Nuestra misión es ayudar a las empresas a obtener valor de sus datos no estructurados

Amenazas internas

Andres Julian Marin
Varonis Systems Engineer -

ACERCA DE VARONIS

- Comenzó a operar el año 2005
- Más de **4000** Clientes
- Soluciones de software para datos generados por humanos

AGENDA

- La anatomía de las brechas internas
- Brechas reales: estadísticas y ejemplos
- 6 consejos para disminuir las amenazas internas

LOS PASOS

Ingresar
(si es que ya no está ahí)

- Realizado a través del phishing o de ingenería social

Husmear

- Enumerar el acceso actual; intentar elevar
- ¿Alguien quiere tarjetas Visa?

Exfiltración

- Obtener los datos sin activar las alarmas

VARONIS

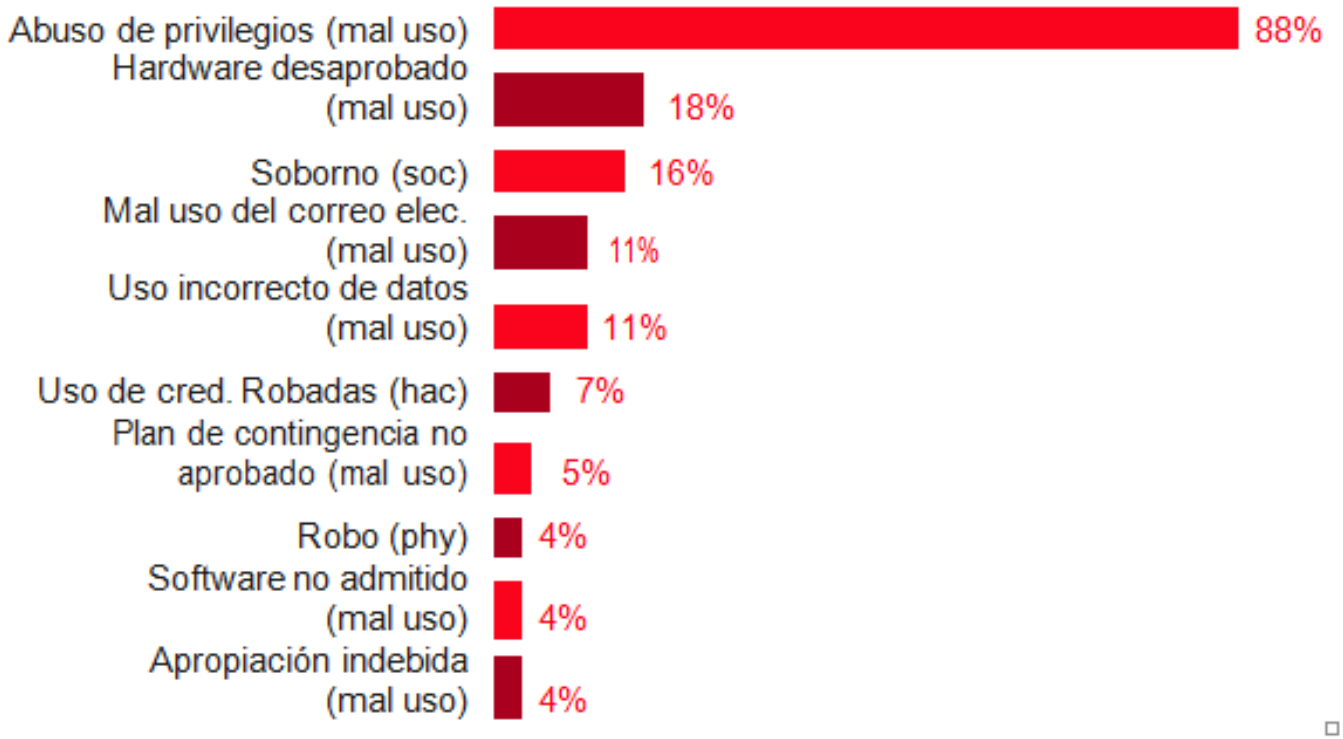
LAS CIFRAS

Imagen 43. El top 10 de las amenazas provocadas por errores (n=558)

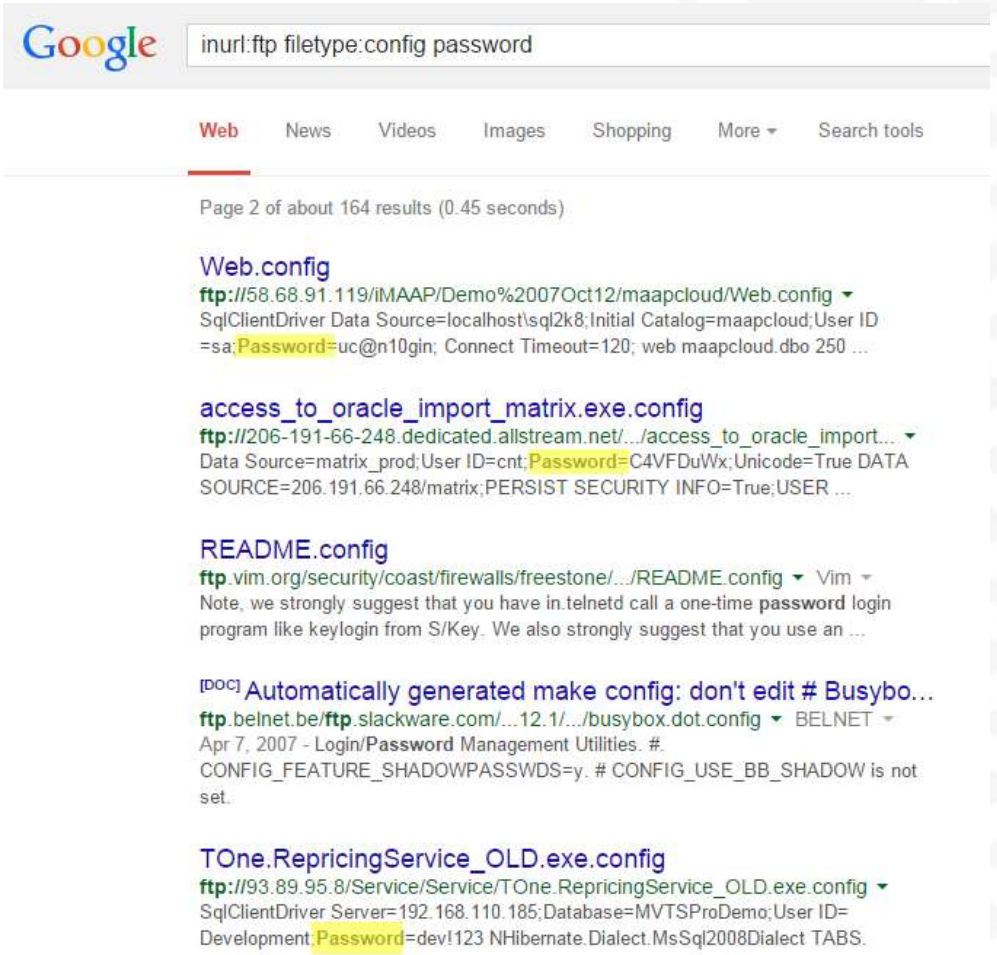
Imagen 44. El top de los activos afectados por errores (n=546)

ABUSO DE PRIVILEGIO

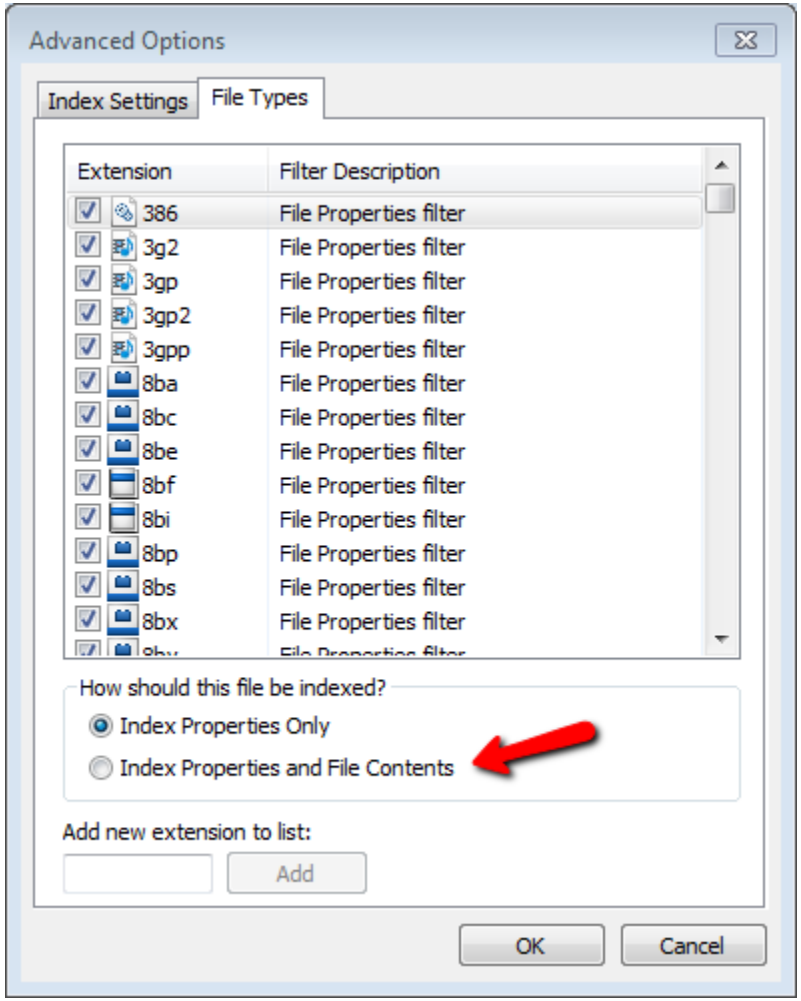
Imagen 30. El top 10 de las amenazas provocadas por el mal uso interno (n=153)

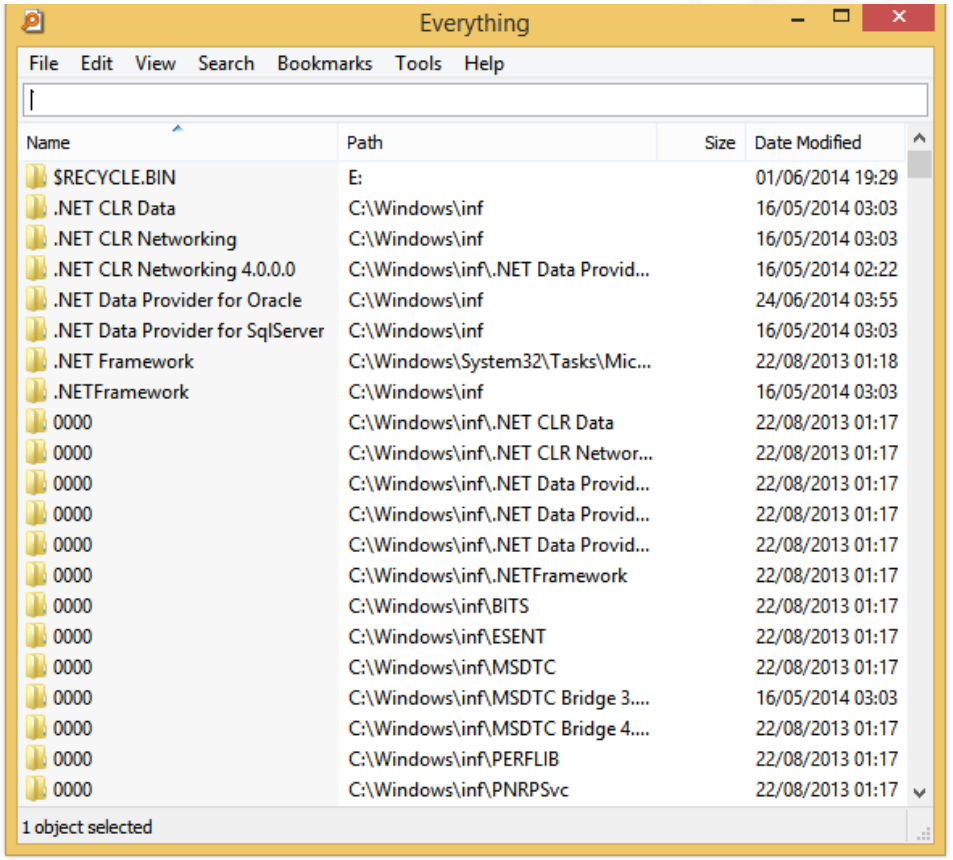


NUESTRO PEOR ENEMIGO



HUSMEAR DETRÁS DEL FIREWALL



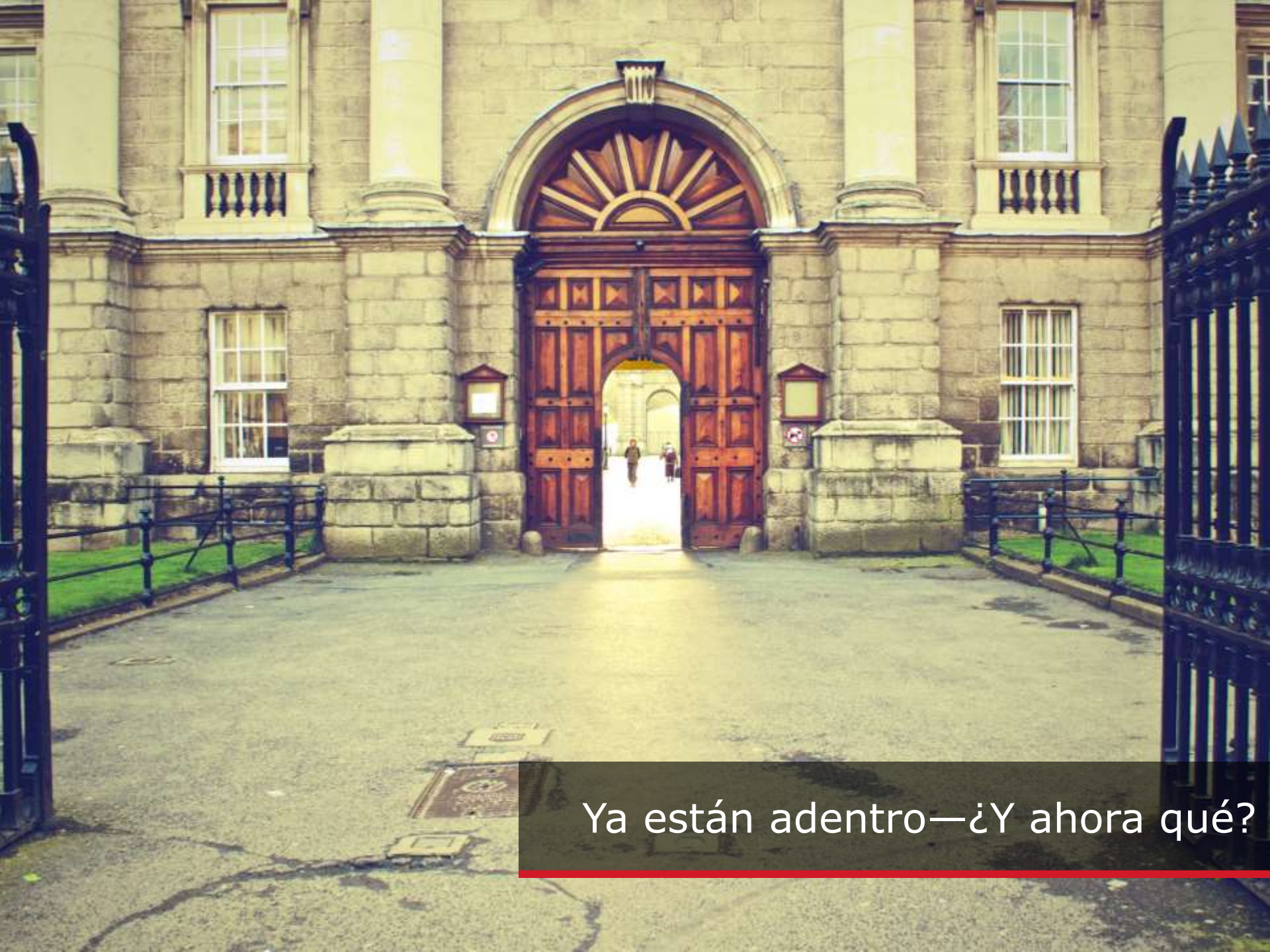


TARGET COMO BLANCO

- 40,000,000 archivos perdidos
- Muchas herramientas sofisticadas vigilando el perímetro (sindrome del caramelo)
- "[…] la vocera, Molly Snyder, dice que los intrusos ganaron acceso al sistema utilizando credenciales robadas de un vendedor"

Tweet

@Avivahl de Gartner dice que de haberse asesorado con analistas del comportamiento, se pudo haber prevenido una #Brechadedatos en Target


Ya están adentro—¿Y ahora qué?

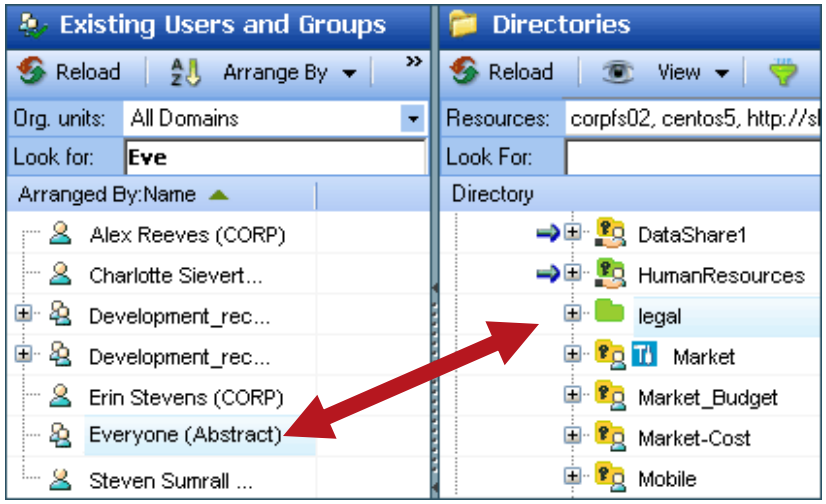
6 CONSEJOS DE MITIGACIÓN

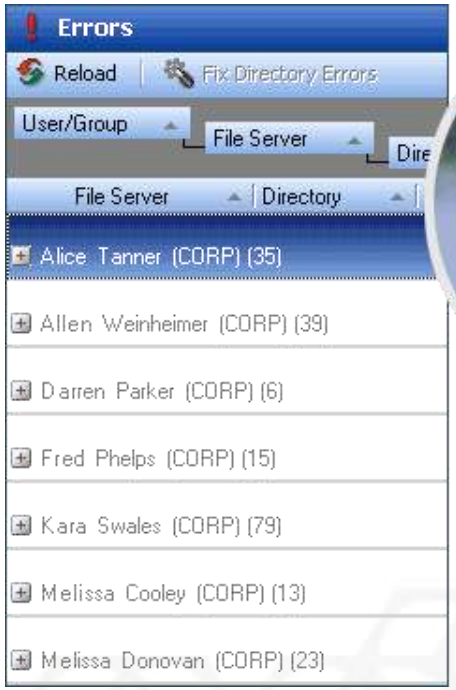
1. Elimine el acceso global
2. Elimine los permisos excesivos
3. Alerte las escaladas de privilegios
4. Alerte las desviaciones de comportamiento
5. Instale ~~panales de miel~~ trampas
6. Monitoree de cerca a las personas y los datos de alto riesgo

VARONIS

CONSEJO #1: ELIMINE EL ACCESO GLOBAL

- Localice a grupos como “Todos” y “Usuario autenticado” y reemplacelos por grupos de seguridad más cerrada
- ¿Cómo evito cortar el acceso legítimo?

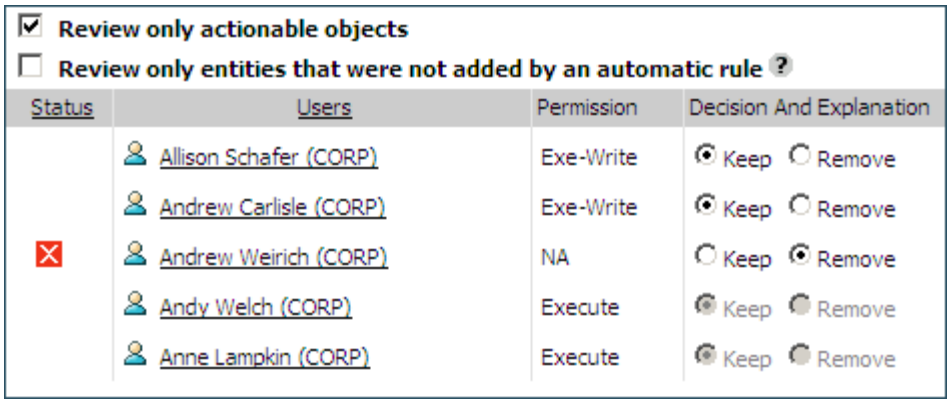




¡Alice Tanner perderá el acceso a los datos que ha estado utilizando!

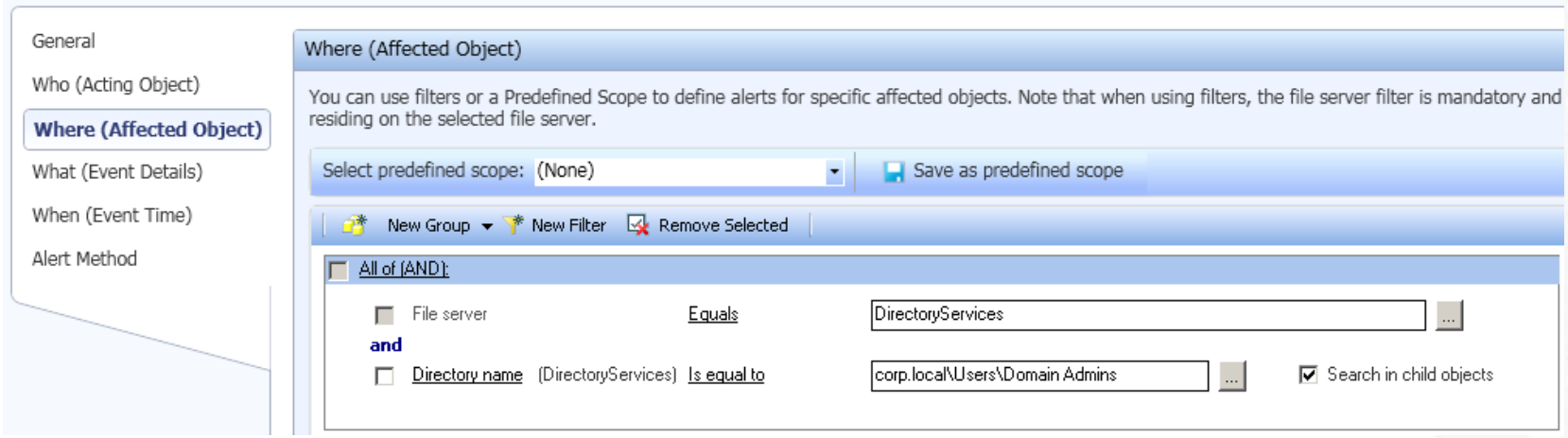
CONSEJO #2: ELIMINE LOS PERMISOS EXCESIVOS

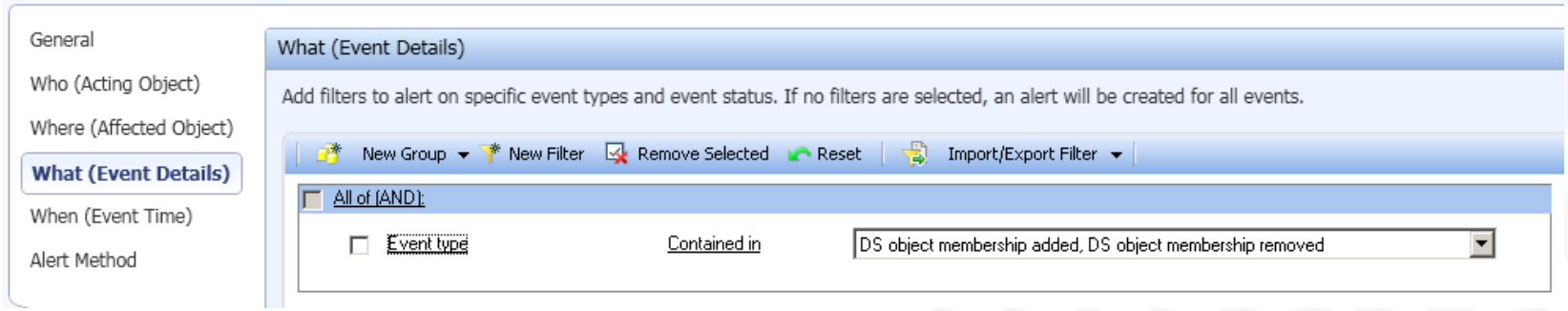
- ¡Gente *y* software!
- Descubra a qué información *prohibida* tiene acceso la gente
  - Recomendaciones como las de Amazon
- Acceso temporal de auto-expiración
- Revise los ~~derechos~~ permisos periódicamente



CONSEJO #3: ALERTE LAS ESCALADAS DE PRIVILEGIOS

- ¿Sabe cuándo alguien tiene acceso a la raíz?



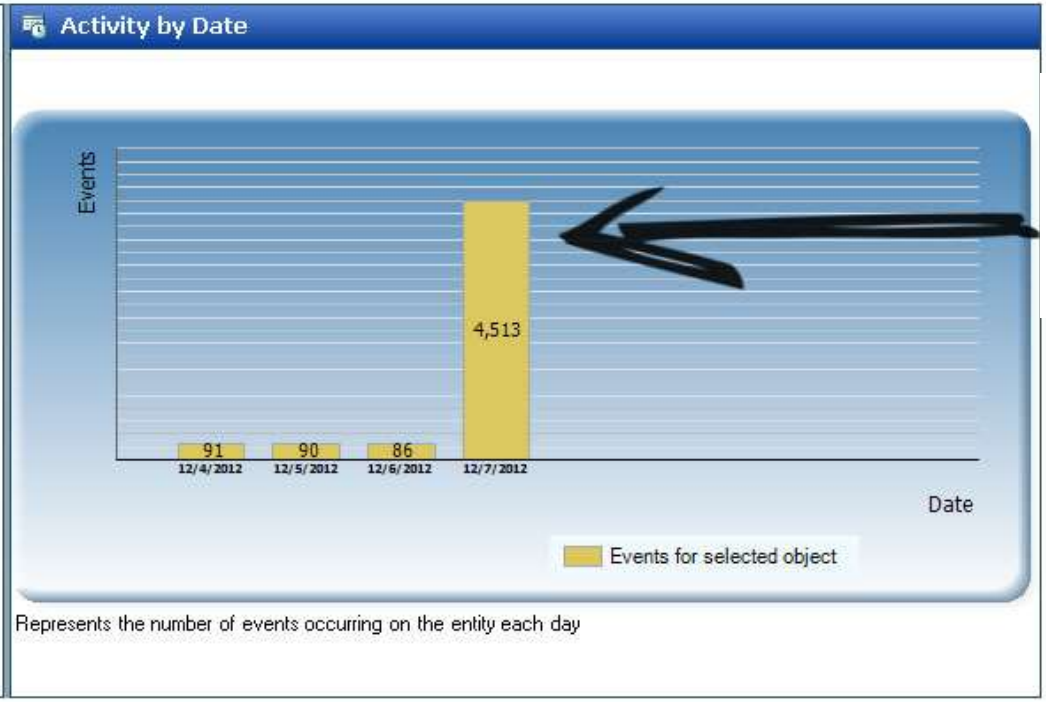


CONSEJO #4: ALERTE LAS DESVIACIONES DE COMPORTAMIENTO

- Aumento de actividad de comportamiento (Correo elect., archivos, acceso denegado)
- Monitoree la actividad fuera del horario de trabajo

Kara Swales

El usuario Kara Swales ha estado utilizando recursos en aumento hace 74 días, 937 veces por sobre su uso normal



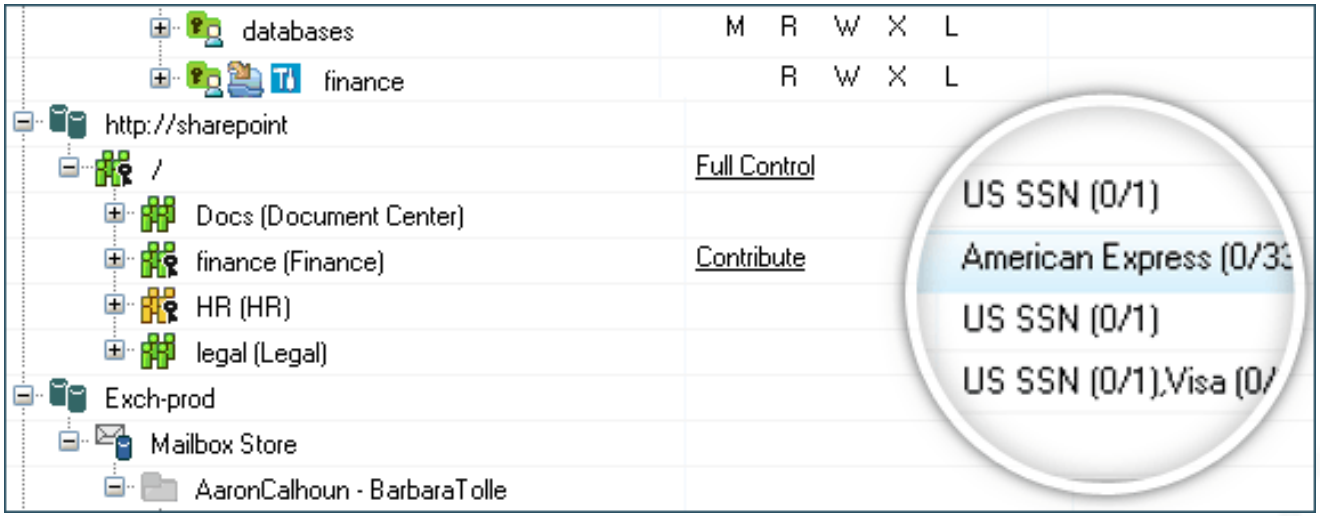
Alerte la actividad anómala

CONSEJO #5: INSTALE TRAMPAS ~~PANALES DE MIEL~~

- Configure una carpeta compartida que esté abierta para todos los usuarios
  - X:\Share\Payroll
  - X:\Share\Confidential
  - X:\Share\CEO
- Vea quién comete abuso de dicha carpeta

CONSEJO #6: MONITOREE A LAS PERSONAS Y DATOS DE ALTO RIESGO

- Alerte o envíe a cuarentena a los datos sensibles cuando aparezca en un lugar público
- Supervise a los administradores de raíz/dominio
- Supervise a los contratistas



¡Gracias!

Andres Julian Marin
Varonis Systems Engineer - Latin America and the Caribbean
amarin@varonis.com

Arturo Medina
Varonis Sales Rep (Mexico y Puerto Rico)
amedinaramos@varonis.com

Evaluacion de amenazas gratuita
http://hub.varonis.com/evaluation-es