than 30 Risk events to address 22 / All events [Select A Goal](#)

Risk factor: All [Apply](#)

Risk factor	Risk event	Most impacted... ⓘ	Real-time scor... ↓	Remediation steps
System confi...	Stale Azure AD Account	96	1	• Remove or disable the stale account (account that remains inactive for more than 180 days).
System confi...	Application Execution Check Disabled	30	1	• Enable Hypervisor-protected code integrity (HVCI). Learn More
Cloud app ac...	Risky Cloud App Access	59	1	• Avoid accessing the reported cloud app.
XDR detection	Early Indicators of Being Targeted by Ryuk Ransomware	1	Less than 1	• Investigate the event using the Workbench.
XDR detection	Potential Malicious Webshell Execution - No Device Direction	1	Less than 1	• Investigate the event using the Workbench.
Threat detec...	Malicious Download from Website	1 1	Less than 1	• Check event details on product management server.

Paso 3: Una vez elegido el riesgo que queremos remediar, dentro se nos dará una instrucción de cómo solucionarlo y nos mostrara a los Usuarios/Equipos que están afectados, es ira variando según el riesgo que queramos corregir.

STALE AZURE AD ACCOUNT

Risk Factor








System configuration

Remediation Steps

• Remove or disable the stale account (account that remains inactive for more than 180 days).

Complete remediation steps to lower the Risk Index. The Risk Index may take up to 24 hours to update.

Assets with Actionable Risk Events

Asset name	Latest risk score ↓	Data source / processor	Detected
>  Sofia	61	Azure AD	2023-04-16 21:00:00
>  Melina	61	Azure AD	2023-04-16 21:00:00
>  Marcos	60	Azure AD	2023-04-16 21:00:00
>  O365	60	Azure AD	2023-04-16 21:00:00
>  Ariadna	54	Azure AD	2023-04-16 21:00:00
>  EDSI	54	Azure AD	2023-04-16 21:00:00
>  Joel	50	Azure AD	2023-04-16 21:00:00

Paso 4: Ya realizada la tarea para remediar, esta va a tardar un tiempo en verse reflejada en nuestro índice de riesgo disminuyendo los puntos necesarios acorde la gravedad del riesgo.