RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: STR-W01

Cloud Powered Compromise Blast Analysis: In the trenches with Microsoft IT

Sarah Handler

Program Manager II
Microsoft
@sarahhandler

Kristina Laidler

Sr. Director, Security Operations & Incident Response
Microsoft

To many, Microsoft is a vendor for security solutions to mitigate compromise…

…to some, Microsoft is their target

Microsoft

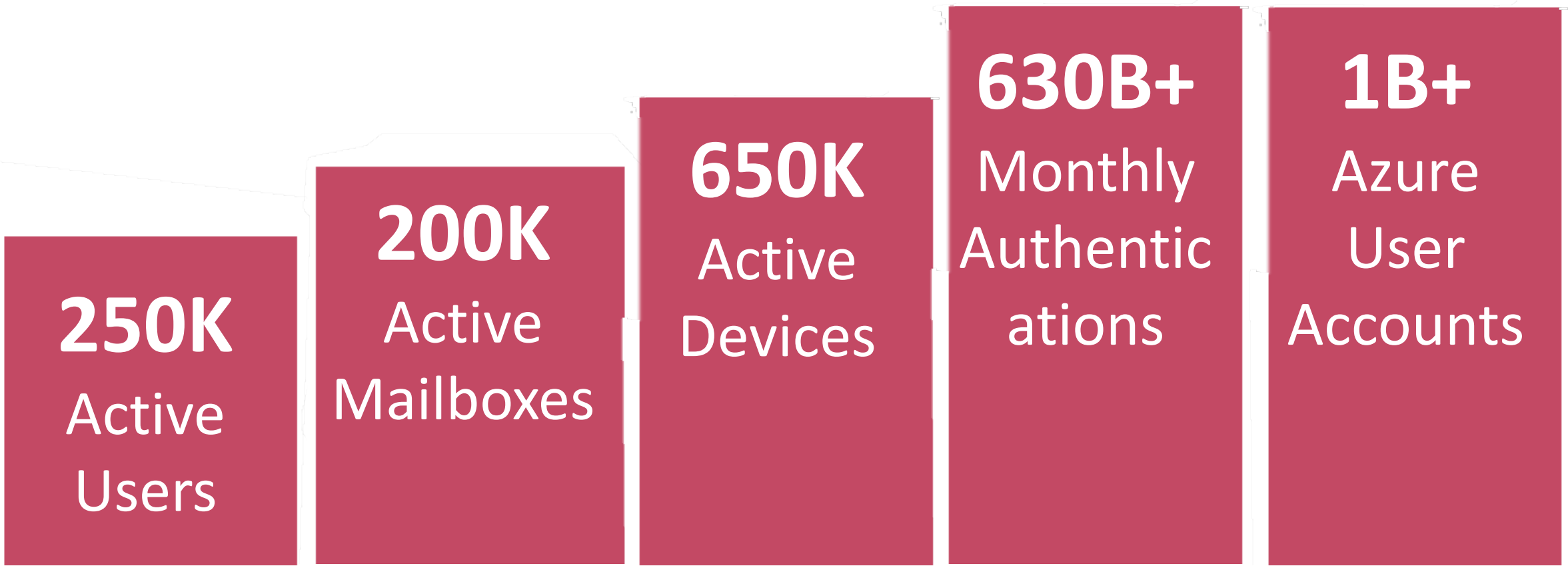
Security world view

- 63% of workers report **using the same password** for multiple work devices and/or applications
- According to the 2019 Verizon data breach investigation report, 34% of breaches involved an internal actor
- Microsoft has seen a **300% increase in identity attacks** over the past year
- More than half of US companies protect IP and company financial info using only passwords
- Multifactor authentication can help **reduce the risk of identity compromise by more than 99.9%**
- According to the Verizon data breach report, 81% of security breaches leverage stolen or weak passwords
- 90% of all cyberattacks, both incidents and breaches, are delivered **via phishing emails**
- Microsoft SOC volume of identity related incidents is….

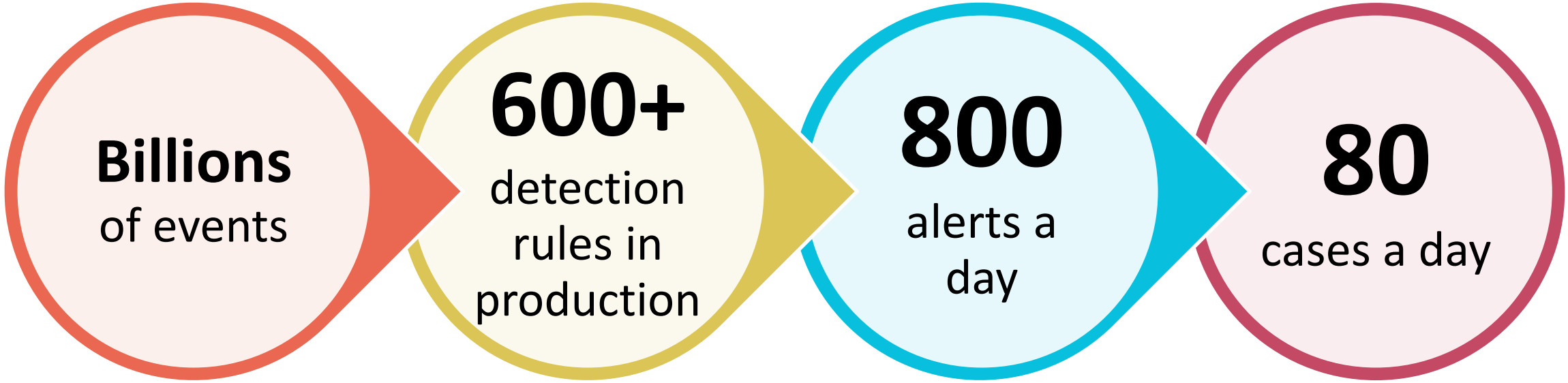
Persistent and expanding cyberattacks are the new normal. The World Economic Forum ranks cyberattacks near “natural disasters” as a top risk for 2019.

Signal at scale

Microsoft's SOC operates on a massive scale to support a highly dynamic, mobile workforce



Events, detections, alerts, cases



- An observable event on a system, in an environment, process, workflow or identity
- Detections identify security impacting, anomalous or suspicious activity
- Automated notifications resulting from a detection
- Plus, proactive hunting, IOC sweeps and user reporting
- Triage, investigate, remediate

Microsoft SOC

Enforce Quality + Apply Technology

Detect

Respond

Identity

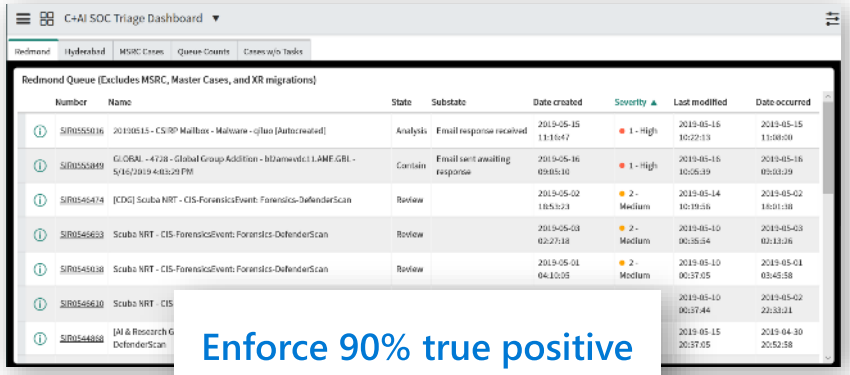
Endpoint

Cloud

Network

And More

Billions of events per month



Enforce 90% true positive on alert feeds

Machine Learning
(Artificial Intelligence)

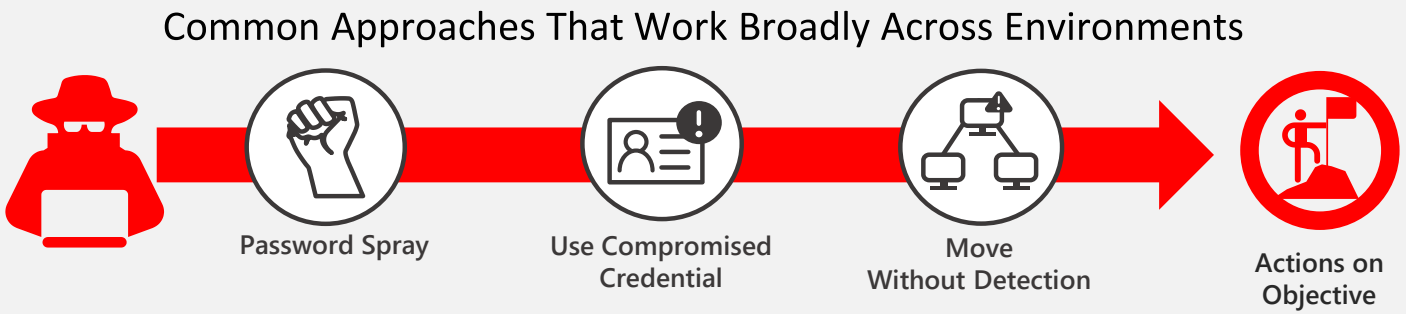
Behavioral Analytics (UEBA)
(User and Entity)

Focus on time to acknowledge and remediate

Security Orchestration, Automation, and Remediation (SOAR)

Microsoft

Attacker Driven Identity Events



Tactics, techniques, procedures

- Initial access
- Persistence
- Action on objective

Prevention: protecting identities

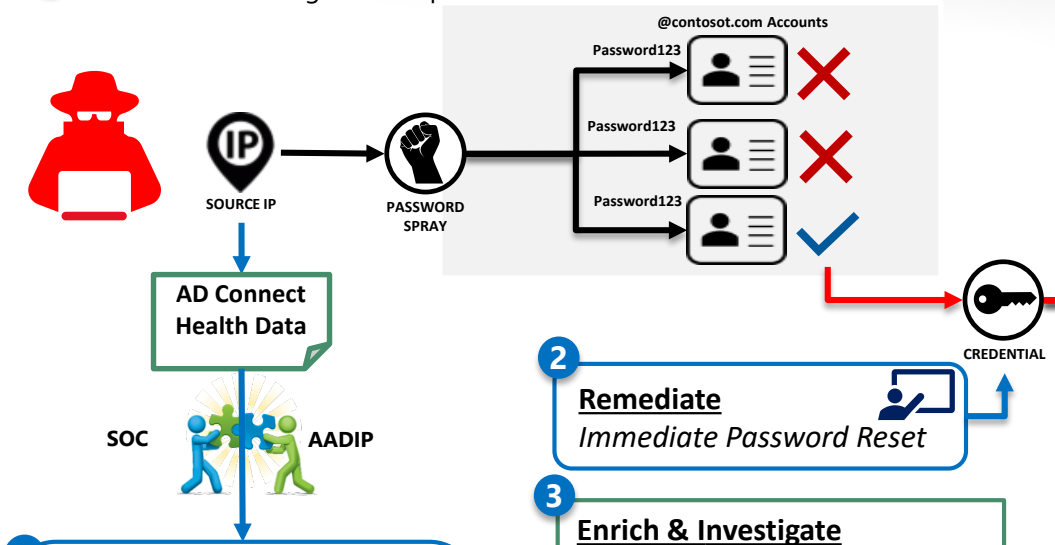
- Technical controls
  - Uniqueness filter protection for non-predictable passwords
  - Passwordless or Multi-Factor Authentication
  - Zero Trust / Least Persistent Admin
  - Block legacy authentication
  - UEBA detections
- Assessments
  - Password spray to identify potentially guessable passwords
  - Risk scoring framework
  - User education and awareness
  - Penetration testing
- Protect your privileged identities!

RSAConference2020

Identifying the existence and extent of attacks

Password Spray Scenario

1. Threat actor sprays large set of accounts with a small set of guessable passwords
2. Successful authentication confirms credential is valid

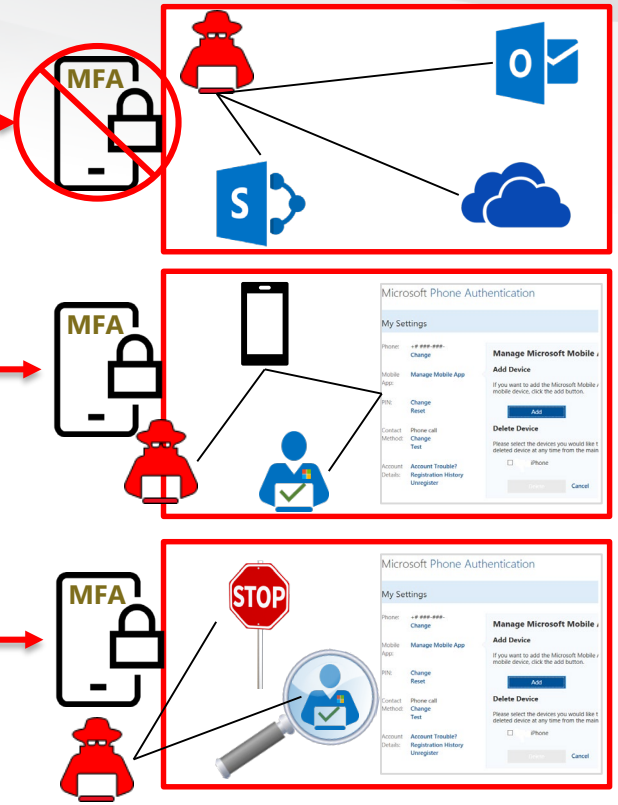


1 Detection
Users with Auth Failure
% Auth Success
% # Success / # Failures
>= 1 Auth Success
Query runs every 15 minutes

2 Remediate
Immediate Password Reset

3 Enrich & Investigate
Anomali Threat Intel Platform
Phone Auth / Reg data
O365 Threat Intelligence
MCAS & AADIP

4
Tipping & Queuing w/ Partners & PGs



3. Adversary has access to resources due to credential successfully guessed during spray attack.

Password filter needs to be implemented for guessable passwords.

4. Credential plus trusted device allows access to corporate assets and services

Better proofing methods are needed for Manager approvals.

5. While guessable passwords continue to create risk, MFA with strong proofing would prevent further access.

+ = More Secure

Solving for Detections

- Applied value of cloud learning and local knowledge
- Developed custom algorithm based on 1 known bad IP
- Tuned and tested detection to remove false positives

Next Steps

- Enforce password filter
- Enable MFA
- Enhance manager approval proofing
- PASSWORDS. = Goal

Microsoft

RSAConference2020

RSAConference2020

Demo: Querying Connect Health logs to discover password spray attacks

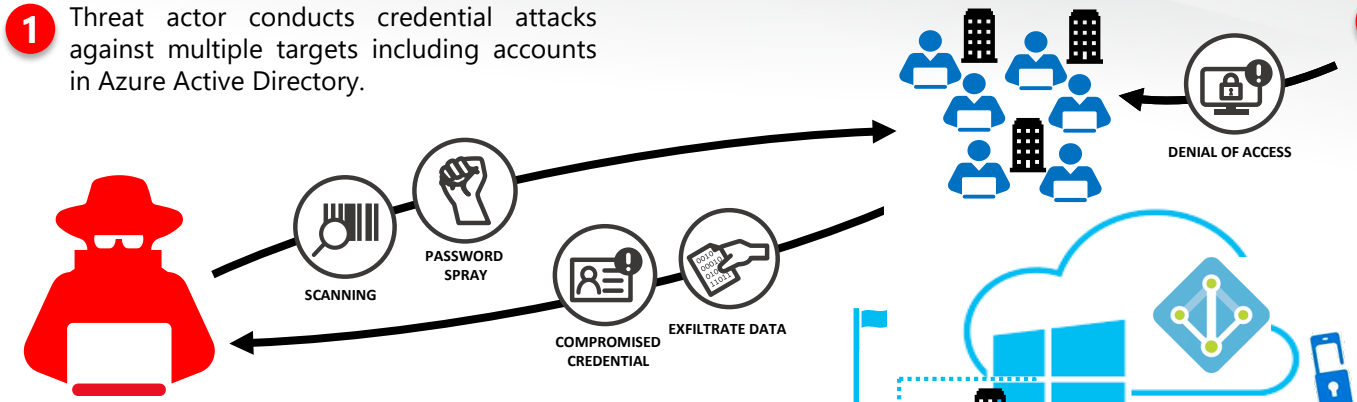
Discovering password spray

```
let valid_logons = (OfficeActivity
      | where TimeGenerated > ago(30d)
      | where Operation == 'UserLoggedIn’
      | summarize by ClientIP);
let only_invalid_logons = (OfficeActivity
      | where TimeGenerated > ago(30d)
      | where Operation == 'UserLoginFailed’
      | summarize by ClientIP)
      | join kind=anti (valid_logons) on ClientIP;
OfficeActivity
      | where TimeGenerated > ago(30d)
      | join kind=inner (only_invalid_logons) on ClientIP
      | extend UserAgent=tostring(parse_json(ExtendedProperties)[0].Value)
      | where (UserAgent matches regex 'Microsoft Office/\\d+\\.\\d+ \\(Windows NT \\d+\\.\\d+; Microsoft
Outlook \\d+\\.\\d+\\.\\d+; Pro\\)’
            or UserAgent == 'CBAInPROD’
            or UserAgent matches regex '^[\\w\\.\\d\\-\\_]{4,15}\\/[\\.\\w\\d\\-\\_]{4,30}$’)
      | summarize by ClientIP, UserAgent
```

@JohnLaTwC

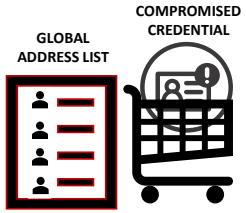
Credentials on the Dark Web

1. Threat actor conducts credential attacks against multiple targets including accounts in Azure Active Directory.



3. Domain accessed by actor and credentials are advertised for sale.

2. Threat actor advertises access to numerous domains



Password spray detection to detect attempted password spray attacks against accounts

Activity detected on dark web

Attack Services are Inexpensive

- **Spearphishing services** range from $100 to $1,000 per successful account take over
- **Compromised accounts** As low as $150 for 400M. Averages $0.97 per 1k.
- **Compromised accounts** usually come in bulk in very large blocks. Prices average around $1 USD per 1k accounts and quality varies significantly (from 0.1% up to 20% of the username/password pairs may be valid)

]

- Detections related to password spray attacks and password reset activity
- Risk scoring and NRT credential reset/token roll. authentication bypass in the wild.
- This type of attack underscores the importance of two-factor authentication and decommissioning of legacy authentication methods.

RSAConference2020

[Placeholder for story/demo of recent attack we saw]

Waiting for final internal approval to share details

Lessons from our battles- and what's next

- Event logging and data retention
  - Tenant view of all login events, user permissions and detail on applications being requested by those identities
  - Data retention strategy consistent with legal and contractual requirementsLogg
- Separate and protect privileged accounts
  - Separate identity, secure device, closely monitored
- Detect threats through user behavior anomalies
  - Leverage large security-related data sets to evolve from deterministic alerts
  - Use risk scoring to surface highest priority alerts

What to do next in your battle against compromise

- Next week you should:
  - Evaluate data sets to identify potential gaps
  - Assess your data retention strategy
- In the next three months you should:
  - Reduce persistent admins
  - Implement conditional access control policies
- Within six months you should:
  - Implement access control policies
  - Apply zero trust policy to access requests

RSAConference2020

Q&A