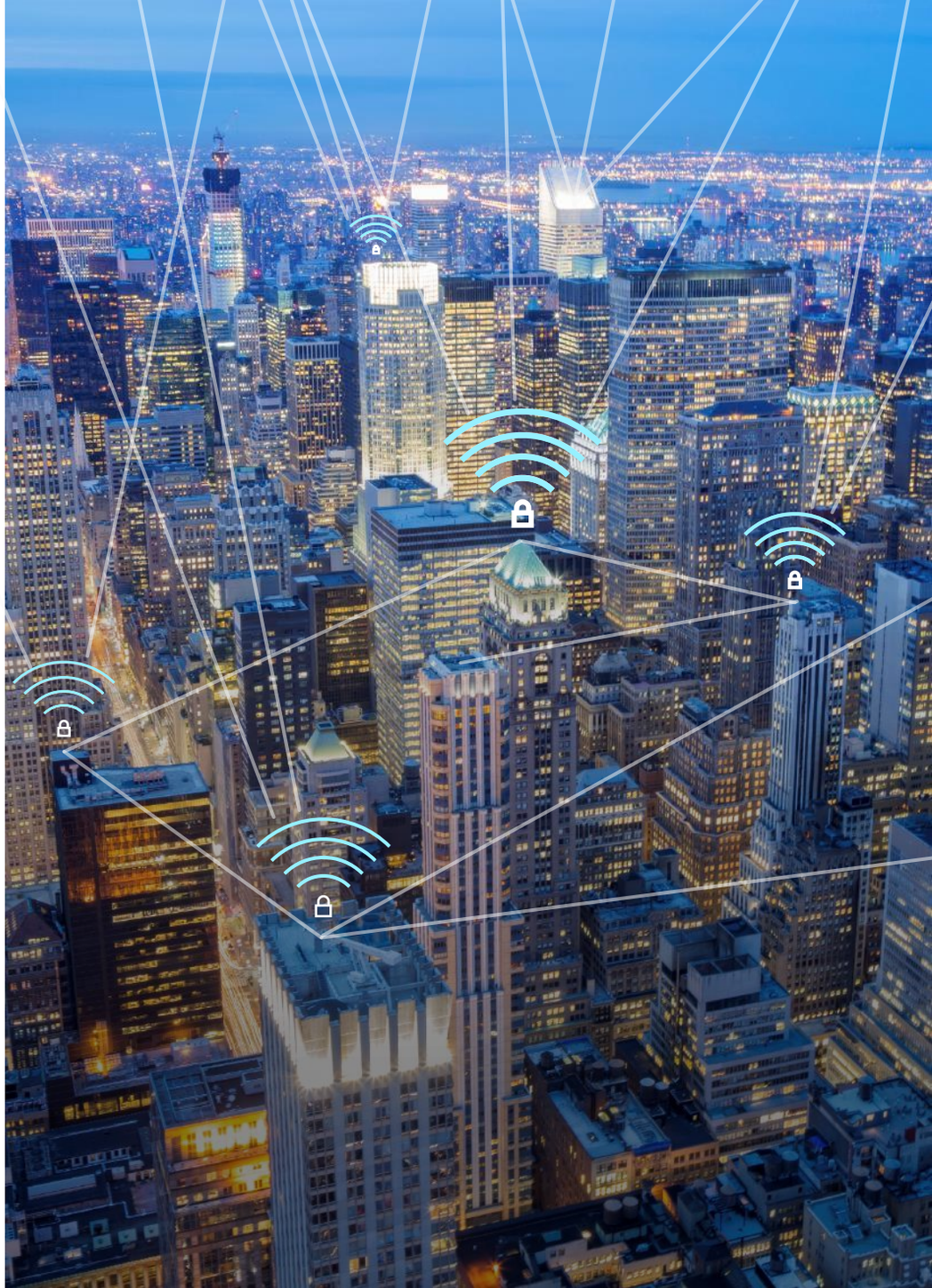
Microsoft

Microsoft Security

Simplify and fortify security with Microsoft Security solutions

SATALYST



Aging technology increases risks

- Sophisticated threats
- Legacy tech creates barriers
- Maintenance impedes innovation

Between January and October 2020, **730 publicly disclosed events** resulted in over **22 billion records exposed**. **35% of breaches** analysed were **caused by ransomware** attacks, resulting in tremendous financial cost, while **14.4%** of breaches were the **result of email compromises**.

18,358 new Common Vulnerabilities and Exposures (CVEs) were reported in 2020, representing a 6% increase from 2019 and a 183% increase from 2015. From 2015 to 2020, the number of reported CVEs increased at an annual percentage growth rate of 36.6%

Over 35% of all zero-day flaws exploited were browser vulnerabilities in Google Chrome, Mozilla Firefox, Internet Explorer and Microsoft Edge.

In 2020, **18 ransomware groups** were operating leak websites that name and shame victims to secure ransom demands.

Source: Tenable’s 2020 Threat Landscape Retrospective

A strong security posture is critical

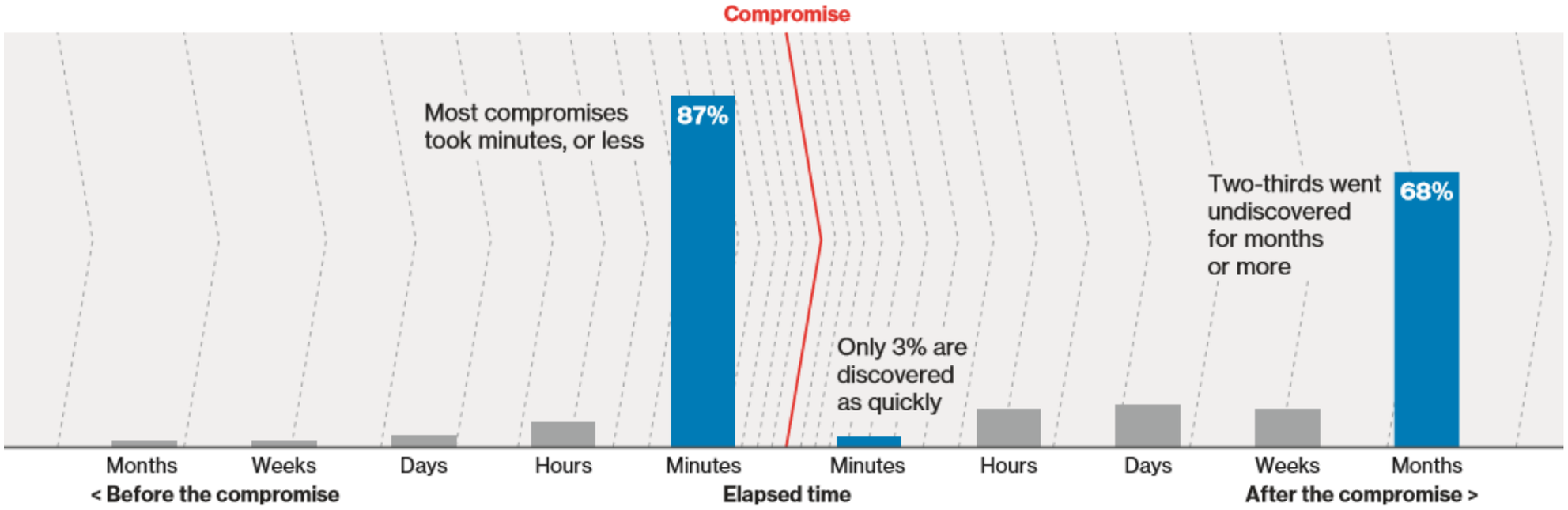
In just minutes, a breach can damage customer trust for a lifetime

4.2B
records stolen by hackers in 2016

20%
of organizations **lose customers** during an attack

30%
of organizations **lose revenue** during an attack

28%
of attacks **come from the inside** – harder to detect



Verizon Data Breach Investigations Report 2018

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

Microsoft integrated security

Simplify and fortify security with Microsoft Security solutions

Identity and access management

Protect users' identities and control access to valuable resources based on user risk level

Threat protection

Protect against advanced threats and recover quickly when attacked

Information protection

Ensure documents and emails are seen only by authorized people

Security management

Gain visibility and control over security tools

Microsoft integrated security

Simplify and fortify security with Microsoft Security solutions

Identity and access management

Protect users' identities and control access to valuable resources based on user risk level

Threat protection

Protect against advanced threats and recover quickly when attacked

Information protection

Ensure documents and emails are seen only by authorized people

Security management

Gain visibility and control over security tools

Reduce costs with an integrated solution

Secure hybrid environments effectively

Employ the world's largest and most trusted security presence

Identity & Access Management

Prove users are authorized and secure before granting access to apps and data

Protect at the front door

Simplify access to devices and apps

Safeguard your credentials

Threat protection

Protect against advanced attacks; detect and respond quickly if breached

Protect
organizations from advanced cyber attacks

Detect
malicious activities

Respond
to threats quickly

Information protection

Protect sensitive data throughout the lifecycle – inside and outside the organization

Detect

Classify

Protect

Monitor

DEVICES

CLOUD

ON PREMISES

Intelligent security management

Comprehensive security integration with the Microsoft Intelligent Security Graph

Microsoft integrated security

Leveraging industry-leading technologies for 360° protection

Identity and access management

Azure Active Directory

Conditional Access

Windows Hello

Windows Credential Guard

Threat protection

Advanced Threat Analytics

Windows Defender Advanced Threat Protection

Office 365 Advanced Threat Protection

Office 365 Threat Intelligence

Information protection

Azure Information Protection

Office 365 Data Loss Prevention

Windows Information Protection

Microsoft Cloud App Security

Office 365 Advanced Security Mgmt.

Microsoft Intune

Security management

Azure Security Center

Office 365 Security Center

Windows Defender Security Center

Munich RE

"Azure gives us the ability to improve the analysis of the risks of change resulting from climate change to a new level."

– Robin Johnson: CIO – Munich Re

Next steps

Todd Elliott
Managing Director
todd.elliott@satalyst.com

Leigh Shayler
Chief Technical Officer
leigh.shayler@satalyst.com

Daniel Maddern
Cloud Security Practice Lead
daniel.maddern@satalyst.com

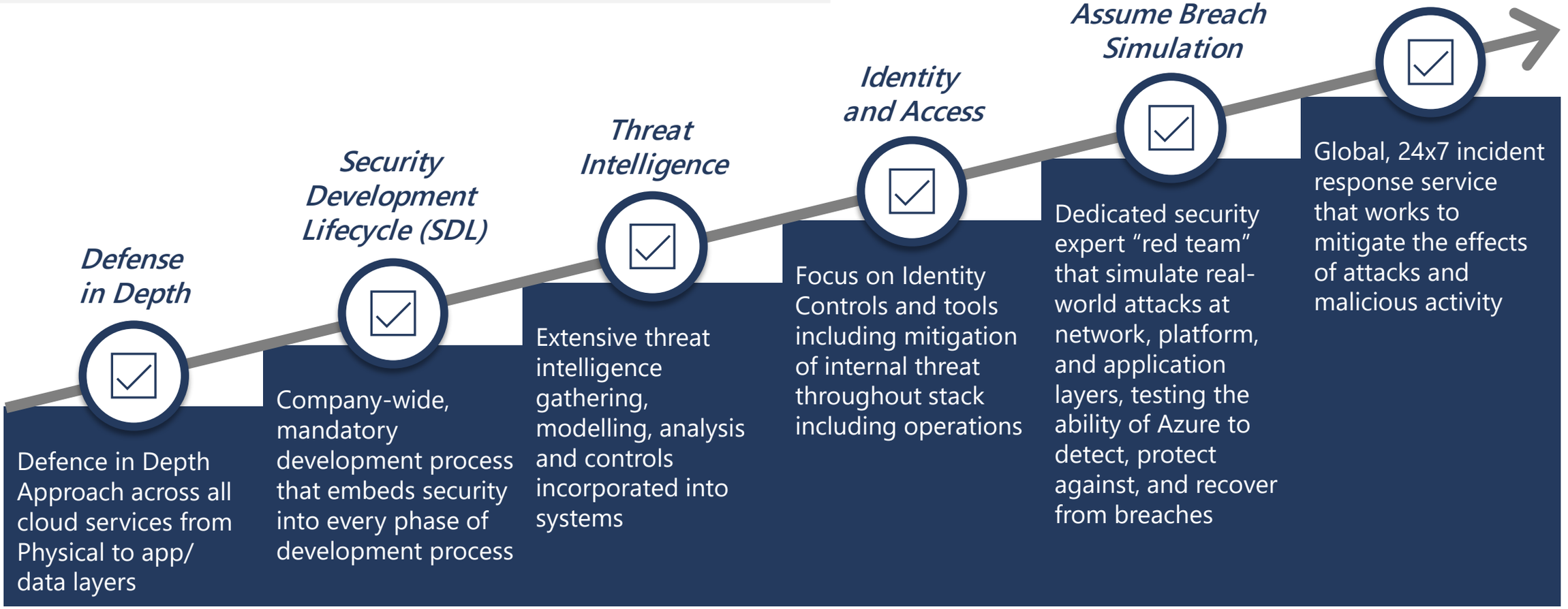
Contact us to learn more about security solutions from Microsoft

SATALYST

satalyst.com

Security Practices

Microsoft makes security a priority at every step, from code development to incident response



Built-in intelligence and advanced analytics

Threat intelligence

Looks for known malicious actors using Microsoft global threat intelligence

Partners

Integrates alerts from partner solutions, like firewalls and antimalware

Anomaly detection

Uses statistical profiling to build historical baselines

Alerts on deviations that conform to a potential attack vector

Behavioral analytics

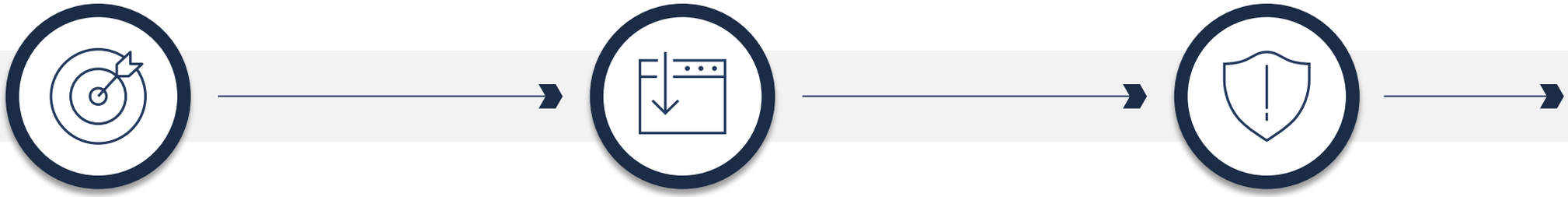
Looks for known patterns and malicious behaviors

Fusion

Combines events and alerts from across the kill chain to map the attack timeline

Powered by Microsoft Intelligent Security Graph

Detect threats across the kill chain



Target and attack

Inbound brute-force RDP, SSH, SQL attacks and more

Application and DDoS attacks (WAF partners)

Intrusion detection (NG Firewall partners)

Install and exploit

In-memory malware and exploit attempts

Suspicious process execution

Lateral movement

Internal reconnaissance

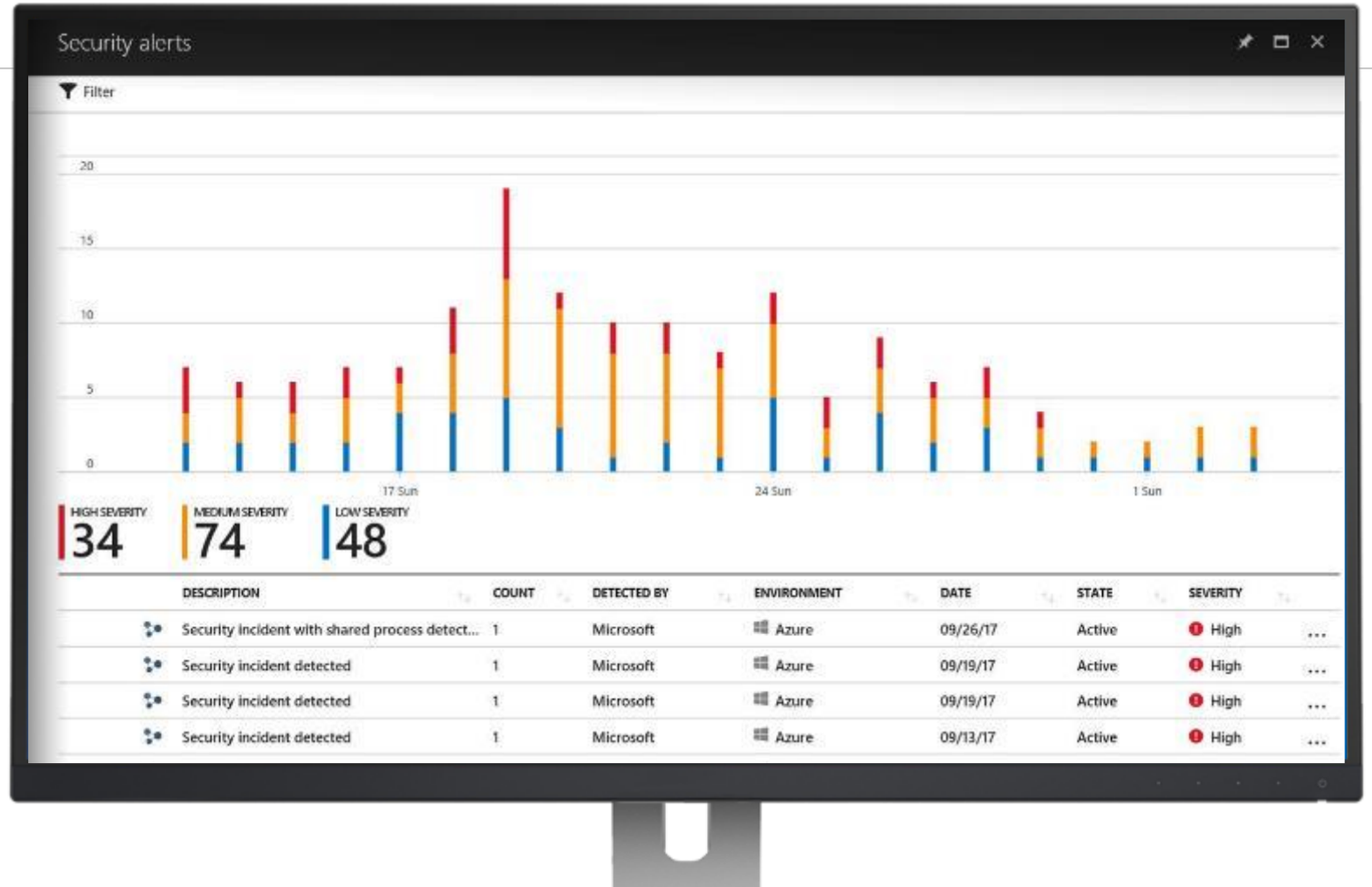
Post breach

Communication to a known malicious IP (data exfiltration or command and control)

Using compromised resources to mount additional attacks (outbound port scanning, brute-force RDP/SSH attacks, DDoS, and spam)

Focus on the most critical threats

- **Get prioritized security alerts**
  - Details about detected threats and recommendations
- **Detect threats across the kill chain**
  - Alerts that conform to kill chain patterns are fused into a single incident

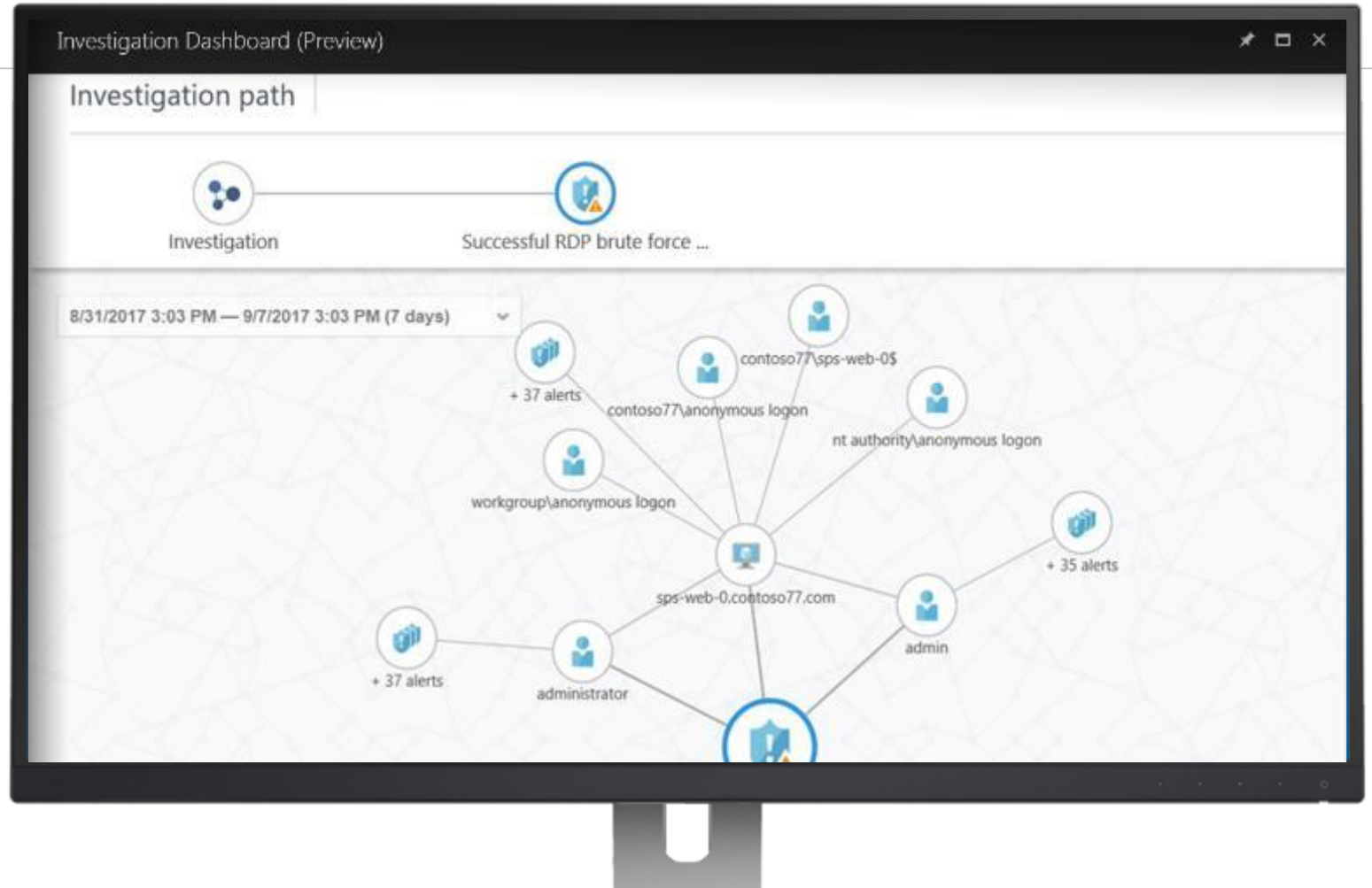


Gain valuable insights about attackers

- **Visualize source of attacks with interactive map**
  - Analyzes data from your computers and firewalls logs
- **Gain insights through threat reports**
  - Attacker's known objectives, tactics, and techniques

Simplify security operations and investigation

- **Quickly assess the scope and impact of an attack**
  - Interactive experience to explore links across alerts, computers and users
  - Use predefined or ad hoc queries for deeper examination



Respond quickly to threats

Automate and orchestrate common security workflows

- Create playbooks with integration of Azure Logic Apps
- Trigger workflows from any alert to enable conditional actions

Common workflows

- Route alerts to a ticketing system
- Gather additional information
- Apply additional security controls
- Ask a user to validate an action
- Block a suspicious user account
- Restrict traffic from an IP address