RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: PART4-T08

XDR: Improving EDR effectiveness by adding email & network visibility

Eric Skinner

VP, Market Strategy
Trend Micro
@EricSkinner

Social engineering risk

Code from 3rd party repositories

Misconfigurations

Network vulnerabilities

Application Vulnerabilities

User behavior

Vulnerable OT devices

Endpoint Vulnerabilities

Old operating systems

SOC/IR ANALYST

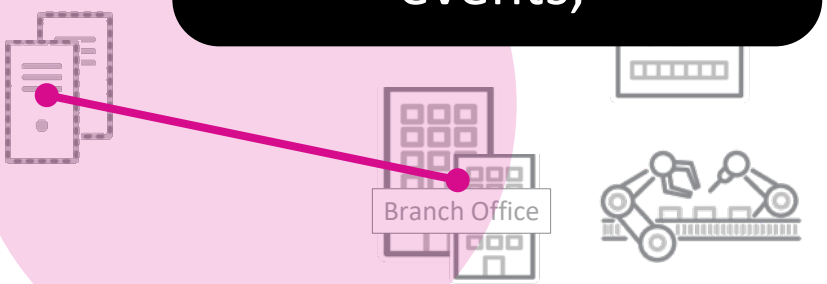
Wants fast detection & response across entire environment

…and limited visibility to threats affecting cloud workloads

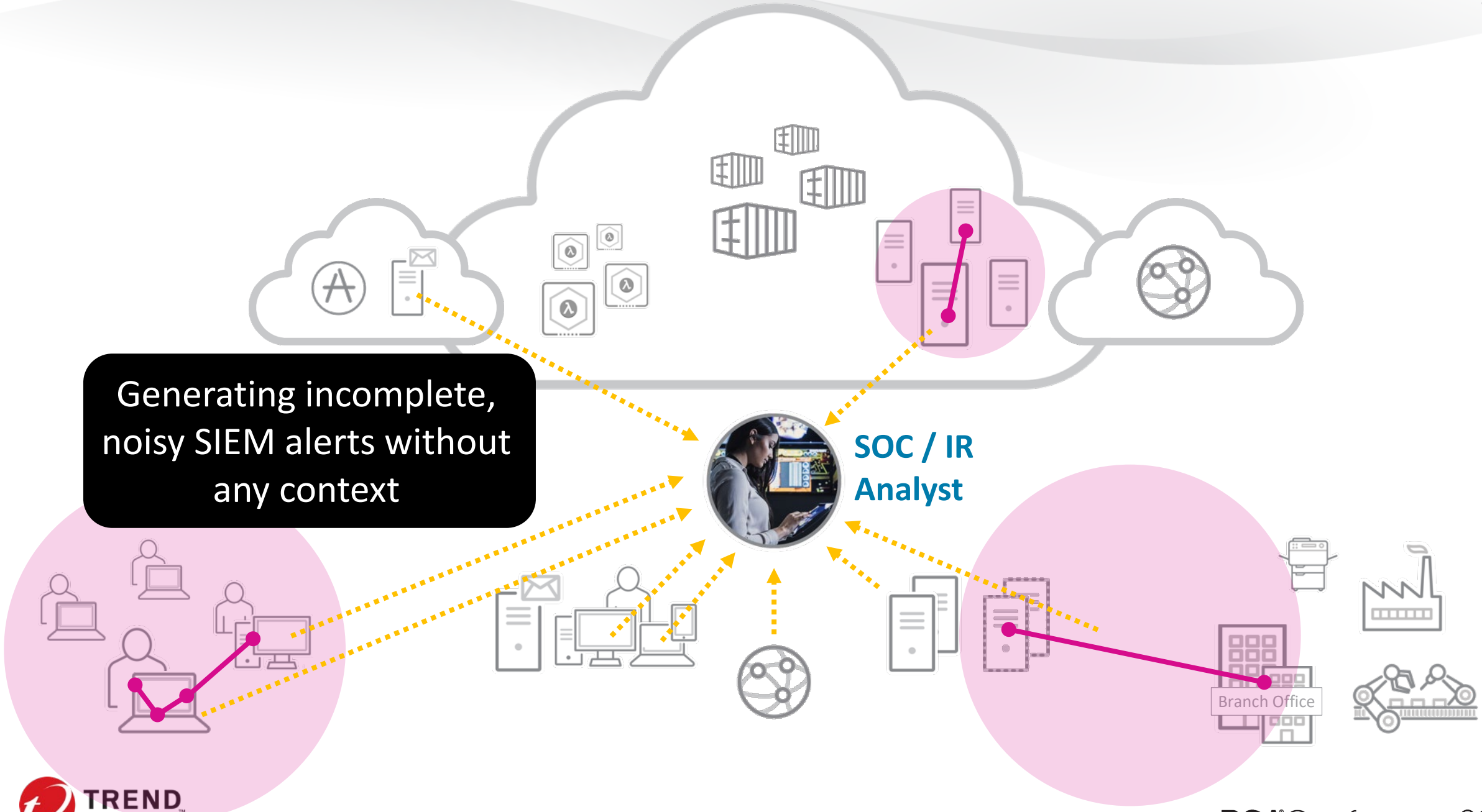
Today, the SOC gets siloed insight into endpoints (EDR)…

SOC / IR Analyst

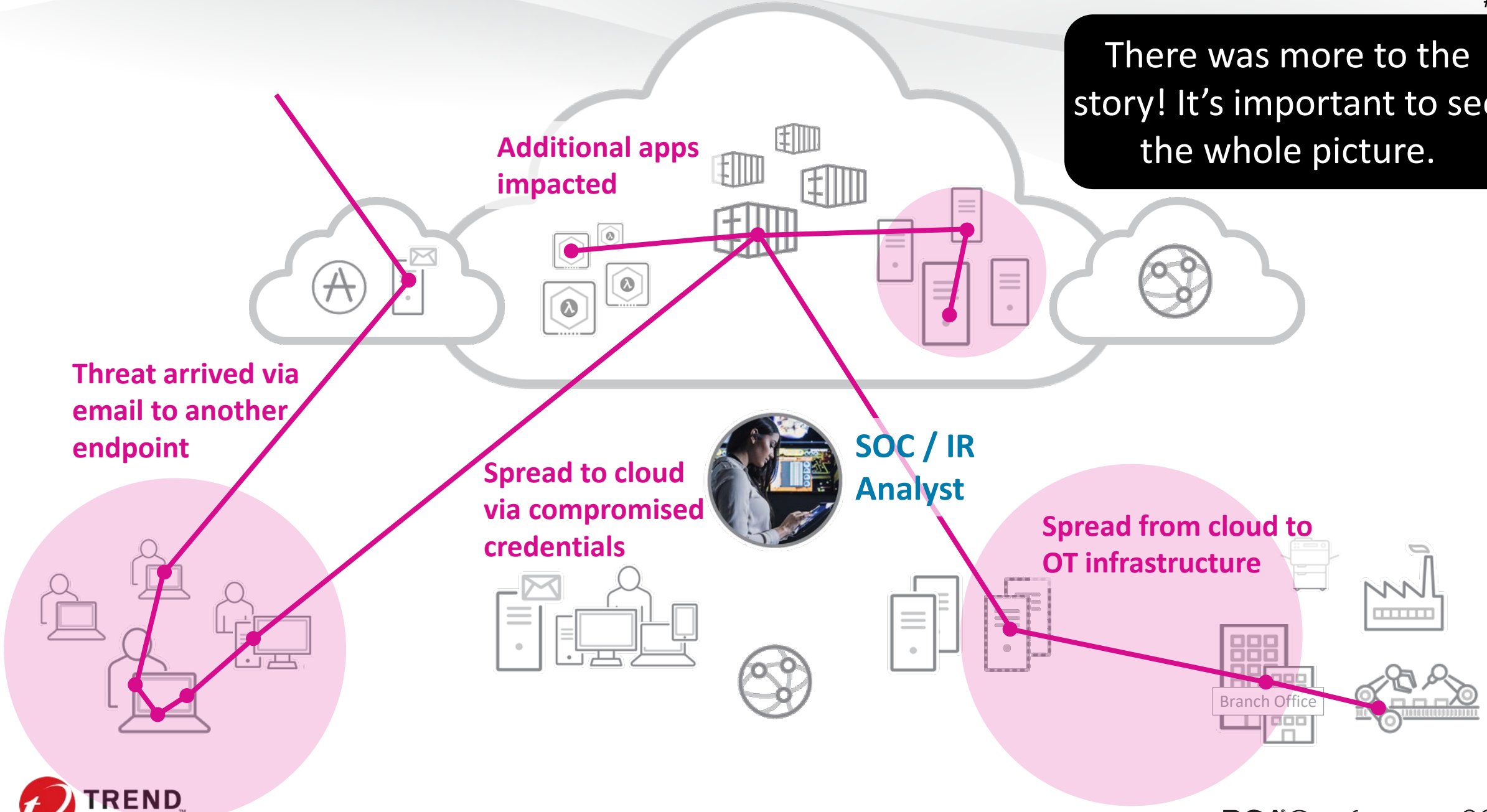
…a separate siloed view into network events,



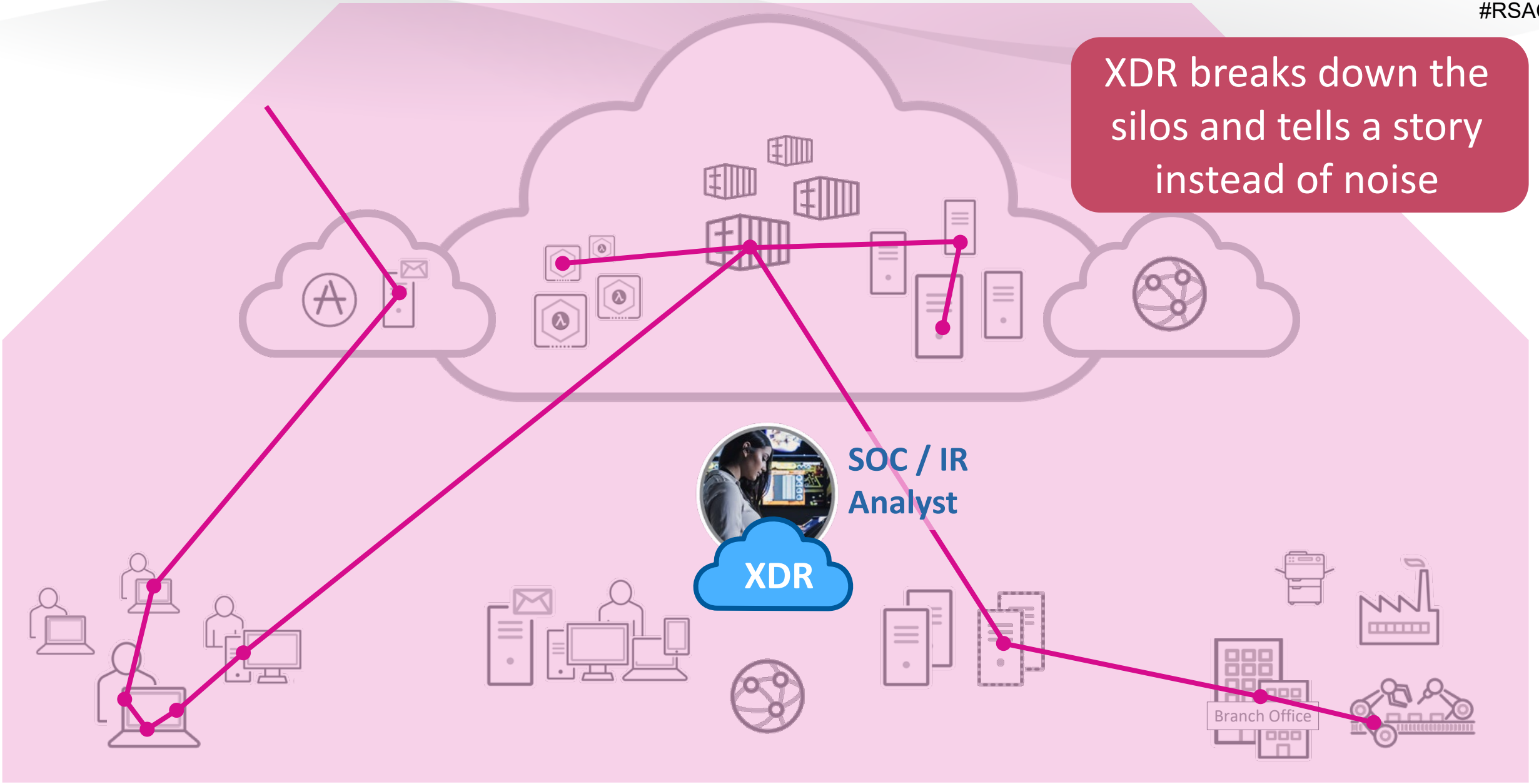
TREND MICRO

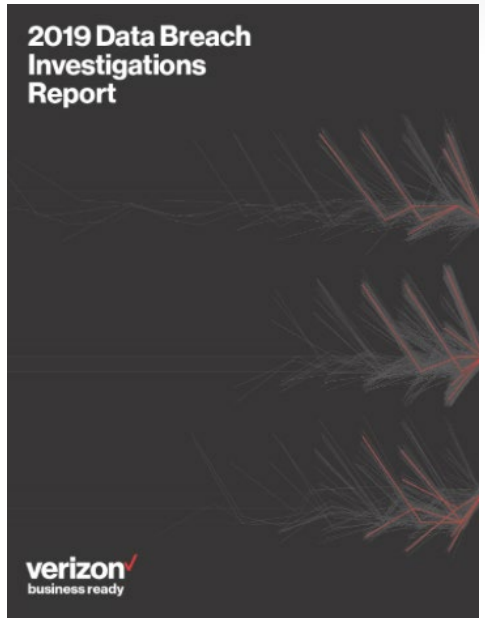

Generating incomplete, noisy SIEM alerts without any context
SOC / IR Analyst
Branch Office

There was more to the story! It's important to see the whole picture.



XDR breaks down the silos and tells a story instead of noise





Source: Verizon Data Breach Investigations Report, May 2019

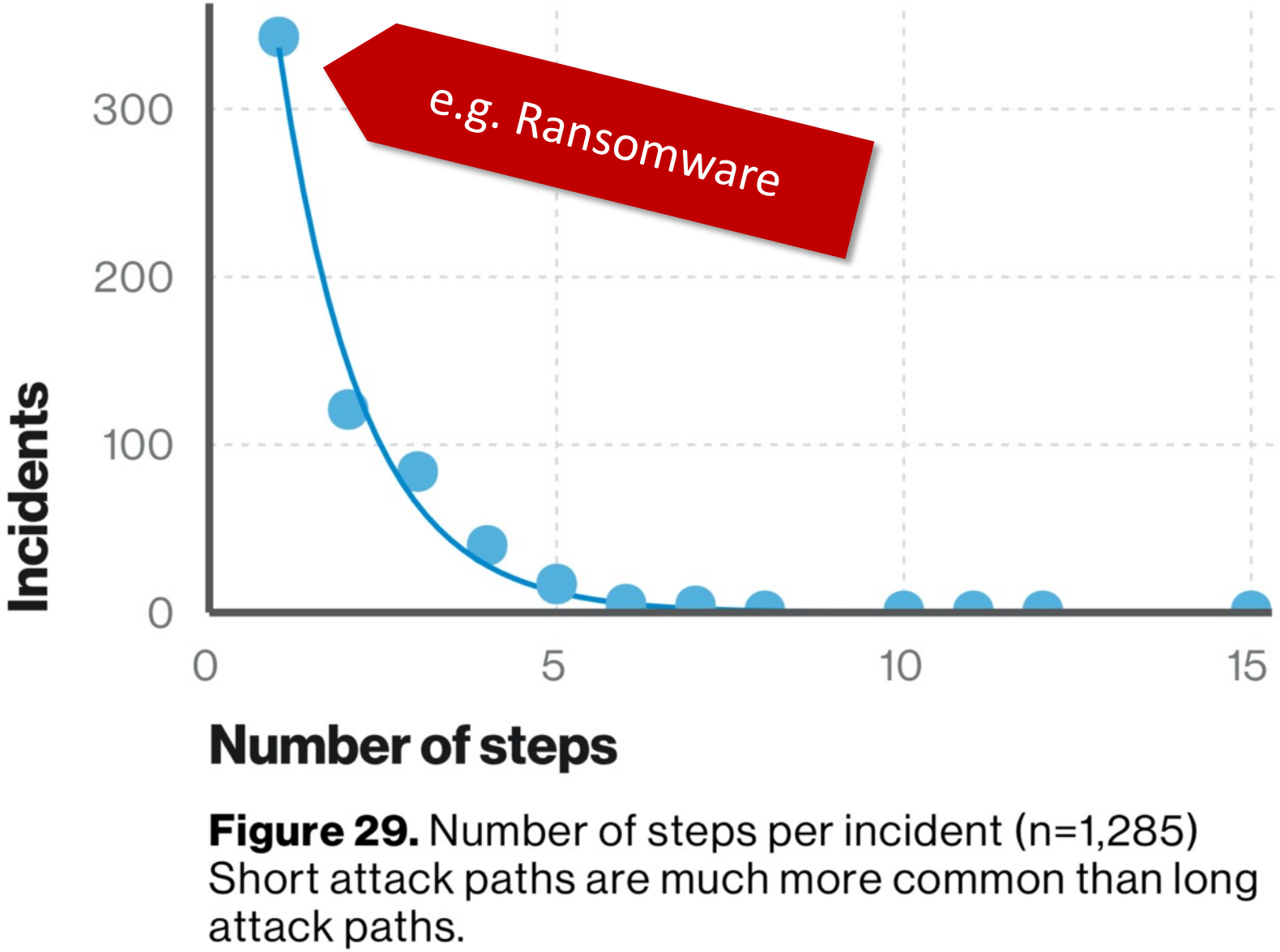


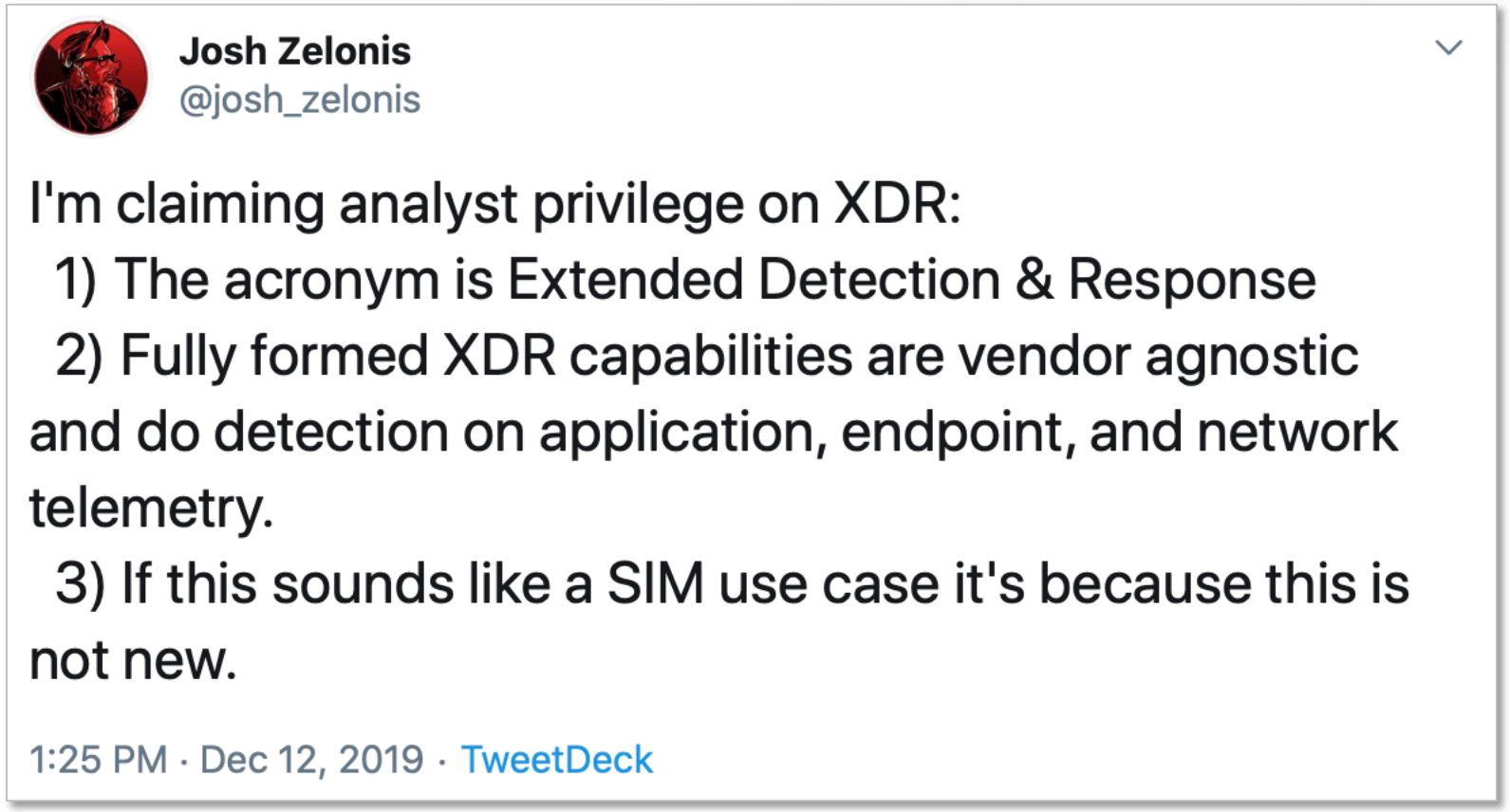
Figure 29. Number of steps per incident (n=1,285) Short attack paths are much more common than long attack paths.

RSAConference2020

What's XDR, anyway?

An emerging industry term, not vendor-specific.

XDR Definition, emerging:



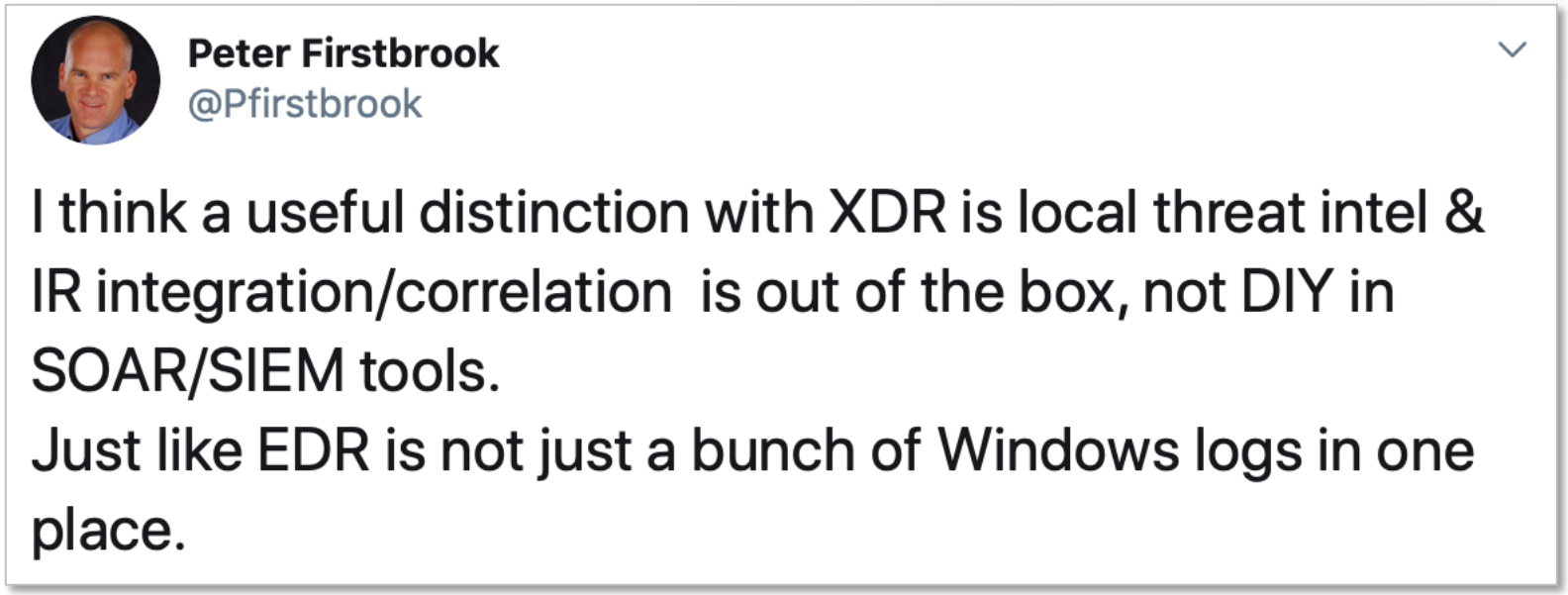
Josh Zelonis
@josh_zelonis

I'm claiming analyst privilege on XDR:
1) The acronym is Extended Detection & Response
2) Fully formed XDR capabilities are vendor agnostic and do detection on application, endpoint, and network telemetry.
3) If this sounds like a SIM use case it's because this is not new.

1:25 PM · Dec 12, 2019 · TweetDeck

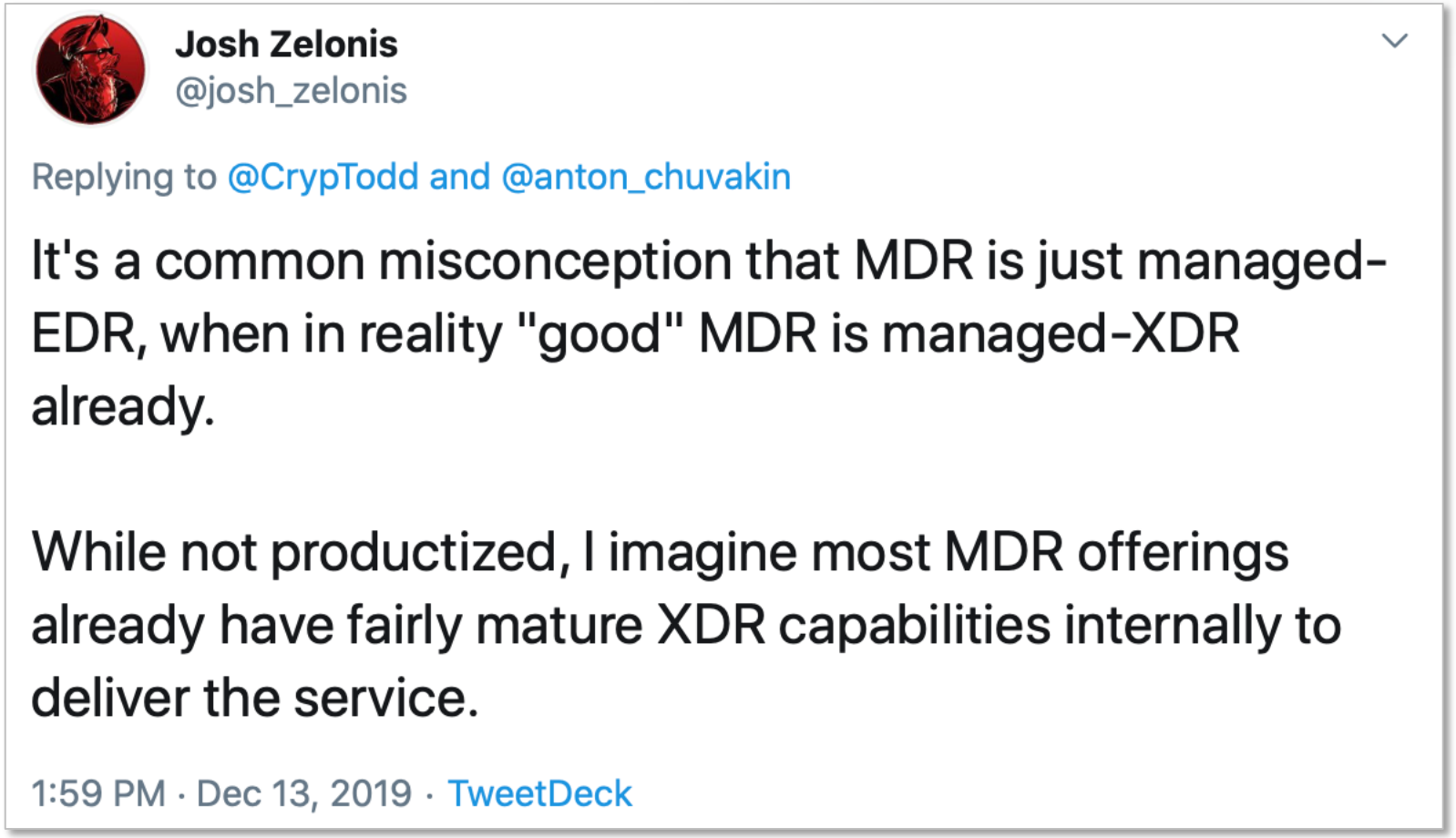
Josh Zelonis, Principal Analyst, Forrester Research Inc.
December 12, 2019
https://twitter.com/josh_zelonis/status/1205192042843758592

With focus on built-in correlation, not just collection:



Peter Firstbrook, VP Analyst, Gartner Inc.
Dec 13, 2019
https://twitter.com/Pfirstbrook/status/1205559416755511296

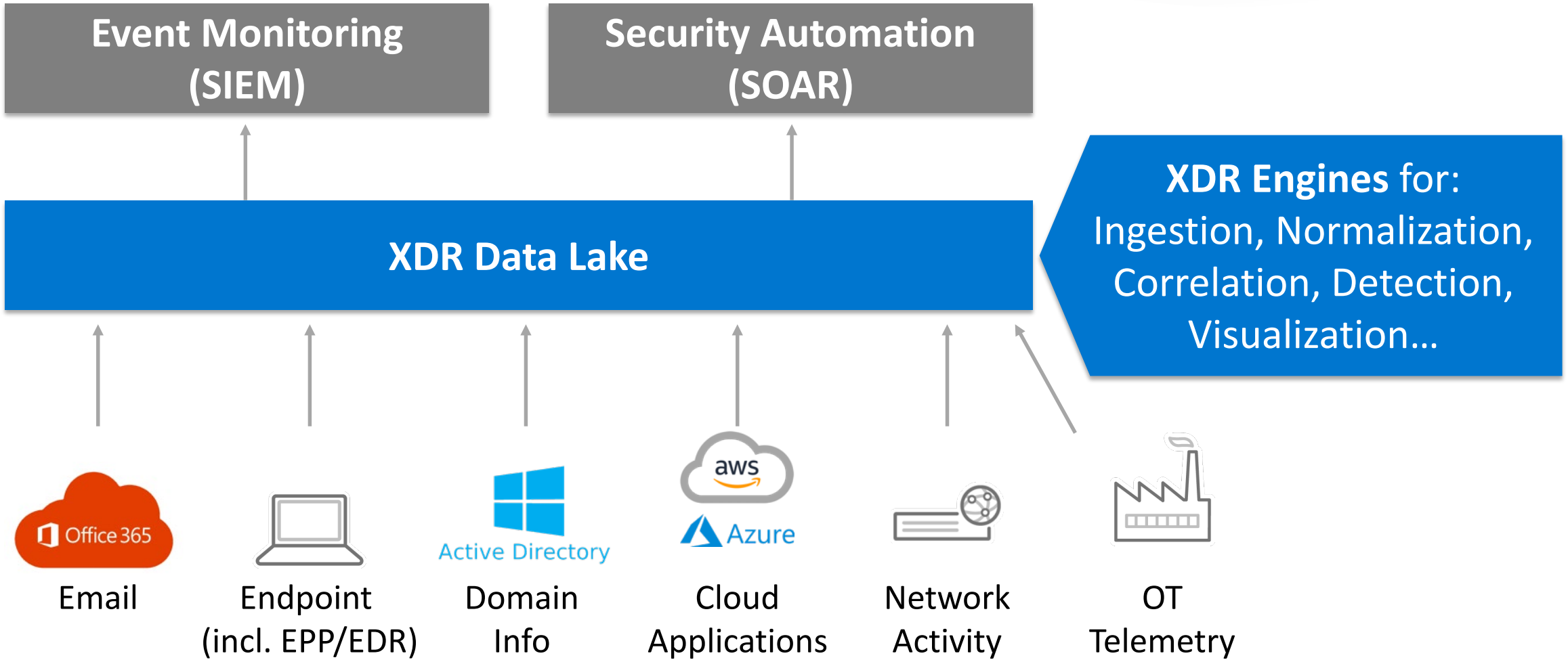
Some Managed Services do “XDR” today



Josh Zelonis, Principal Analyst, Forrester Research Inc.
December 13, 2019
https://twitter.com/josh_zelonis/status/1205563012163108864?s=20

XDR Acronym, Expanded

An XDR system view

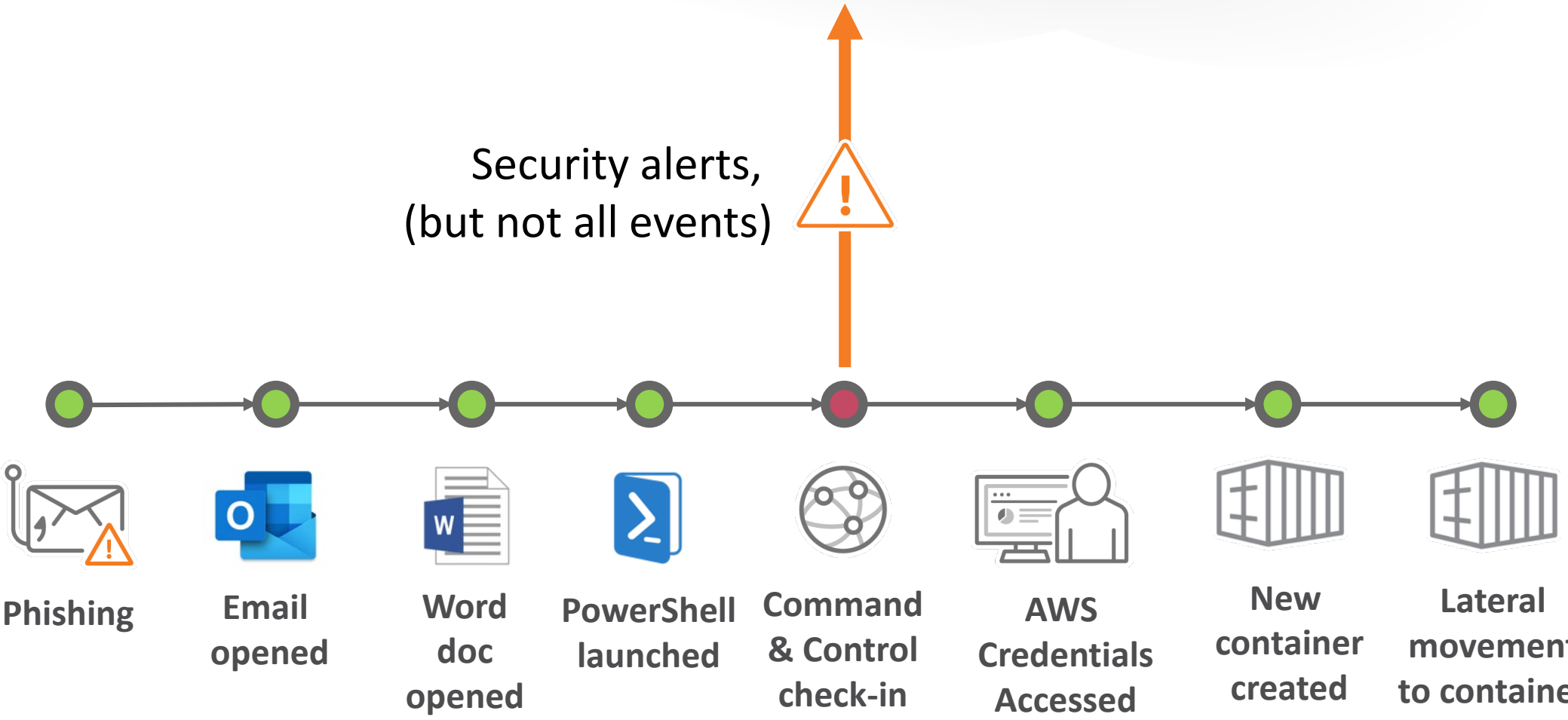


RSAConference2020

Isn’t this just SIEM? No.

SIEM (Security Information and Event Management)

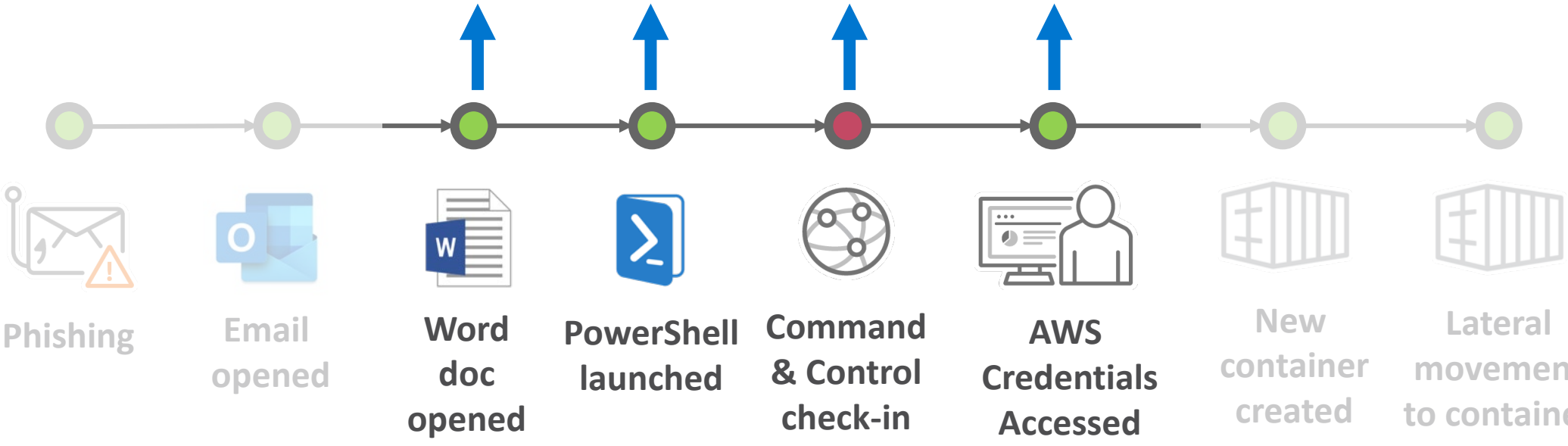
Security alerts,
(but not all events)

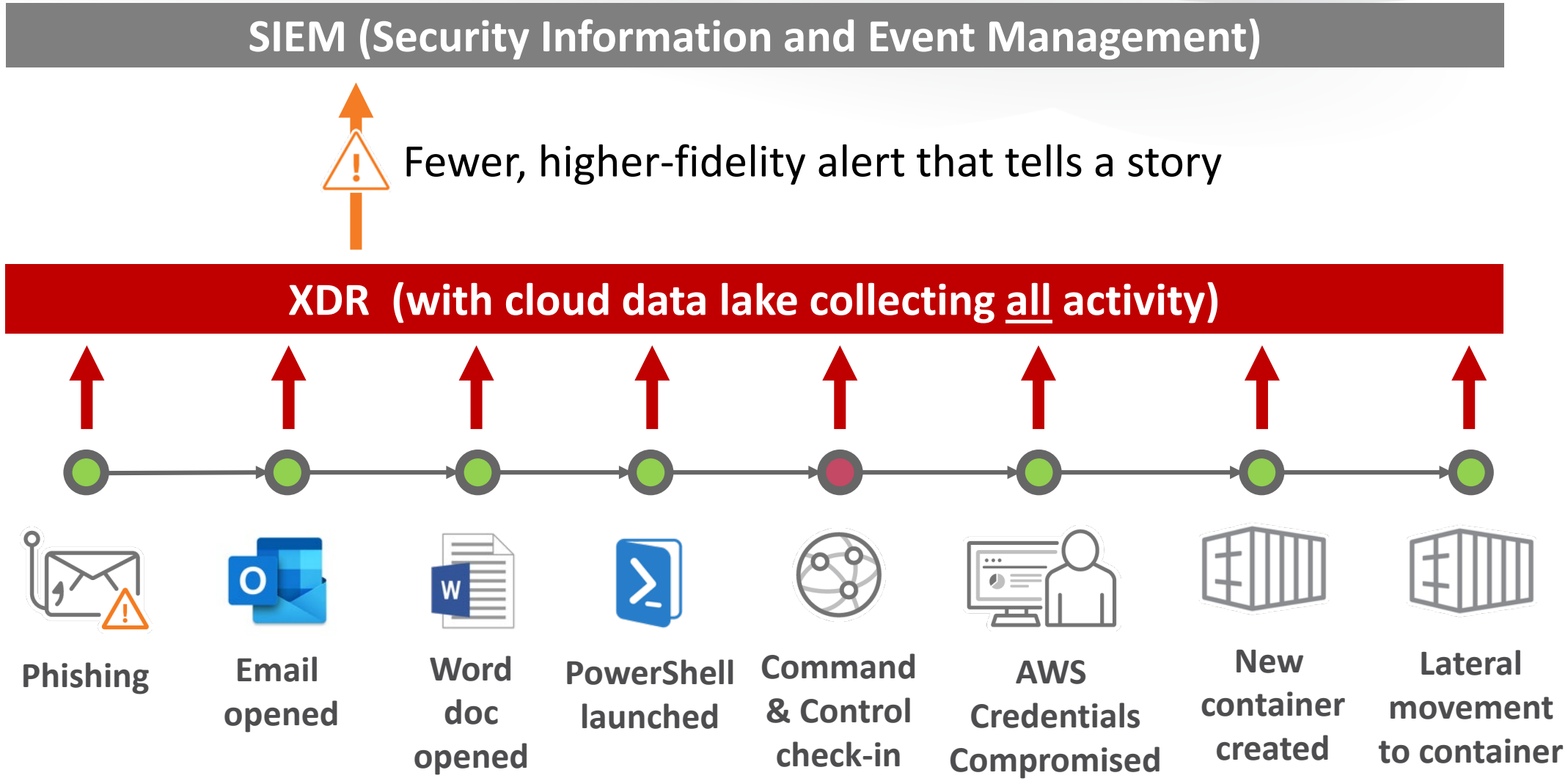


SIEM (Security Information and Event Management)

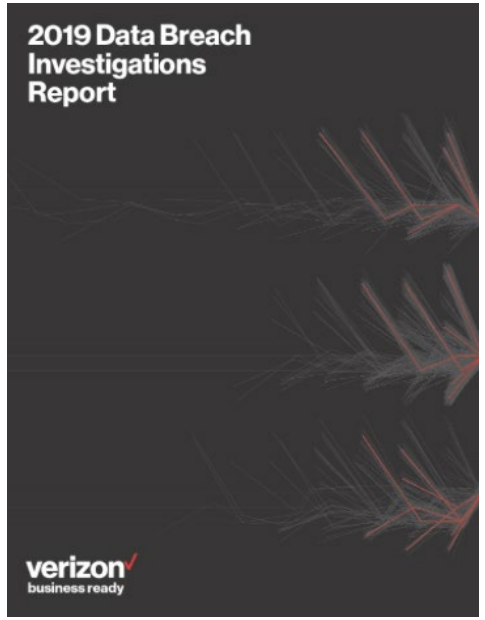
Collecting all **endpoint** activity, not just alerts

EDR (Endpoint Detection & Response)



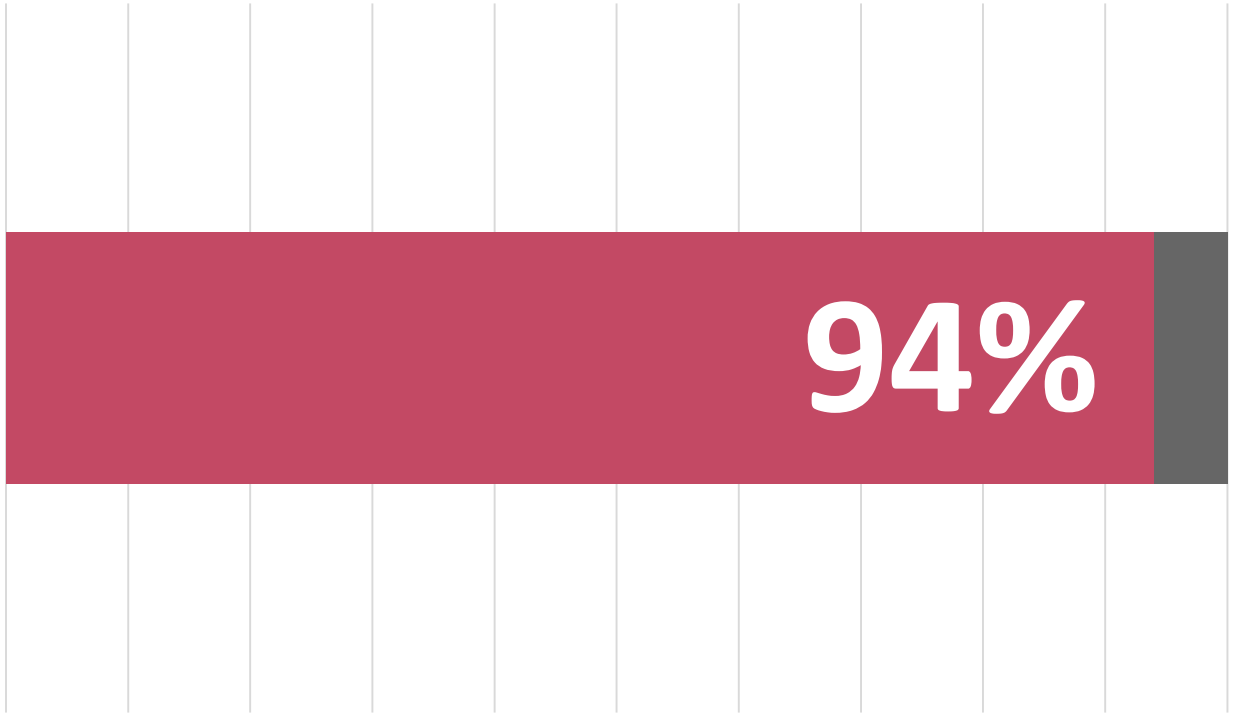

SIEM (Security Information and Event Management)
Fewer, higher-fidelity alert that tells a story
XDR (with cloud data lake collecting all activity)
Phishing
Email opened
Word doc opened
PowerShell launched
Command & Control check-in
AWS Credentials Compromised
New container created
Lateral movement to container

Why email detection & response?

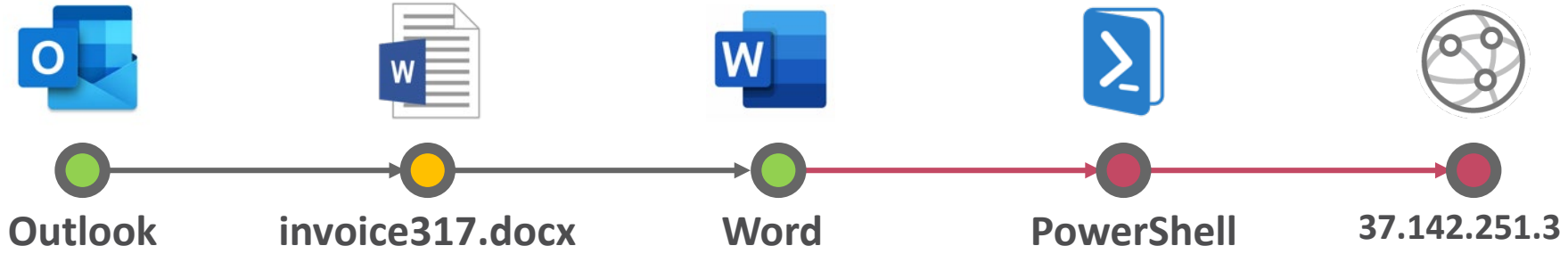


Source: Verizon Data Breach Investigations Report, May 2019

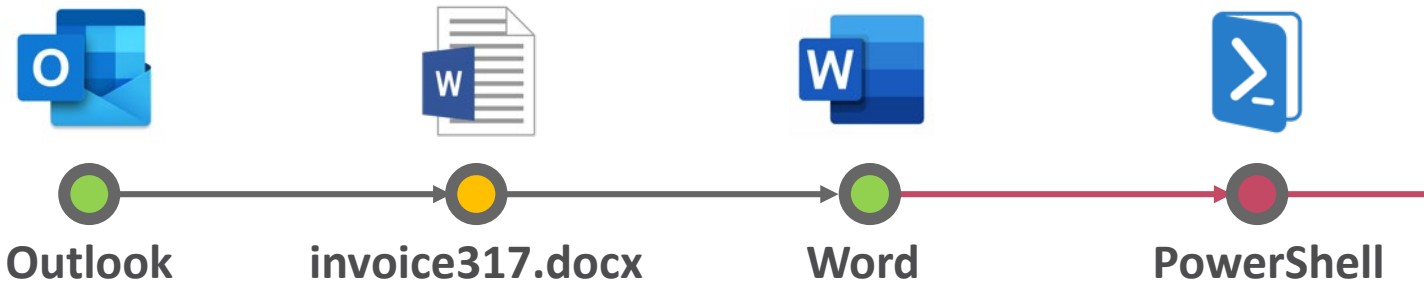
Email as the delivery method for malware:

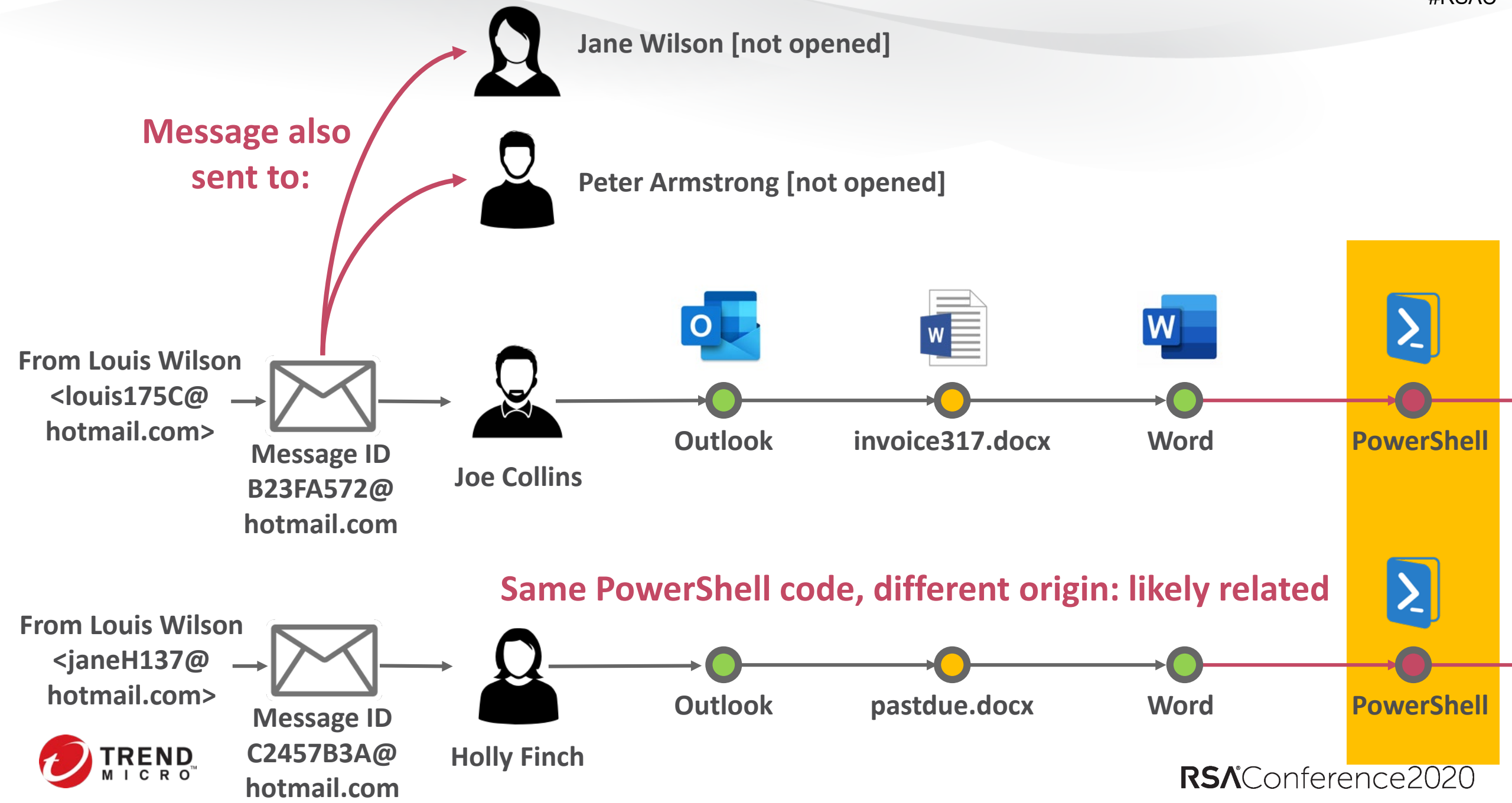


This looks bad, and can trigger detection…



…but knowing what happened earlier is really useful!




Jane Wilson [not opened]
Message also sent to:
Peter Armstrong [not opened]
From Louis Wilson <louis175C@ hotmail.com>
Message ID B23FA572@ hotmail.com
Joe Collins
Outlook
invoice317.docx
Word
PowerShell
Same PowerShell code, different origin: likely related
From Louis Wilson <janeH137@ hotmail.com>
Message ID C2457B3A@ hotmail.com
Holly Finch
Outlook
pastdue.docx
Word
PowerShell

Server & Endpoint Attacks are Different

Typical Endpoint Attack

Email origin, tricks user to activate threat

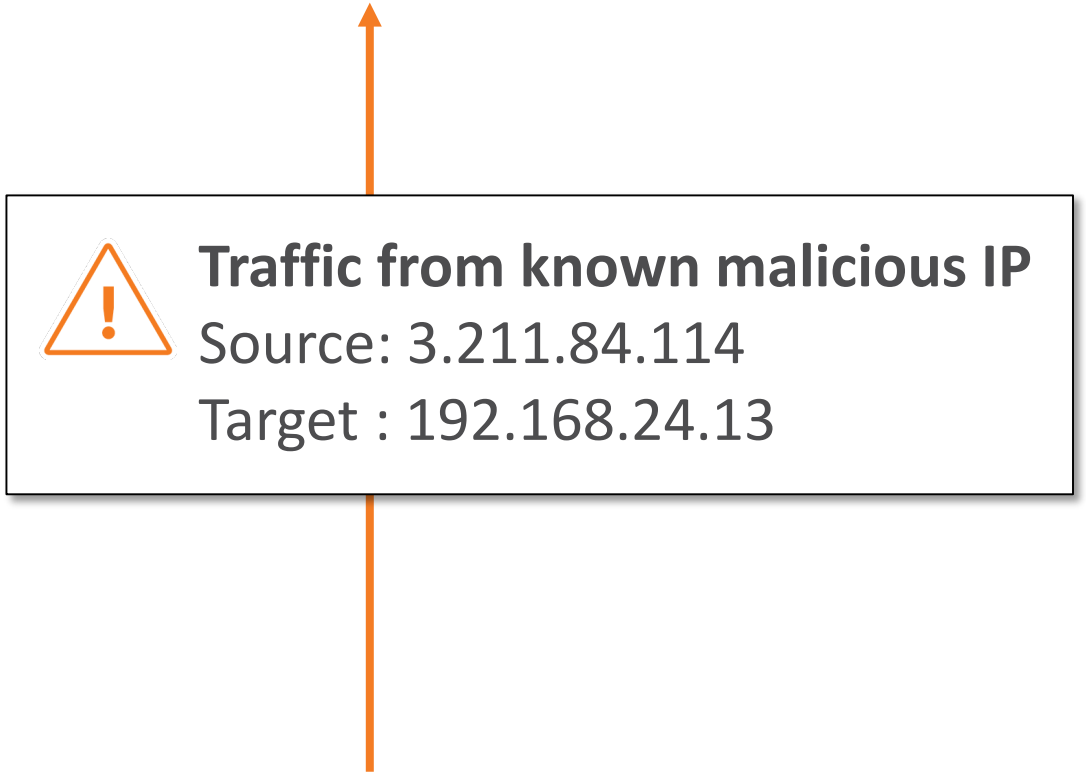
Threat launches, performs actions, spreads laterally

Typical Server Attack

Attack arrives remotely, targets OS or application vulnerability

Vulnerability exploit launches malicious actions

SIEM



Server Workload

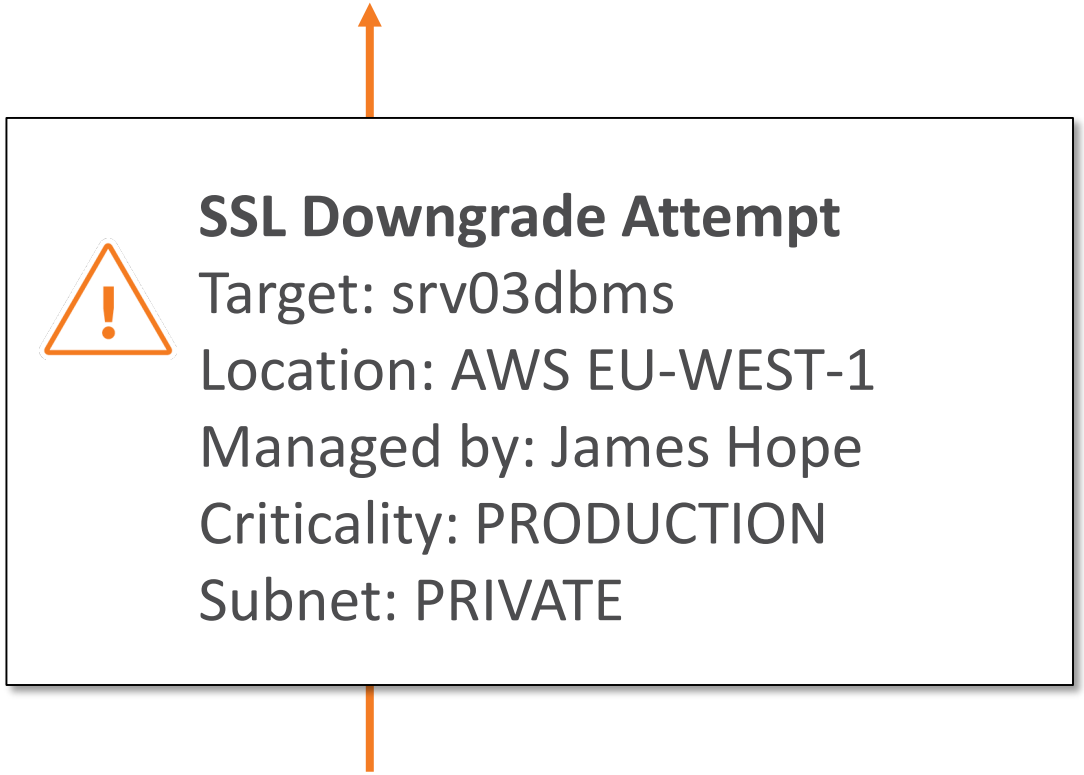
Server IR challenge #1:
SIEM has Insufficient Context

Who manages this server?

Is it in the datacenter or in AWS/Azure?

How critical is the workload?

XDR



Server Workload

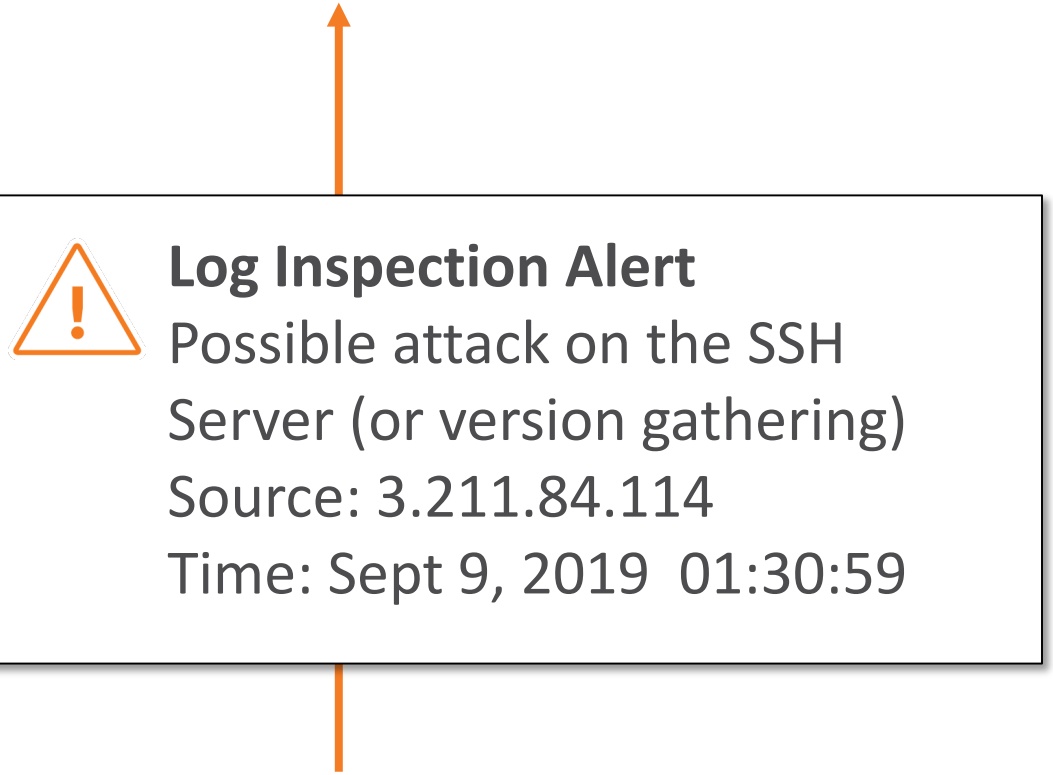
More Context with XDR Telemetry

Speeding response

Prioritizing severity

Leveraging meta-data from cloud platforms

SIEM



Server Workload

Server IR challenge #2:
Alerts don't tell whole story

General Information

Time:	September 9, 2019 01:30:59
Computer:	ec2-54-201-30-214.us-west-2.compute.amazonaws.com (Hybrid Jump) [i-a504727d]
Event Origin:	Agent
Reason:	1002828 - Application - Secure Shell Daemon (SSHD)
Description:	Possible attack on the ssh server (or version gathering)
Rank:	50 = Asset Value x Severity Value = 1 x 50
Severity:	High (8)
Groups:	syslog,sshd,
Program Name:	sshd
Event:	Bad protocol version identification '\026\003\001\002' from 3.211.84.114 port 51302
Location:	/var/log/secure
Source IP:	
Source Port:	
Destination IP:	

SIEM

Log Inspection Alert
Possible attack on the SSH Server (or version gathering)
Source: 3.211.84.114
Time: Sept 9, 2019 01:30:59

Server Workload

Server IR challenge #2:
Alerts don't tell whole story

This is likely one step of many

What's the bigger picture?

Has the attacker been successful?

XDR tells a story

Enables faster/automated response

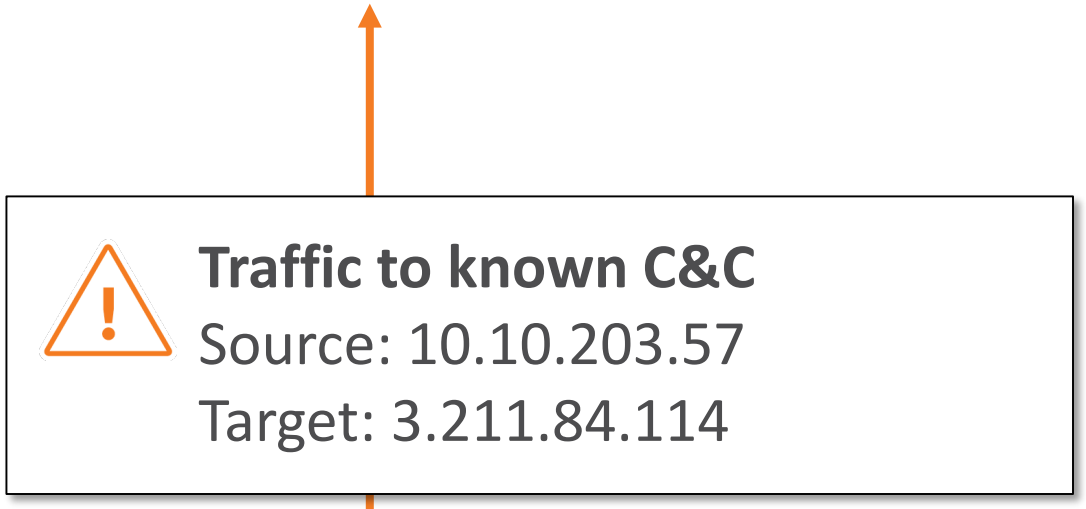
XDR

Suspicious process launched after likely SSH brute force attack

Malformed SSH protocol (likely version gathering)	SSH Login Failure Account: maint3 Qty: 23	SSH Login Success Account: maint3	Unknown Process /svc/daemon34

Server Workload

EDR



Server Workload using Containers

Server IR challenge #3:
Endpoint EDR doesn't deeply understand containers

What container has the issue?

What about images that aren't running?

XDR

Additional vulnerable container images require remediation
Inactive containers
Image IDs: 84c2af573c22 + 14
Vulnerability: CVE2017-1000408

Traffic to known C&C from vulnerable container
Source: 10.10.203.57
Target : 3.211.84.114
Docker Container d7886598dbe2
Image ID: e31487ab6f14
Vulnerability: CVE2017-1000408

Inbound C&C traffic detected to second vulnerable container
Running container
Container: 17cfa731521f
Image ID: 37a2426c631a
Vulnerability: CVE2017-1000408

Server Workload using Containers

RSAConference2020

XDR Demo

State of XDR Today

Analysts / vendors / customers shaping the category & term

Vendors understand their own telemetry best. SIEM sees more but understands less.

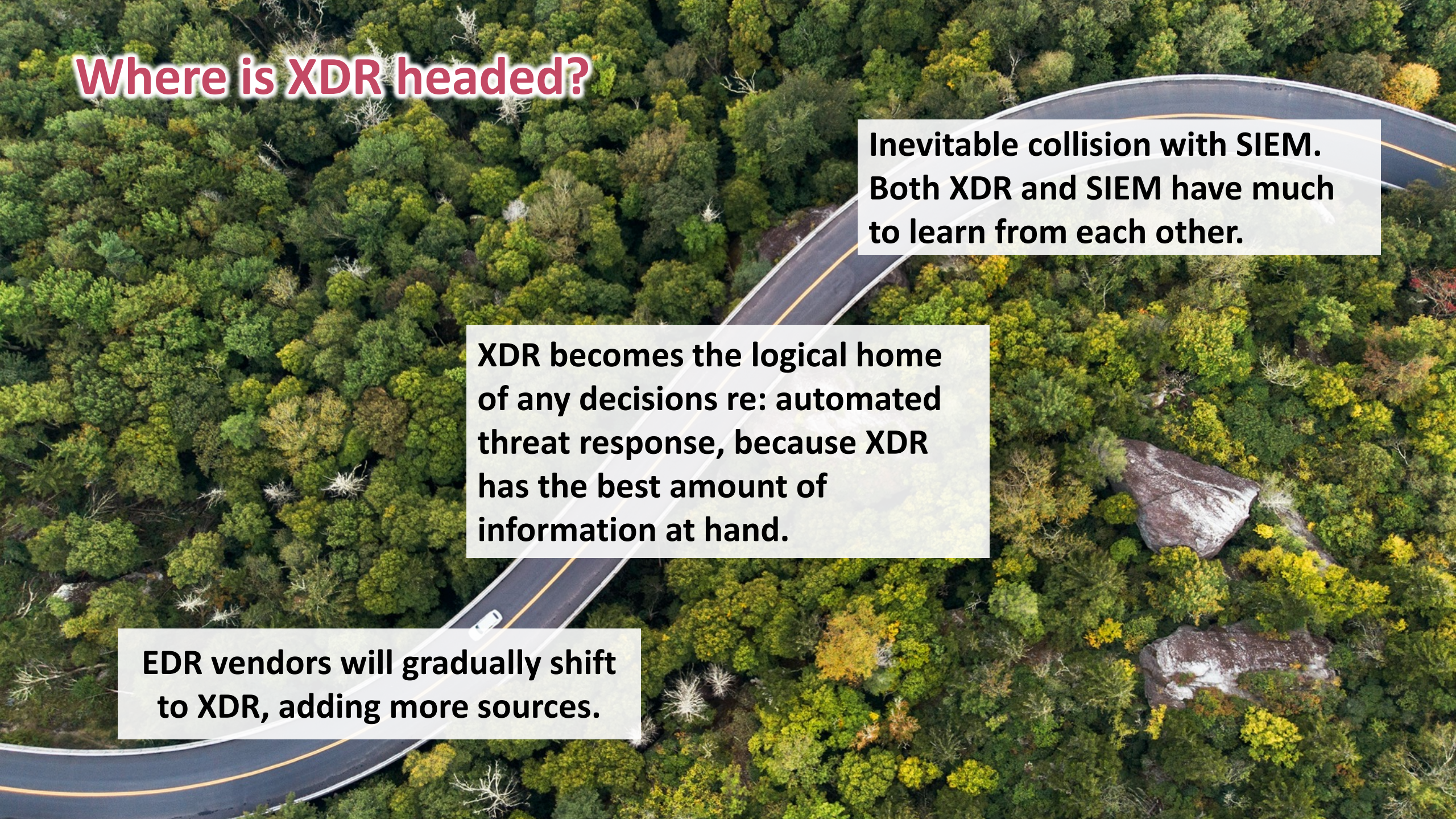
Currently either goes broad or deep but not both – which sources matter to you? Which deliver most important visibility?

Enabling expanded MITRE ATT&CK mapping as their frameworks evolve

Activity telemetry = lots of storage required. Expensive for cloud-based XDR.

What is optimal balance between automated response vs. manual review?

Where is XDR headed?



Inevitable collision with SIEM. Both XDR and SIEM have much to learn from each other.

XDR becomes the logical home of any decisions re: automated threat response, because XDR has the best amount of information at hand.

EDR vendors will gradually shift to XDR, adding more sources.

XDR: Lessons to Apply Today

1. Explore whether your existing EDR can see beyond the endpoint; if yes, and sources are useful, understand and enable that
2. In particular, aim to integrate email visibility into the SOC/IR process, since a high volume of threats originate there.
3. Review whether your server workloads are being treated as more than just a regular endpoint. Can you see containers, misconfigurations, the dev pipeline?
4. Aim for tight linkage between investigation & automated response functions, for example EPP + EDR, as a foundation for automated XDR response

RSAConference2020

Thank you!

eric_skinner@trendmicro.com
@EricSkinner