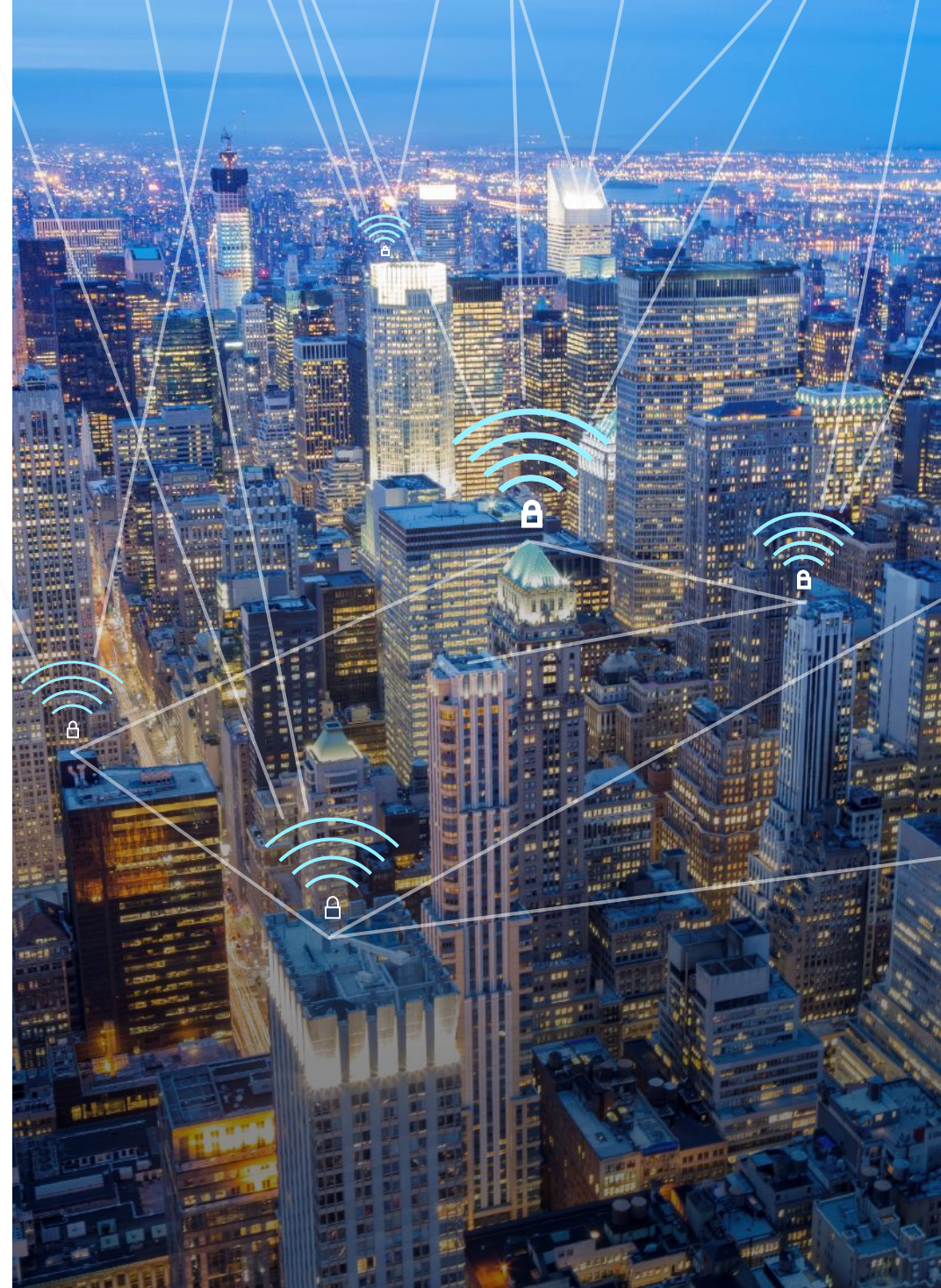




# Microsoft Security

Simplifique y refuerce la seguridad con las soluciones de seguridad de Microsoft



# La tecnología obsoleta aumenta los riesgos

- Amenazas sofisticadas
- La tecnología antigua genera barreras
- El mantenimiento impide la innovación

## TECH INSIDER

### Las 21 vulneraciones de datos de 2018

PAIGE LESKIN

12 DE DICIEMBRE DE 2018, 12:00 AM



MARRIOTT

500 millones de clientes afectados por el ataque informático a Marriott



CATHAY PACIFIC

9.4 millones de clientes; 860,000 números de pasaporte, 245,000 tarjetas de identidad

**TICKETFLY**

27 millones de datos personales de clientes robados




SingHealth


1.5 millones de IIP e historiales médicos de pacientes comprometidos


# Es vital adoptar una postura de seguridad fuerte

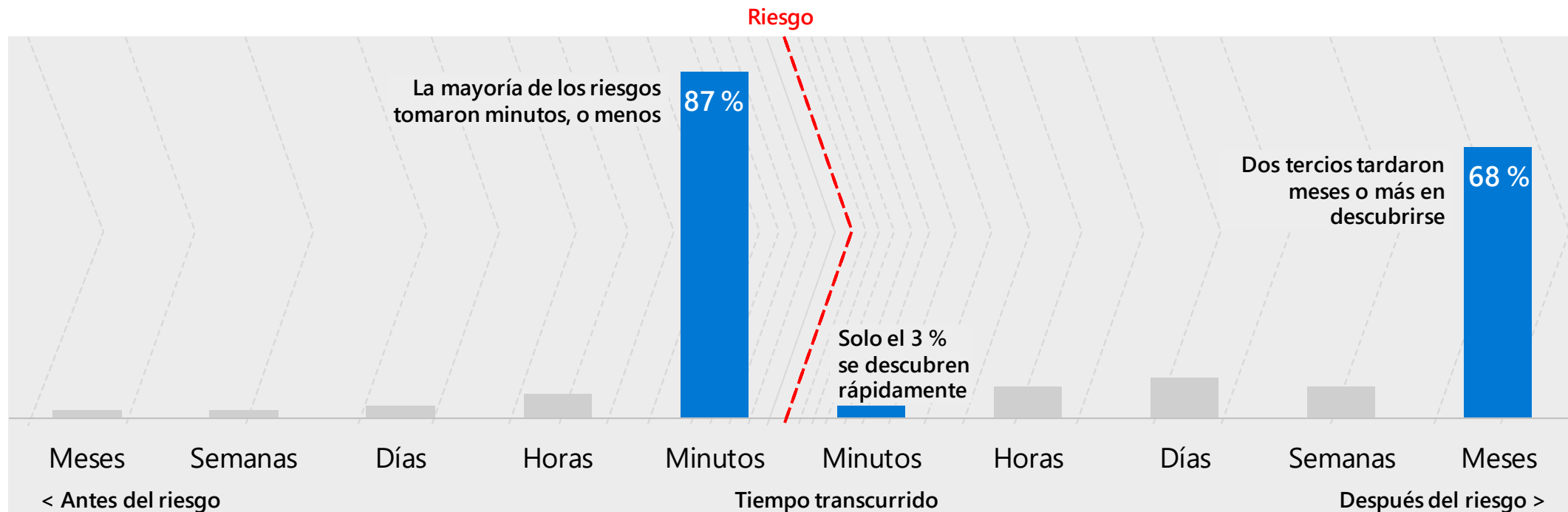
En solo minutos, una vulneración puede dañar la confianza de los clientes para siempre

 **4,200 millones**  
de registros  
robados por  
hackers en 2016

 El **20 %**  
de organizaciones  
pierden clientes  
durante un ataque

 El **30 %**  
de organizaciones  
pierden ingresos  
durante un ataque

 El **28 %**  
de los ataques se  
originan dentro,  
más difícil de detectar



Verizon Data Breach Investigations Report 2018

Fuentes: Risk Based Security Report, 2017; Cisco 2017 Annual Cybersecurity Report; Juniper Research Cybercrime & The Internet of Threats, 2017; Verizon Data Breach Investigations Report 2018

# Seguridad integrada de Microsoft

Simplifique y refuerce la seguridad con las soluciones de seguridad de Microsoft



## Administración de identidad y acceso

Proteja las identidades de los usuarios y controle el acceso a recursos valiosos de acuerdo con el nivel de riesgo del usuario



## Protección contra amenazas

Proteja contra amenazas avanzadas y recupérese rápidamente cuando sea atacado



## Protección de la información

Asegúrese de que los documentos y los correos electrónicos sean vistos solo por las personas autorizadas



## Administración de seguridad

Obtenga visibilidad y control de herramientas de seguridad

# Seguridad integrada de Microsoft

Simplifique y refuerce la seguridad con las soluciones de seguridad de Microsoft



**Administración de identidad y acceso**

Proteja las identidades de los usuarios y controle el acceso a recursos valiosos de acuerdo con el nivel de riesgo del usuario

Reduzca los costos con una solución integrada



**Protección contra amenazas**

Proteja contra amenazas avanzadas y recupérese rápidamente cuando sea atacado

Proteja los entornos híbridos de forma efectiva



**Protección de la información**

Asegúrese de que los documentos y los correos electrónicos sean vistos solo por las personas autorizadas

Adopte la presencia de seguridad más grande y más confiable del mundo



**Administración de seguridad**

Obtenga visibilidad y control de herramientas de seguridad

# Administración de identidad y acceso

Antes de otorgar acceso a las aplicaciones y a los datos demuestre que los usuarios están autorizados y seguros



**Proteja en la  
puerta principal**



**Simplifique el acceso  
a dispositivos  
y aplicaciones**



**Proteja sus  
credenciales**

# Protección contra amenazas

Proteja contra ataques avanzados; detecte y responda rápidamente si la seguridad se ve comprometida



## Proteja

las organizaciones contra  
ciberataques avanzados



## Detecte

actividades maliciosas



## Responda

rápidamente a las  
amenazas

# Protección de la información

Proteja los datos confidenciales en todo el ciclo de vida, dentro y fuera de la organización



**Detectar**



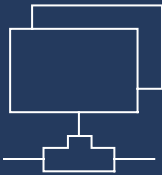
**Clasificar**



**Proteger**



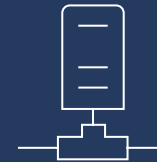
**Monitorear**



**DISPOSITIVOS**



**NUBE**



**EN LAS INSTALACIONES**



# Administración inteligente de la seguridad

Integración de seguridad completa con Microsoft Intelligent Security Graph



# Seguridad integrada de Microsoft

Aprovechando las tecnologías líderes del sector para una protección de 360°



## Administración de identidad y acceso

Azure Active Directory  
Conditional Access  
Windows Hello  
Windows Credential Guard



## Protección contra amenazas

Advanced Threat Analytics  
Windows Defender Advanced Threat Protection  
Office 365 Advanced Threat Protection  
Office 365 Threat Intelligence



## Protección de la información

Azure Information Protection  
Office 365 Data Loss Prevention  
Windows Information Protection  
Microsoft Cloud App Security  
Office 365 Advanced Security Mgmt.  
Microsoft Intune



## Administración de seguridad

Azure Security Center  
Office 365 Security Center  
Windows Defender Security Center



*“Azure proporciona la capacidad de mejorar el análisis de los riesgos del cambio debido al cambio climático a un nuevo nivel”.*

*– Robin Johnson: CIO – Munich Re*



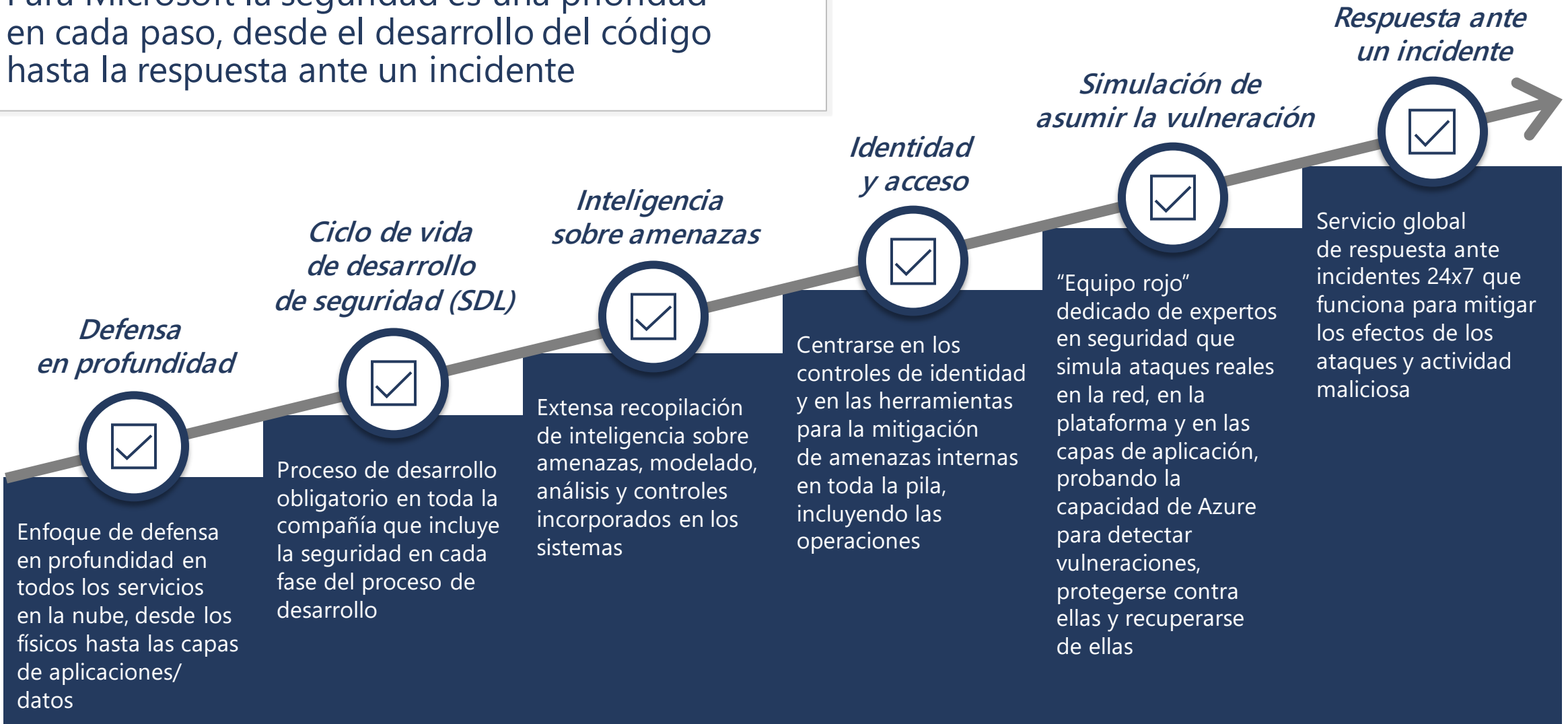
# Próximos pasos



**Para obtener más información sobre las soluciones de seguridad de Microsoft, comuníquese con su asociado de Microsoft.**

# Prácticas de seguridad

Para Microsoft la seguridad es una prioridad en cada paso, desde el desarrollo del código hasta la respuesta ante un incidente



# Inteligencia integrada y análisis avanzado



## Inteligencia sobre amenazas

Busca elementos maliciosos conocidos usando la inteligencia global sobre amenazas de Microsoft



## Detección de anomalías

Usa perfiles estadísticos para construir líneas de referencia históricas  
Alerta sobre desviaciones que pueden indicar un posible origen de ataque



## Análisis de comportamiento

Busca patrones conocidos y comportamientos maliciosos



## Asociados

Integra alertas de soluciones de asociados, como firewalls y antimalware



## Fusión

Combina eventos y alertas provenientes de la cadena de ataque para mapear la cronología del ataque



Con tecnología de Microsoft Intelligent Security Graph

# Detectar amenazas en la cadena de ataque



## Objetivo y ataque

## Instalar y vulnerabilidad de seguridad

## Exponer la vulneración

Ataques entrantes de fuerza bruta RDP, SSH, SQL y más  
Ataques de aplicación y DDoS (asociados WAF)  
Detección de intrusos (asociados NG Firewall)

Malware en memoria e intentos de vulnerar  
Ejecución de proceso sospechoso  
Movimiento lateral  
Reconocimiento interno

Comunicación con un IP malicioso conocido (filtración de datos o comando y control)  
Uso de recursos en peligro para montar más ataques (examen saliente de puerto, ataques de fuerza bruta RDP/SSH, DDoS y spam)

# Centrarse en las amenazas más críticas

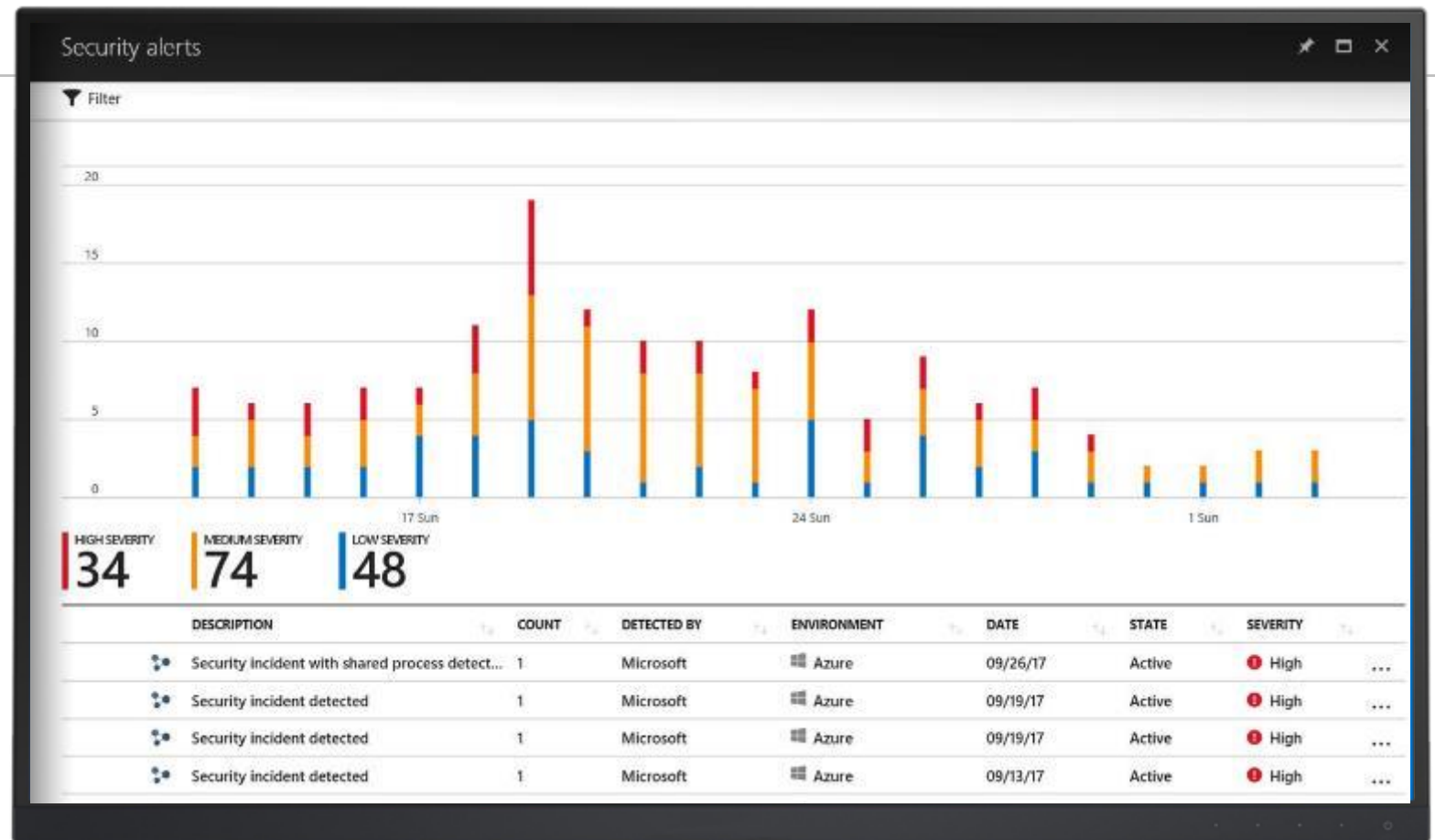


## Obtener alertas de seguridad por prioridad

- Detalles sobre las amenazas detectadas y recomendaciones

## Detectar amenazas en la cadena de ataque

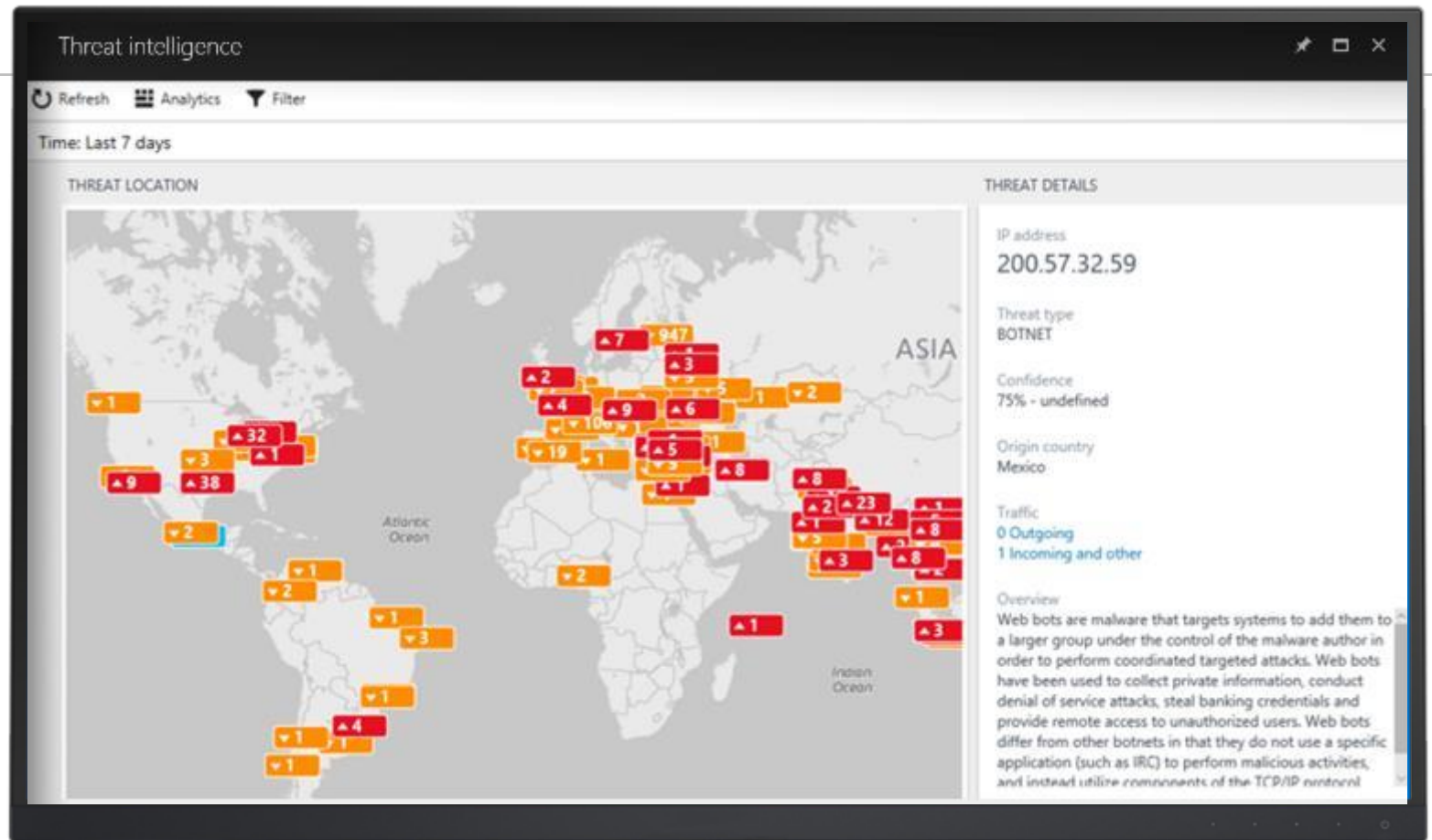
- Las alertas que cumplen con patrones de cadena de ataque se juntan en un solo incidente





# Obtener recomendaciones valiosas sobre los atacantes

- Visualizar el origen de los ataques con un mapa interactivo
  - Analizar datos de las computadoras y registros de firewalls
- Obtener recomendaciones mediante informes de amenazas
  - Objetivos, tácticas y técnicas conocidos del atacante

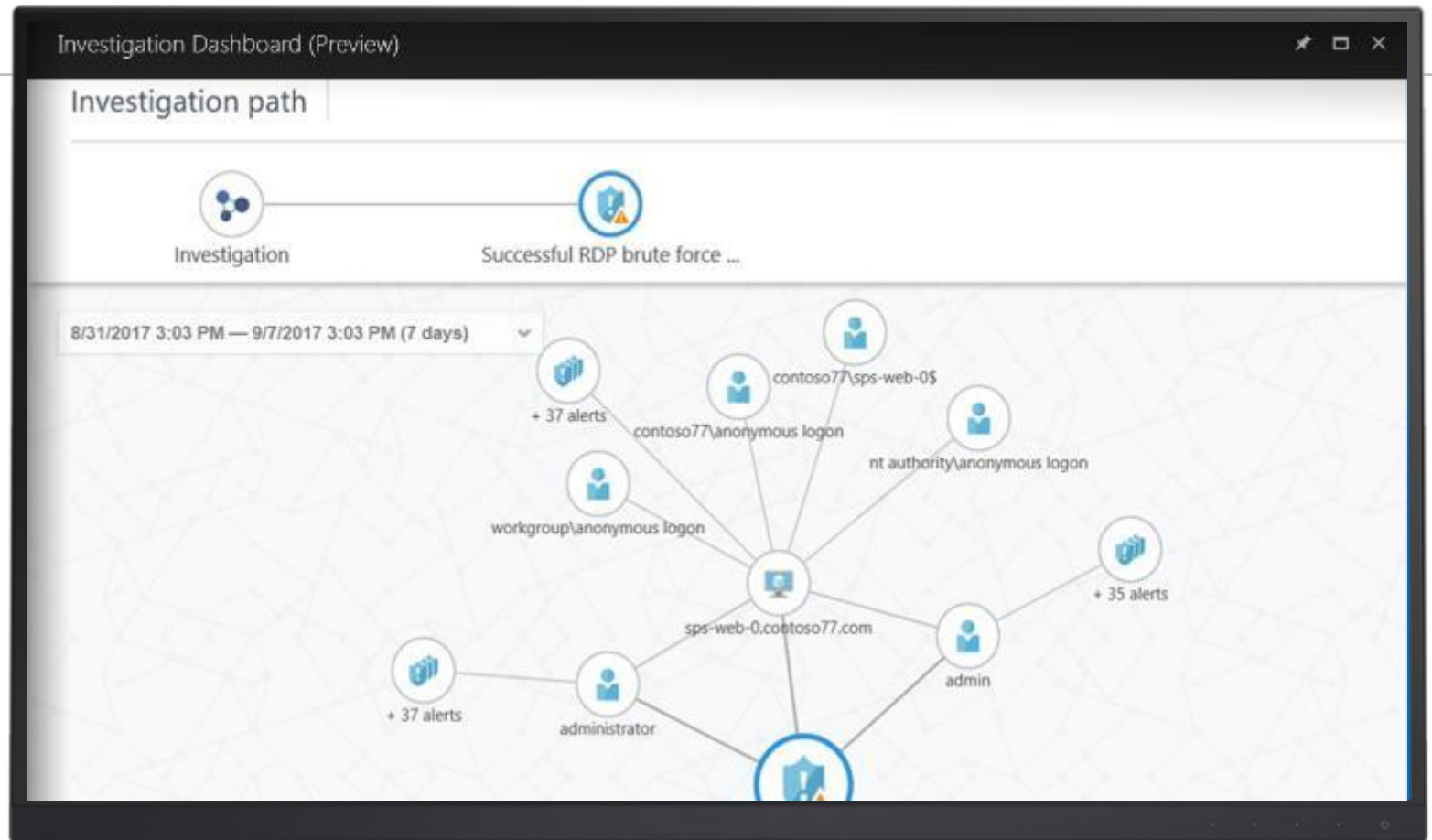


# Simplificar las operaciones e investigación de seguridad



## Evaluar rápidamente el alcance y el impacto de un ataque

- Experiencia interactiva para explorar enlaces entre alertas, computadoras y usuarios
- Uso predefinido o consultas ad hoc para un examen más profundo



# Responder rápidamente a las amenazas



## Automatizar y organizar flujos de trabajo de seguridad comunes

- Crear cuadernos de estrategias con integración de Azure Logic Apps
- Desencadenar flujos de trabajo a partir de una alerta para activar acciones condicionales



## Flujos de trabajo comunes

- Dirigir alertas a un sistema de tickets
- Obtener más información
- Aplicar más controles de seguridad
- Pedir a un usuario que valide una acción
- Bloquear una cuenta de usuario sospechosa
- Restringir el tráfico desde una dirección IP