7ma Jornada de Ciberseguridad de la Universidad Nacional de Colombia

2026

Detectando lo que las reglas y las líneas base no ven: UEBA basado en series de tiempo

Aplicación interactiva

Resumen

Las series de tiempo detectan mucho más actividad maliciosa que los métodos tradicionales evaluados. Este trabajo trata la actividad de cada usuario como una **serie de tiempo con ciclo semanal**: un modelo SARIMA por usuario y contador estima cuánto es normal cada día y el centro de operaciones de seguridad (SOC) revisa los mayores aumentos. En CERT r4.2 (1.000 usuarios, 70 incidentes simulados), con 10 alertas diarias, SARIMA identifica **240 días maliciosos: 47 % más que la línea base estática por usuario y 6,7 veces los de la regla global**, y cubre 67 de 70 incidentes. Tiene potencial para reducir el trabajo de los equipos de seguridad y la fatiga de alertas: el analista revisa 14 alertas por cada día malicioso encontrado, en vez de 21.

Propósito

Evaluar si incorporar la historia y el ciclo semanal de cada usuario permite identificar más actividad maliciosa con el mismo número de alertas para revisar.

> **¿Es normal que *este* usuario haga *esto*, *este día* y con *esta* intensidad?**

Contexto e importancia

- **Las firmas no bastan:** detectan lo conocido (NIST SP 800-94), pero una persona puede usar credenciales válidas para acciones maliciosas (MITRE ATT&CK T1078): lo anómalo es el patrón.
- **Las reglas de umbral generan ruido.** Un analista de SOC lo resume así: "Sabemos que el 99 % de las alarmas que generamos son falsos positivos, pero aun así tenemos que revisarlas" (Alahmadi et al., 2022; traducción propia). Con demasiadas alertas se pierden ataques reales (Hassan et al., 2019).
- **La actividad es una serie de tiempo**, como el tráfico de red (Brutlag, 2000; Rajchel et al., 2020): en estos datos, el 94 % de las series con actividad tiene ciclo semanal.

¿Qué ve que una regla no ve?

- **Robo de datos antes de renunciar:** el modelo de cada usuario capta el aumento de memorias USB. SARIMA encuentra 167 de 861 días maliciosos; la línea base estática, 86, y la regla global, 18 (casos: 28, 25 y 2 de 30).
- **Sesiones fuera de 07:00 a 19:00, raras para ese usuario:** señal principal en 19 de las 30 fugas a WikiLeaks (SARIMA y la línea base estática las detectan todas; la regla global, 7).
- **Lo que no ve:** lo que ya es costumbre del usuario (un robo con USB fuera de horario que la regla global sí detecta) y las acciones sin cambio de volumen. Requiere complementarse con otros controles.

Conclusiones

- **Las series de tiempo superan con claridad a los métodos tradicionales evaluados:** con 10 alertas diarias, los tres modelos detectan entre 35 % y 47 % más días maliciosos que la línea base estática, y SARIMA 6,7 veces los de la regla global.
- **El ritmo semanal aporta si se estima bien:** SARIMA y un perfil por día de la semana superan a la estática (240 y 210 días frente a 163); copiar la semana anterior no basta (93).
- **Menos alertas en vano para el SOC:** cada día malicioso encontrado cuesta 14 alertas revisadas en vez de 21, lo que ayuda a reducir la fatiga de alertas. CERT es sintético: falta validarlo en una organización real.

Glosario

Día malicioso: día de un usuario con alguna acción de un incidente (986 en la prueba); un incidente se detecta si alguno de sus días entra en las alertas.
UEBA: análisis que aprende lo normal de cada usuario y avisa cuando se aparta.
Serie de tiempo: un dato medido día tras día, como las memorias USB conectadas.
Regla global: el mismo umbral para todos los usuarios de la organización.
Línea base estática: promedio y variación de cada usuario, recalculados cada mes; un solo límite.
Regla ingenua: supone que hoy será igual al mismo día de la semana anterior.
Perfil semanal: promedio de cada usuario para cada día de la semana.
ARIMA: pronóstico con los días anteriores, sin ciclo semanal.
SARIMA: versión estacional de ARIMA: incorpora un ciclo de siete días y actualiza la expectativa con la historia observada; espera más actividad un lunes que un domingo.
SARIMAX + pares: SARIMA que además mira la actividad de su departamento.

Método

1. Registros como los que centraliza un SIEM: 32,8 millones de eventos de sesiones, USB, archivos, correo y web

2. Contadores diarios 9 por usuario, en escala log(1 + conteo)

3. Patrón esperado SARIMA semanal por usuario y contador, reentrenado cada mes (ciclo semanal en el 94 % de las series)

4. Cola de revisión los 10 usuarios con mayor aumento sobre lo esperado, cada día

Cómo se alerta: las comparaciones usan la cola diaria (paso 4). El **límite del 99 %**, el valor que un día normal de ese usuario no debería superar más de 1 vez de cada 100 en ese contador (en la prueba, 2 a 8 de cada 1.000), marca los círculos de la Figura 1. **Diseño:** entrenamiento hasta el 9 de junio de 2010, sin incidentes; prueba hasta el 16 de mayo de 2011. Las series casi vacías (37 % de los ajustes) usan la media del usuario.

Resultados

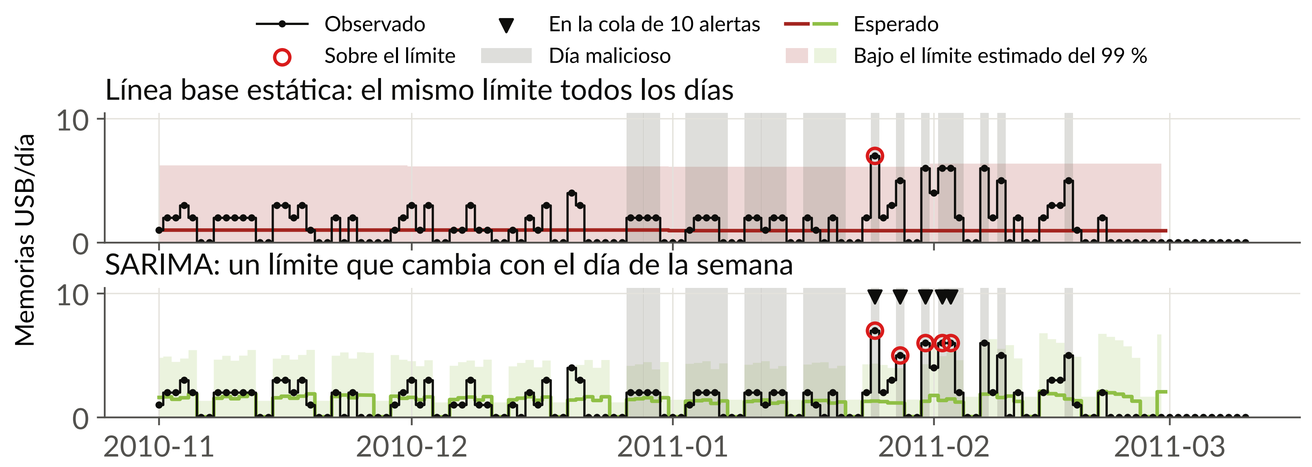


Figura 1. Robo de datos antes de renunciar (empleado IKR0401), uno de los 3 robos que SARIMA prioriza y que ni la regla global ni la línea base estática priorizan con 10 alertas diarias. Círculos: días sobre el límite por contador; triángulos: días que entraron en la cola de 10 alertas. En memorias USB, SARIMA marca 5 de los 28 días maliciosos y los 5 entran en su cola; la línea base estática marca 1, que no entra en la suya.

Detector	Días maliciosos detectados (de 986)	Incidentes detectados (de 70)	Aciertos por cada 100 alertas
Regla global	36	17/70	1,1
Línea base estática	163	64/70	4,8
Regla ingenua	93	46/70	2,7
Perfil semanal (control)	210	**67/70**	6,2
ARIMA	220	**67/70**	6,5
SARIMA	**240**	**67/70**	**7,0**
SARIMAX + pares	234	65/70	6,9

Tabla 1. Con 10 alertas diarias y reentrenamiento mensual. Arriba, métodos que no estiman el patrón de cada usuario en el tiempo; abajo, los que lo estiman con su historia y los superan. El perfil semanal es un control más simple: con 20 alertas diarias, 322 días; SARIMA, 300.

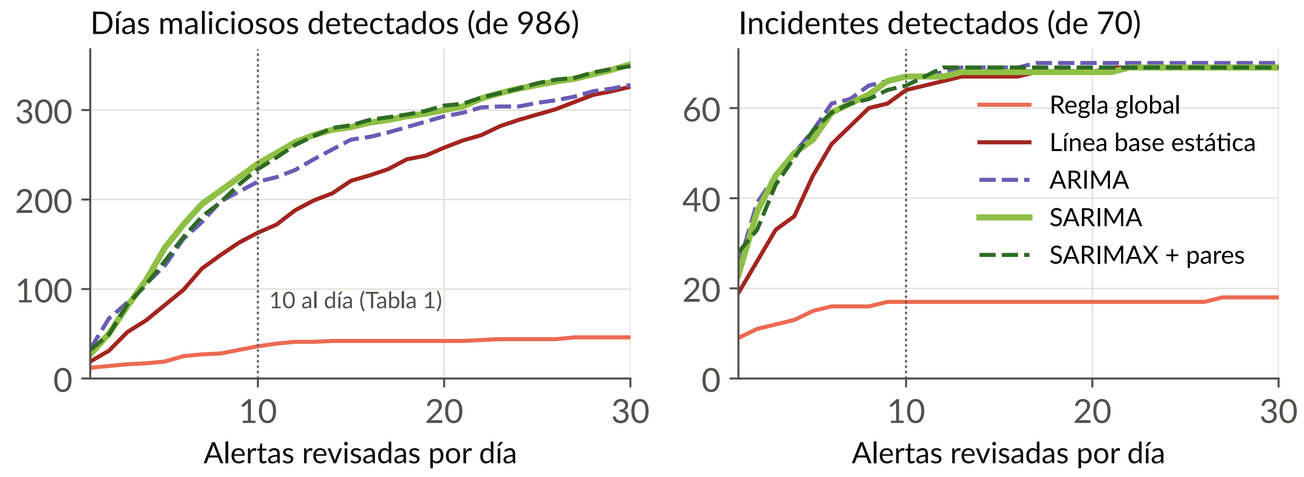


Figura 2. Con 1 a 30 alertas diarias, los tres modelos de series de tiempo detectan más días maliciosos que la línea base estática, sobre todo con pocas alertas (hasta +78 %, con 5); la regla global no pasa de 18 incidentes.

Hallazgos clave

- **47 % más y 6,7 veces más con las mismas alertas:** con 10 alertas diarias, SARIMA identifica 240 de 986 días maliciosos; la línea base estática, 163, y la regla global, 36. Diferencia con la estática: 77 días (intervalo de confianza del 95 %: 43 a 117).
- **Más aciertos por alerta:** 7,0 de cada 100 alertas de SARIMA corresponden a días maliciosos, frente a 4,8 de la línea base estática y 1,1 de la regla global.
- **La línea base estática exige casi el doble:** necesita 18 alertas diarias para lograr los 240 días de SARIMA con 10.
- **Un umbral fijo satura:** con su límite del 99 % y sin tope diario, la regla global dispara 108 alertas al día y SARIMA, 18,5 (falsas: 98 y 95 de cada 100).
- **Estable sin reentrenar:** con parámetros fijos, SARIMA mantiene 233 días (la estática, 171); ARIMA cae a 123.

Referencias

Alahmadi, B. A. et al.: 99% False Positives: A Qualitative Study of SOC Analysts' Perspectives on Security Alarms. USENIX Security (2022).

Brutlag, J. D.: Aberrant Behavior Detection in Time Series for Network Monitoring. USENIX LISA (2000).

Hassan, W. U. et al.: NoDoze: Combatting Threat Alert Fatigue with Automated Provenance Triage. NDSS (2019).

Lindauer, B.: Insider Threat Test Dataset. Carnegie Mellon University (2020). doi:10.1184/R1/12841247

Rajchel, B. et al.: Temporal Behavior in Network Traffic as a Basis for Insider Threat Detection. IEEE SSCI (2020).

Scarfone, K., Mell, P.: Guide to Intrusion Detection and Prevention Systems. NIST SP 800-94 (2007).

Tashman, L. J.: Out-of-sample tests of forecasting accuracy. Int. J. Forecasting 16(4) (2000).

Autor(es):

Alejandro Higuera Castro
Departamento de Estadística
Facultad de Ciencias
Universidad Nacional de Colombia

Organiza:

Universidad Nacional de Colombia
Semillero de Investigación Uqbar
Grupo de investigación Tlön

UNIVERSIDAD NACIONAL DE COLOMBIA