Cloud Security Posture Management from Security Hygiene to Incident Response

Yuri Diogenes
Senior Program Manager at Microsoft
Azure Security Center
@yuridiogenes

Jess Huber
Associate Director at Deloitte Touche Tohmatsu Limited
Global Cyber Incident Response

Why security hygiene should be your number one priority?

Cyber Hygiene Fail: Unpatched Vulnerabilities Drive Data Breaches

Research from *Dark Reading* finds that unpatched vulnerabilities are a primary driver of data breaches. In their report, 60 percent of organizations that experienced a data breach cited a known, unpatched vulnerability as the cause.

The number of security professionals who forgo patching vulnerabilities to avoid disrupting the workplace is staggeringly high: Over 80 percent say they've postponed a patch for this very reason at least once.

Source: https://blog.automox.com/bad-cyber-hygiene-breaches-tied-to-unpatched-vulnerabilities

The truth is that the vast majority of data breaches can be prevented with basic actions, such as vulnerability assessments, patching and proper configurations. An Online Trust Alliance study estimated that 93 percent of reported incidents could have been avoided with basic cyber hygiene best practices, a figure that remains largely unchanged in the past decade. While advanced threats are growing in volume and sophistication, organizations are still getting breached due to poor key management, unpatched applications and misconfigured cloud databases.

Source: https://securityintelligence.com/your-security-strategy-is-only-as-strong-as-your-cyber-hygiene/

37% Of Organisations Have Suffered A Cyberattack On Cloud Environments Due To The Lack Of Basic Cloud Security Hygiene

By Outpost24 August 22, 2019 4721 0

Facebook Twitter G in

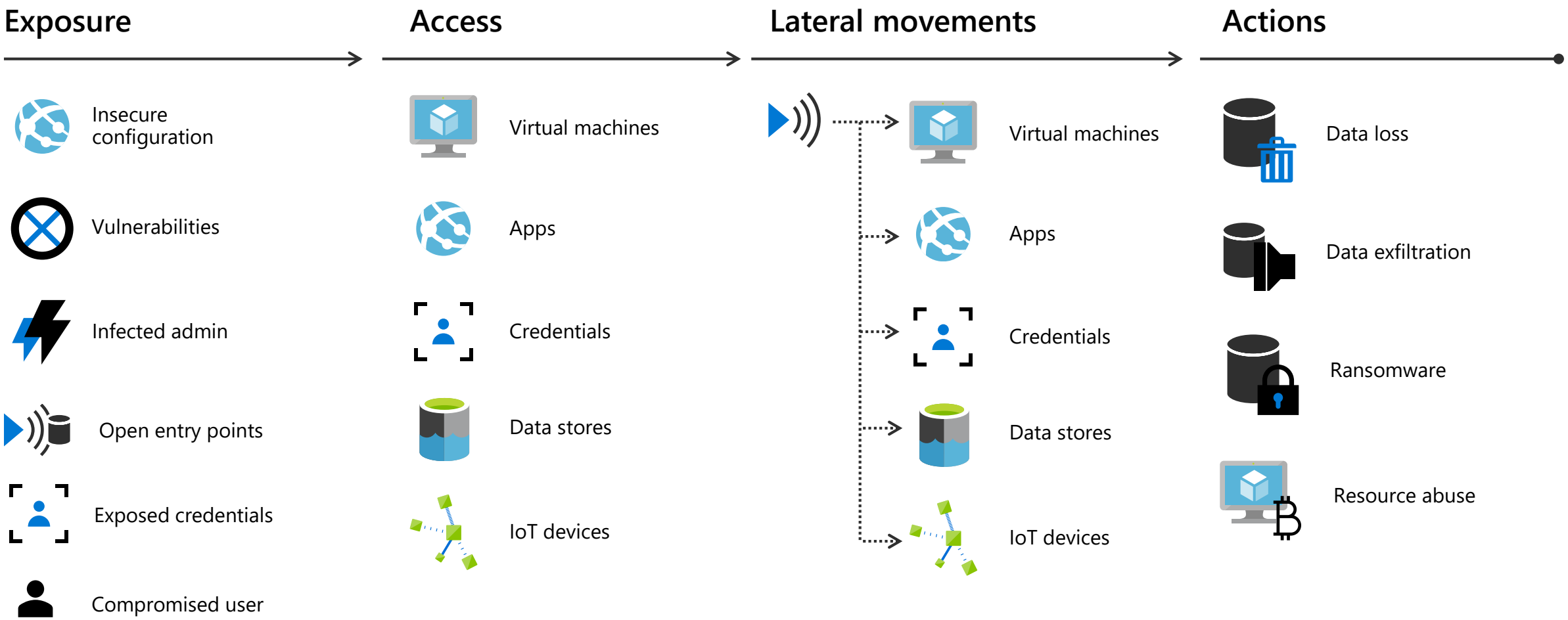
New study reveals 42 percent of organisations are concerned about cloud security but many fail to carry out any security testing on the environment

With the recent exposure of a huge data breach affecting US bank Capital One, cloud security has once again been put under the spotlight. However, a recent survey from Outpost24 has revealed that many companies today would be unable to detect abnormalities in their cloud environment, while 37 percent have already experienced a cyberattack on their cloud systems. As more organisations embrace digital transformation and migrate to the cloud – the results of the survey highlight the lack of security hygiene when it comes to cloud environments.

Source: https://www.informationsecuritybuzz.com/study-research/37-of-organisations-have-suffered-a-cyberattack-on-cloud-environments-due-to-the-lack-of-basic-cloud-security-hygiene/

Traditional defenses are no match for today's challenges

Threat actors leverage a variety of exposures to breach



Improve your defense against threats by enhancing your security posture

PROTECT

across all endpoints, from sensors to the datacenter

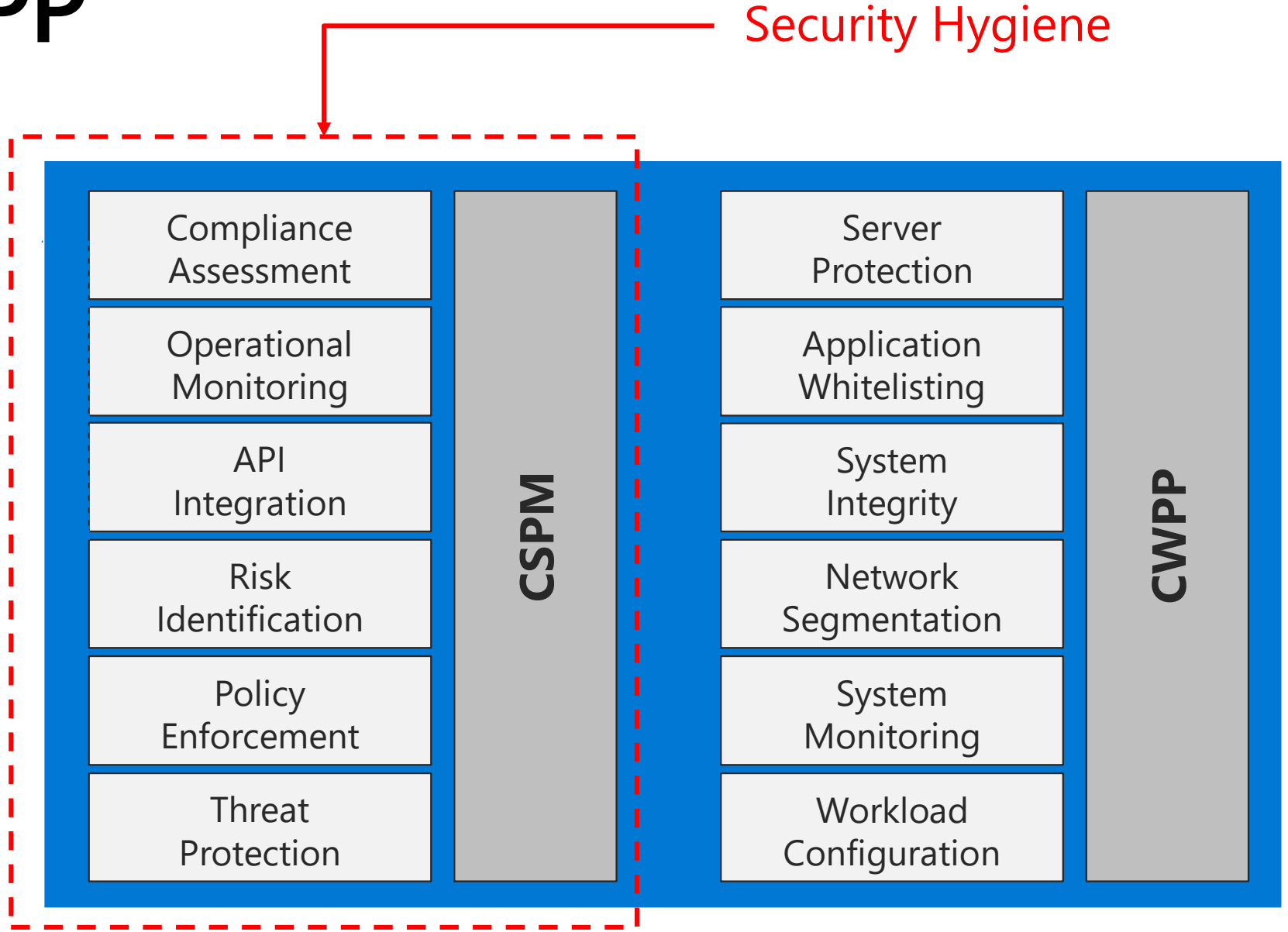
DETECT

using targeted signals, behavioral monitoring, and machine learning

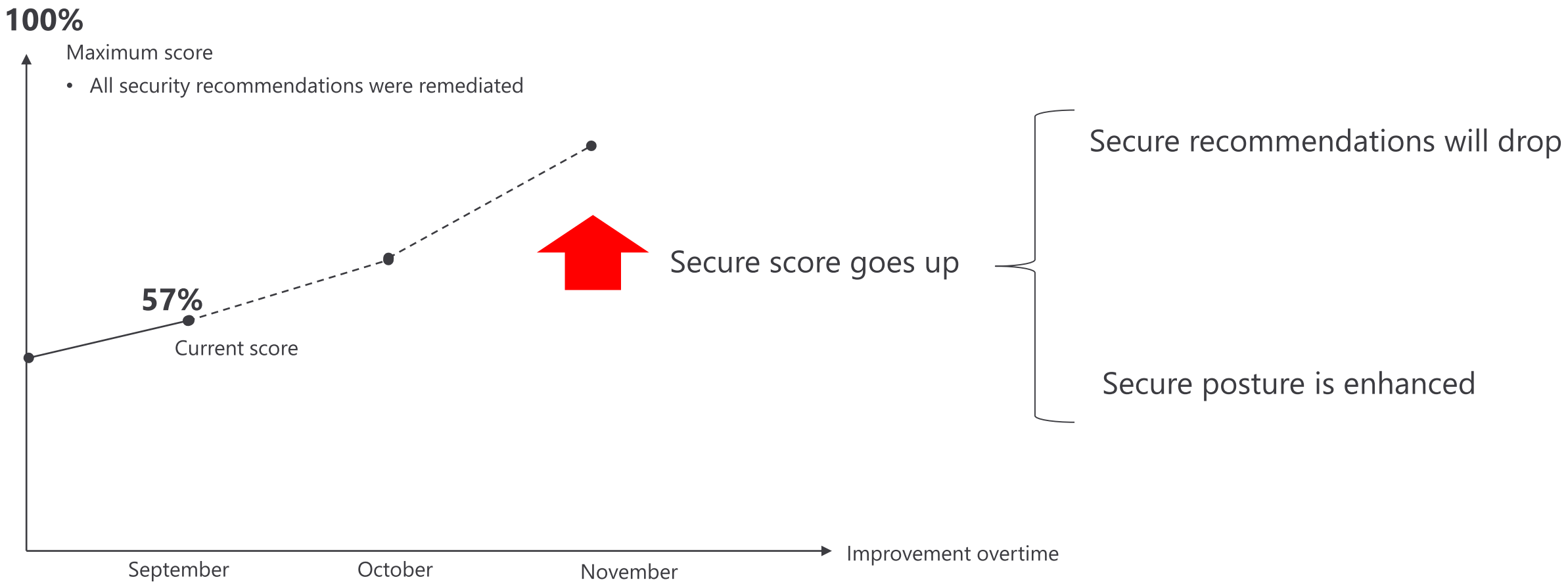
RESPOND

closing the gap between discovery and action

CSPM + CWPP

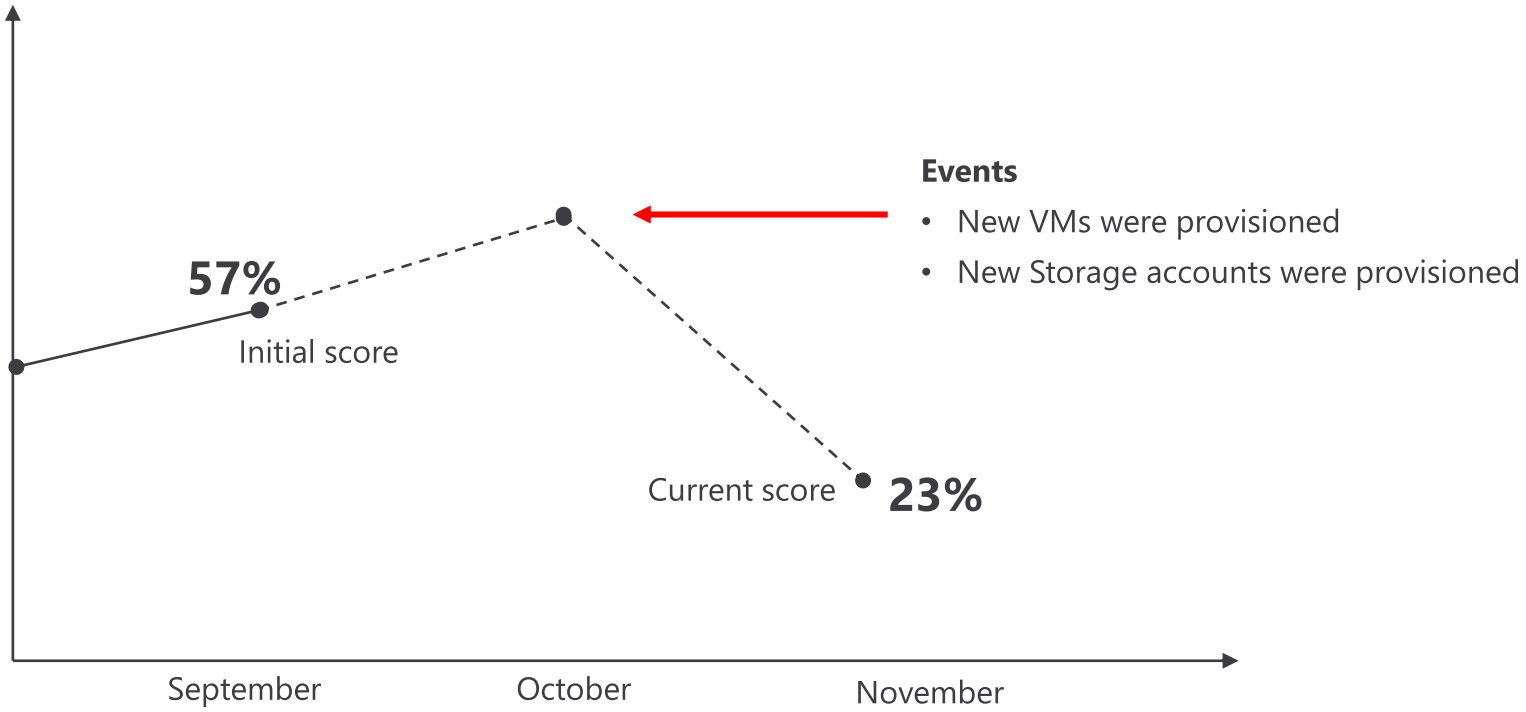

Security Hygiene
Compliance Assessment
Operational Monitoring
API Integration
Risk Identification
Policy Enforcement
Threat Protection
CSPM
Server Protection
Application Whitelisting
System Integrity
Network Segmentation
System Monitoring
Workload Configuration
CWPP

Secure score

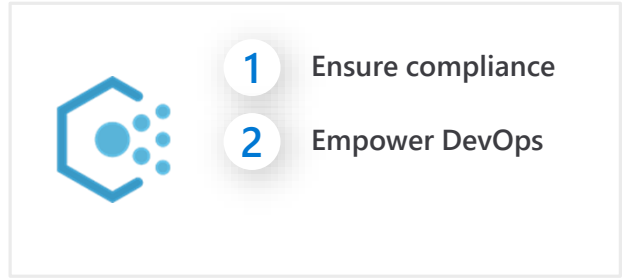


The importance of governance

- Without governance your secure score will drop once you provision new resources that are not secure by default



Policy enforcement



Code

Build/Test

Policy as Code

Pre-flight

Validation

Authoring

Deploy

Operate

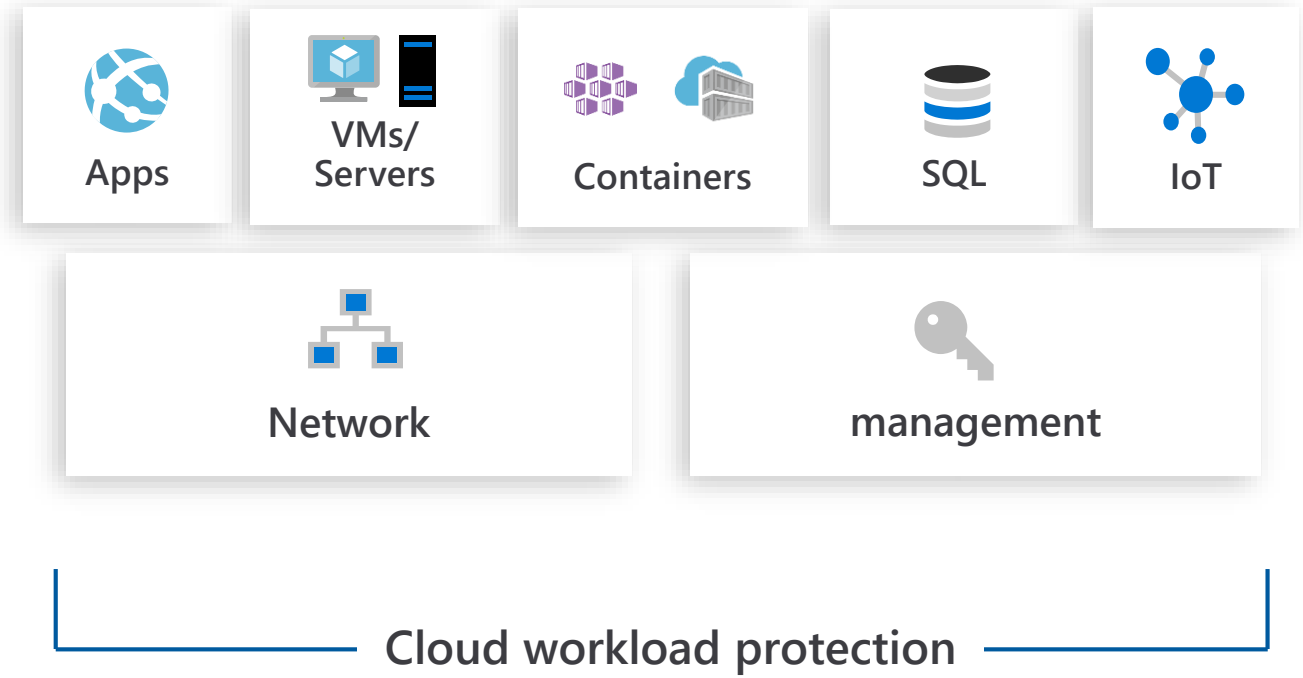
Policy

Security

Monitoring

DevOps + Policy

Protect your workloads from threats



Intelligence and advanced analytics

Threat intelligence

Anomaly detection

Uses statistical profiling to build historical baselines

Alerts on deviations that conform to a potential attack vector

Behavioral analytics

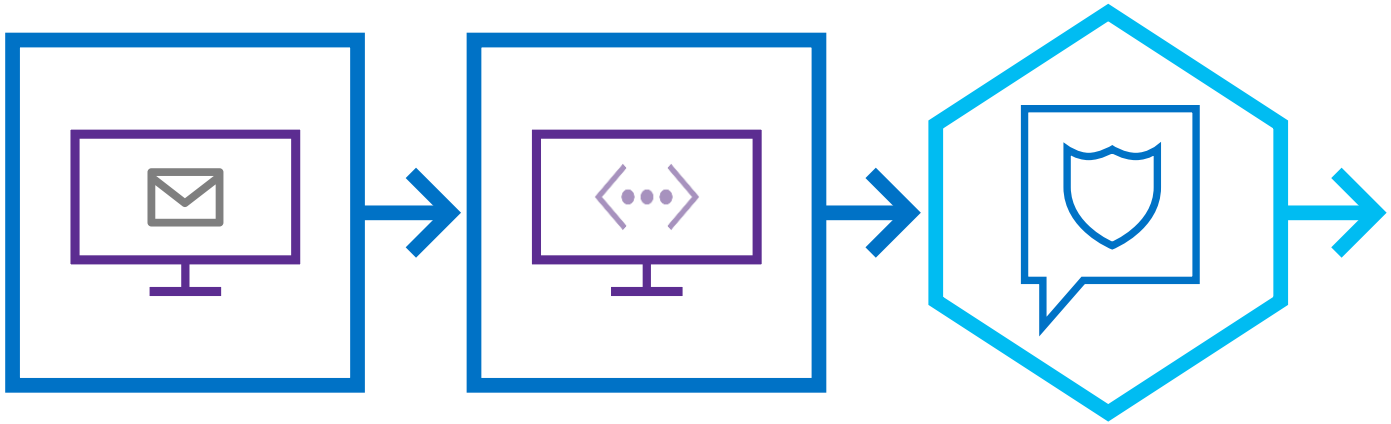
Looks for known patterns and malicious behaviors

Correlation

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

Example of built-in analytics and machine learning

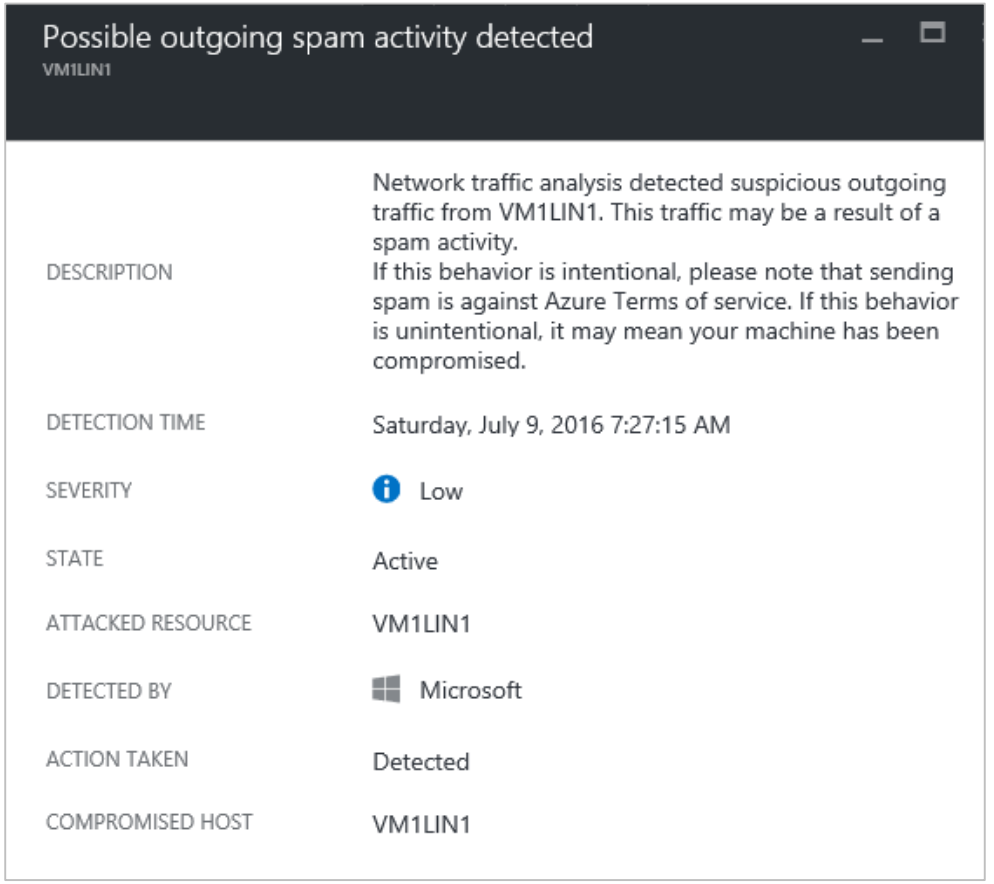
Outbound SPAM scenario



An attacker gains access to a VM and begins to send spam emails.

CWPP uses machine learning detects a spike in SMTP traffic.

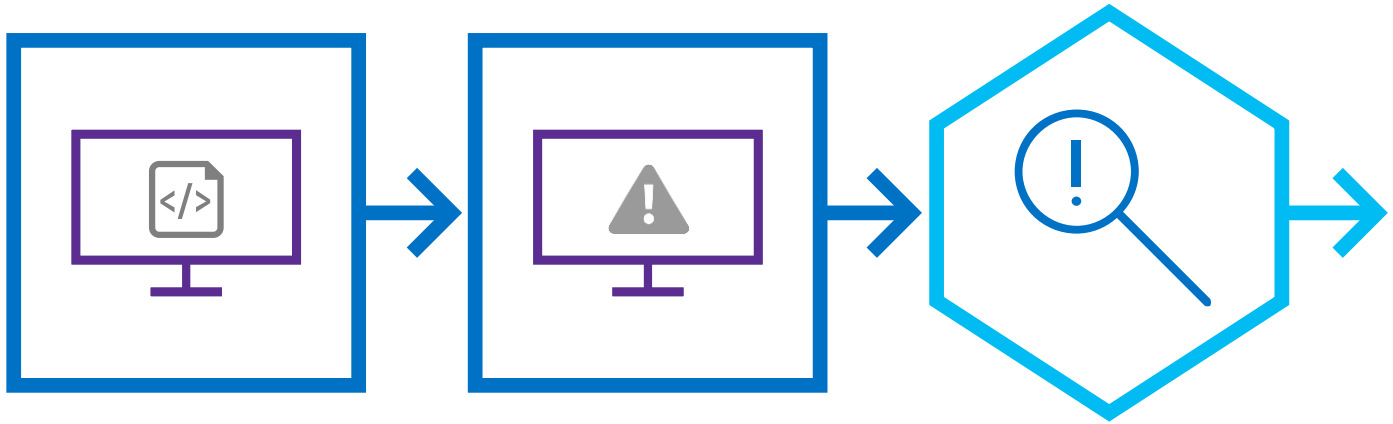
Traffic is correlated with TI database to determine if the traffic is likely legitimate or not.



High fidelity alert is triggered

Sample Scenario: Crash dump analysis

In-memory malware and exploit detected using crash analysis

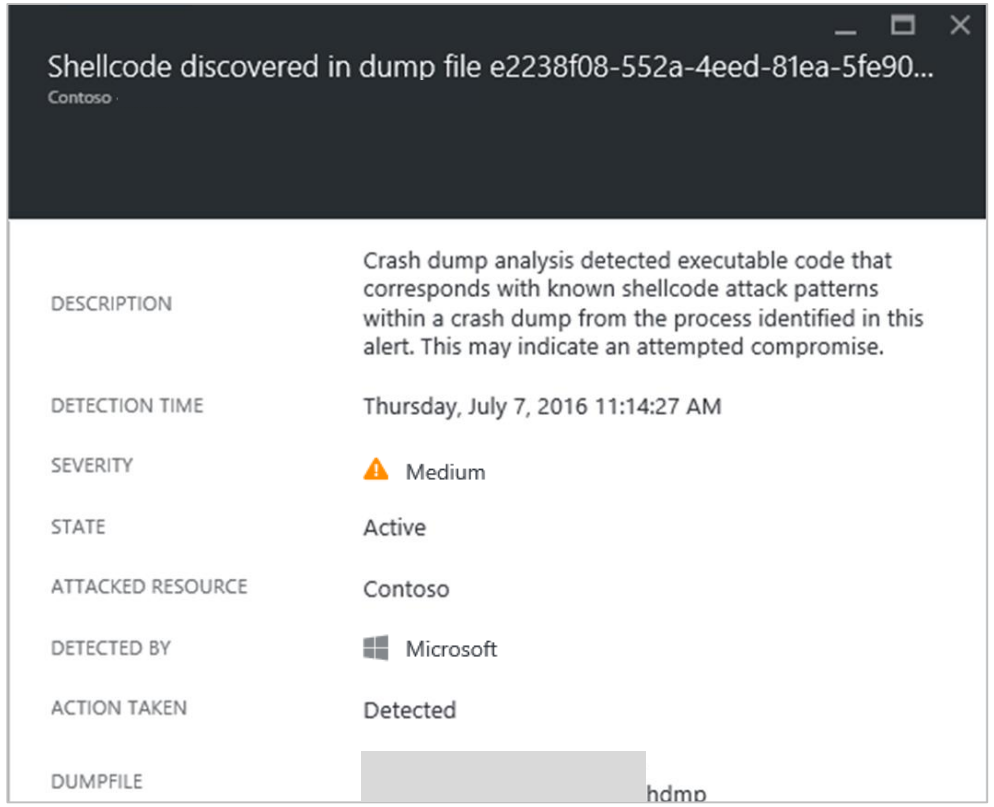


An attacker gains access to a VM and installs malware undetected.

A malicious or non-robust program causes a crash.

Windows Error Reporting generates a memory crash dump.

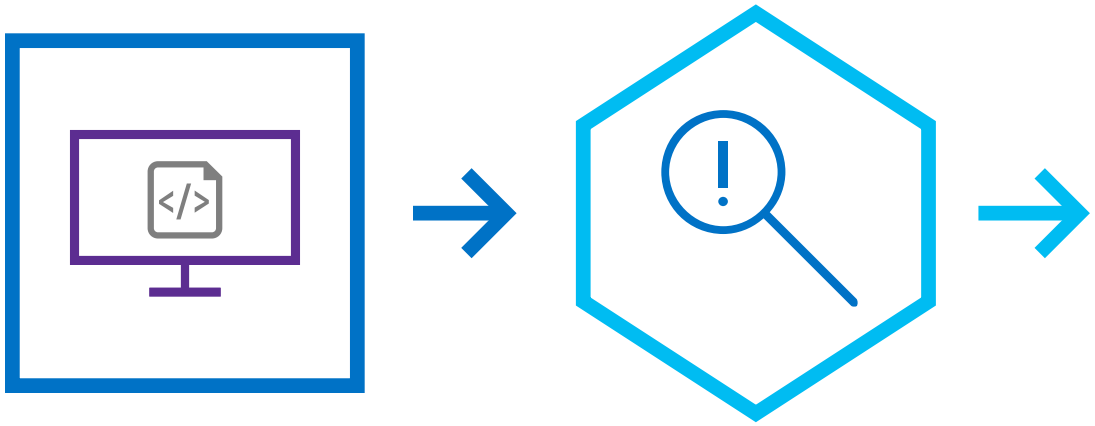
CWPP collects an ephemeral copy of the crash dump and scans it for evidence of exploits and compromises.



High fidelity alert is triggered

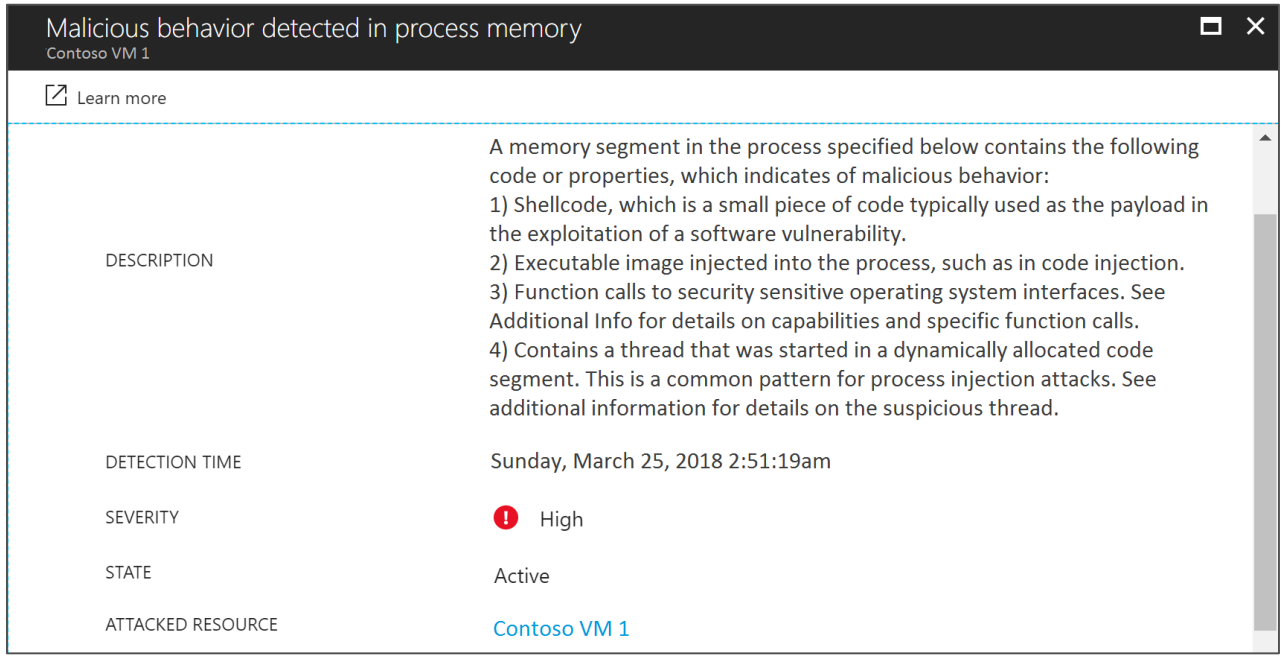
Detecting file-less attacks

Detect malicious code in-memory



An attacker gains access to a VM and injects malicious code into memory

CWPP scans process memory to identify evidence of exploitation and malicious code



Incident Response in the Cloud

Jess Huber

Success…

“Success is the ability to go from one failure to another with no loss of enthusiasm.”
–Winston Churchill

Incident Response…

“Incident Response is the ability to go from one dumpster fire to another with no loss of enthusiasm.”
–Jess Huber

Agile detection, rapid response, force multiplication & why they matter...

24 JUL 2019 NEWS

Cybercrime Costs Global Economy $2.9m Per Minute

https://www.infosecurity-magazine.com/news/cybercrime-costs-global-economy/

The Cybersecurity Skills Gap Won't Be Solved in a Classroom

https://www.forbes.com/sites/martenmickos/2019/06/19/the-cybersecurity-skills-gap-wont-be-solved-in-a-classroom/#7eed3bdb1c30

The human cost of cybersecurity attacks

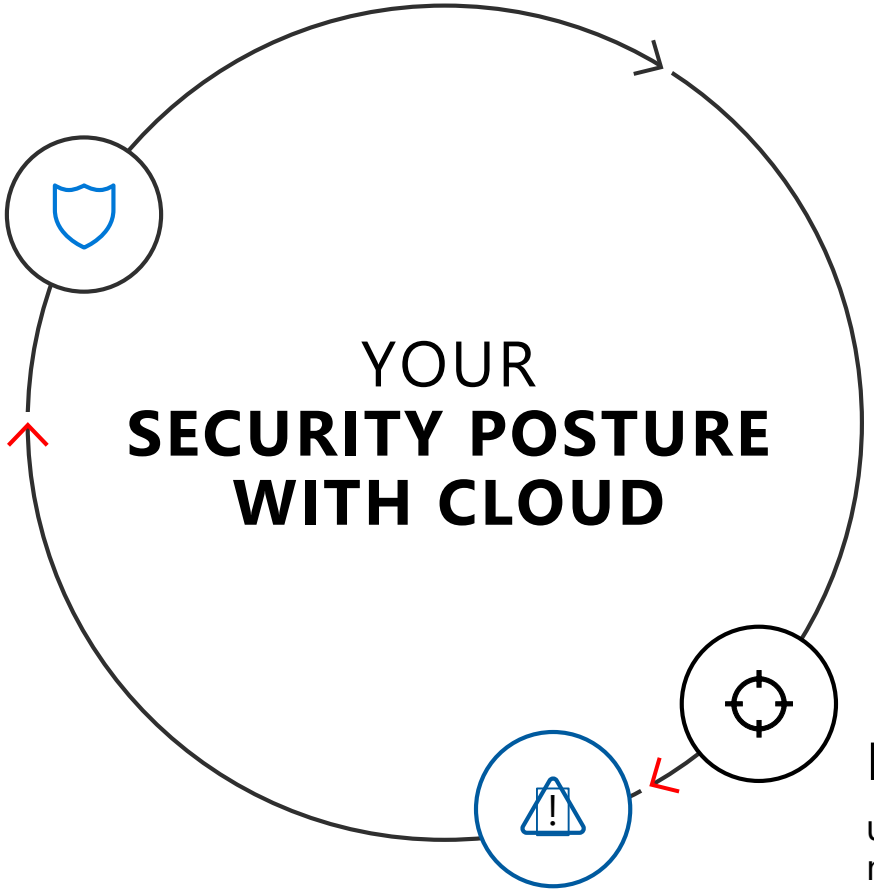
By Chris Ross October 15, 2019

https://www.techradar.com/news/the-human-cost-of-cybersecurity-attacks

The gap, the significant emotional event, & what to do next...

PROTECT

across all endpoints, from sensors to the datacenter



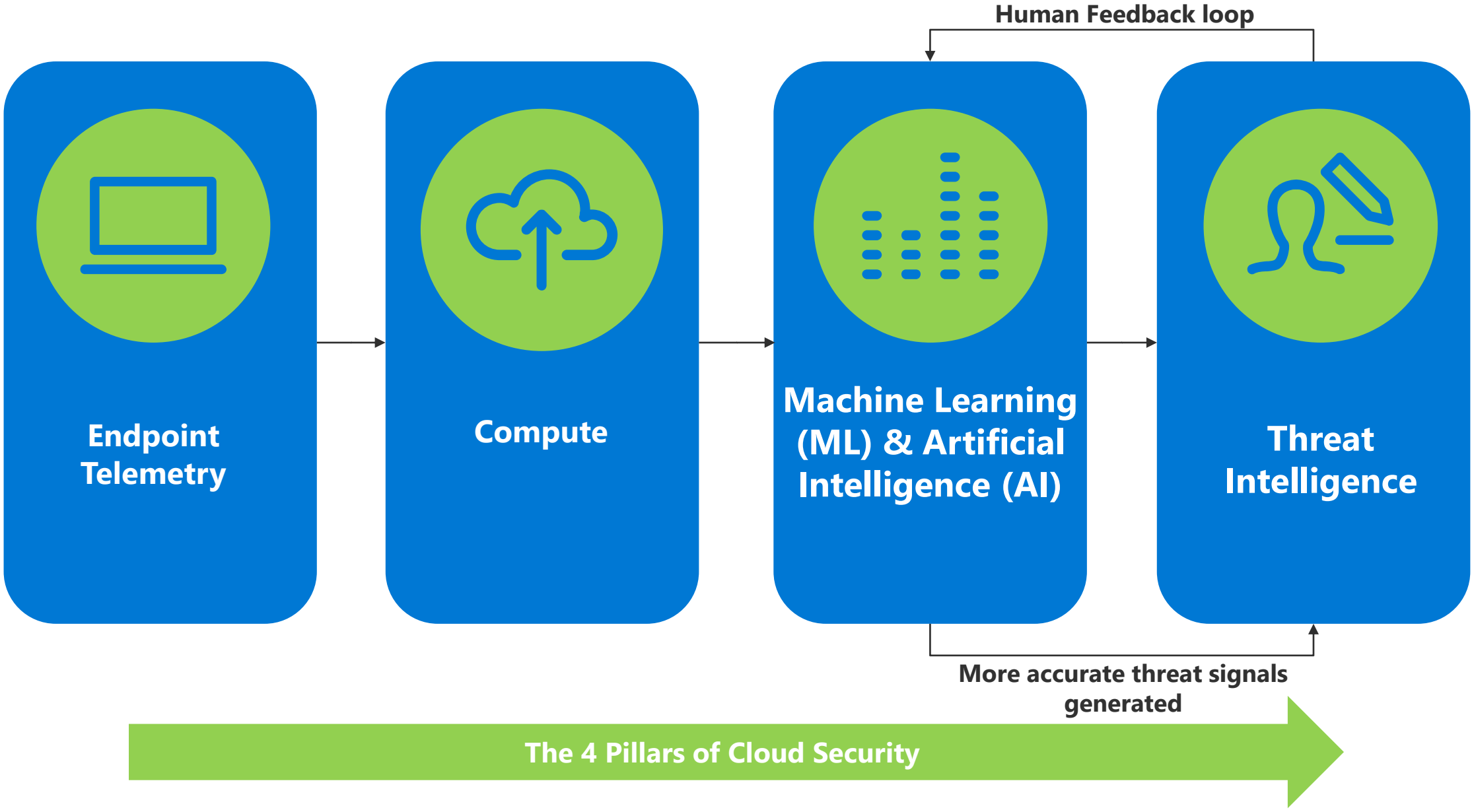
DETECT

using targeted signals, behavioral monitoring, and machine learning

RESPOND

closing the gap between discovery and action

Cloud Security Fundamentals



"When you reach the end of your rope, tie a knot & hang on." ~Abraham Lincoln

If you have to choose the 2 most effective cloud tools in an incident responder's arsenal, sharpen your skills on:

- The EDR solution
- The UEBA solution
  - A force multiplier when the two are integrated

EDR basics…

- EDR console access:
  - Leverage dedicated admin workstations
  - Enforce MFA on EDR console access
- Automate “commodity” detections/remediation whenever possible
- Regularly monitor for anything anomalous auto-starting on key systems such as; identity stores, VM hosts, software distribution systems, other key IT admin systems, & VIP systems (C-suite, IT staff, etc.)
- Alert on potential web shells (Example: W3WP spawning CMD)
  - Web shell activity is usually “targeted” activity more often than not

UEBA basics…

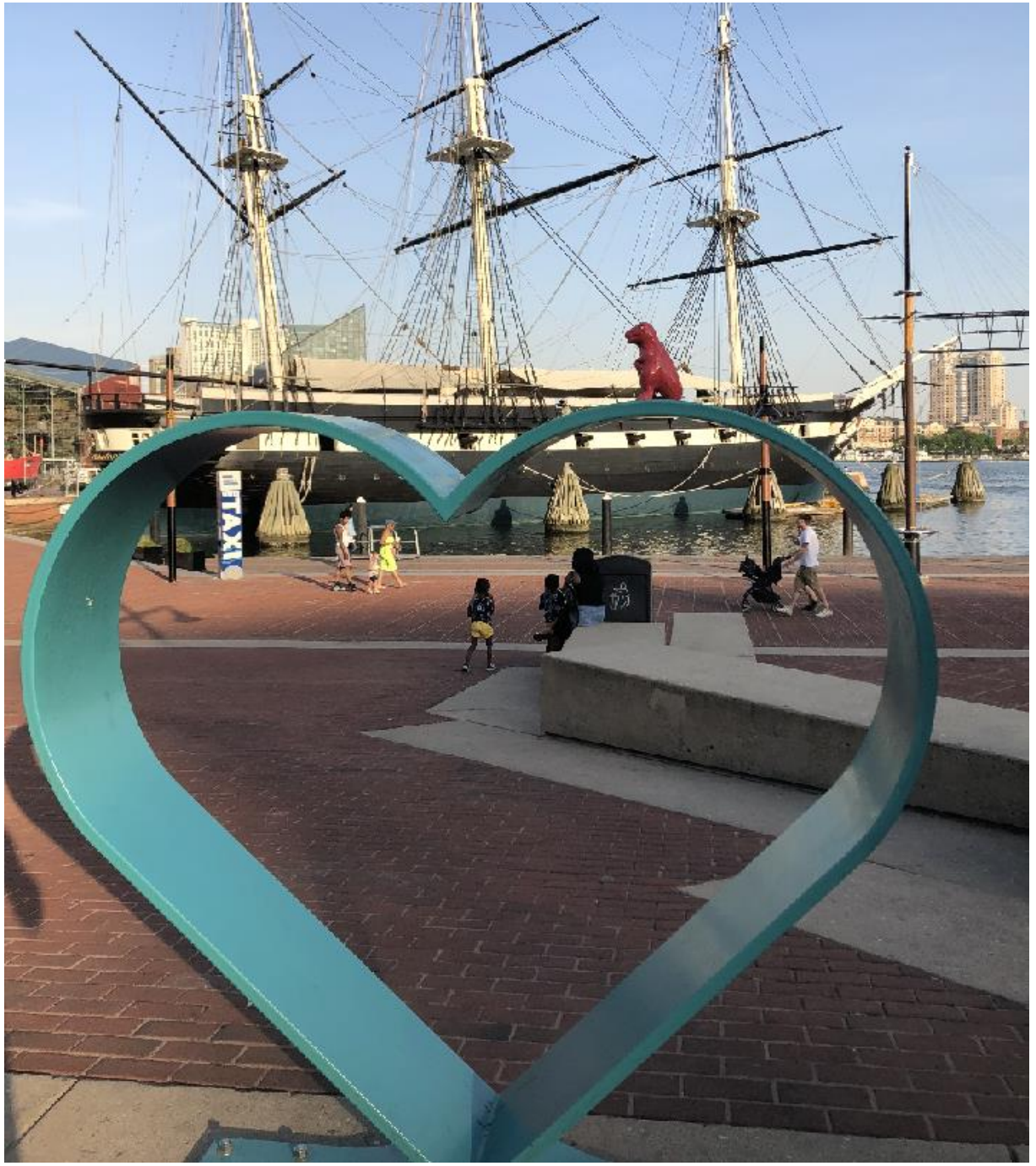
- UEBA console access:
  - Leverage dedicated admin workstations
  - Enforce MFA on UEBA console access
- Focus on the identity…

  "You will lose sheep. It is when you loose shepherds that you have a problem."

  ~Me loosely quoting a friend that loosely quotes other people
- For example…your UEBA solution should be able to detect basic things like 'NTDS.DIT being copied to a workstation'…
  - …that establishes an SSH connection to a Linux server with a SSH forwarder that auto-forwards that DIT to an unknown location on the web for…um…a "cloud enabled backup"? ☺

Target vs Commodity

- This is a loaded question for senior leadership & IR teams around the world.
- Why define & plan for a targeted attack?
- What about attribution really matters to an incident responder?
- How should we initially respond to a “targeted” attack?



What is “Targeted” & who can I blame?...

- At the most basic level, targeted = hands on keyboard
  - Custom implants (onprem)
  - Intent + Access (malware is not needed to persist)
- Your organizational leadership & IT staff will have to determine what is considered targeted
- Attribution in virtually all multi-nationals does not matter as there are really 2 types of adversary that can dictate the response:
  - Is the adversary’s intent to get disruptive or destructive?
  - Is the adversary’s intent to run silent & run deep (undetected) to allow for multi-stage campaigns?

If targeted, immediately switch to an OoB (Out of Band) comms channel…

1. Whip out a credit card & establish a new collaboration platform that provides basic services such as email & document collaboration
2. Send an SMS message to key stakeholders with a flash notification of the incident & how to access the OoB channel leveraging only the cell provider (avoid using domain joined systems)
3. Issue newly built laptops complete with BIOS flash and fresh OS build using known good OEM media for the remainder of the investigation, compromise recovery, planned eviction date, & subsequent tactical monitoring

Key Takeaways

- Good hygiene comes first, strengthen your cloud security posture
- Continuous measure the enhancement of your cloud security posture
- Make sure you have native threat detection for your cloud workloads
- Reduce the attack surface of your workloads
- Move endpoint telemetry to the cloud & fine tune your alerts
- Master the basics of your EDR & UEBA solutions
- Define what you consider “commodity” alerts & “targeted” activity
- Smoke test your out-of-band alert & comms channels

Ricardo Bruno

Information security professional with over 20 years of experience. He currently works as a Principal Security Architect at Fanatics Inc., the global leader for licensed sports merchandise, where he provides expertise in various areas including but not limited to e-commerce fraud, platform security, secure cloud computing, and incident response. He has previously co-founded and ran the security consulting firm ActiveSec, Inc in California where he helped multiple global Fortune 500 organizations improve their posture in areas such as vulnerability management and incident response. Mr. Bruno holds the Certified Information Security Manager ("CISM") credential and thrives in solving and anticipating ever-changing security challenges.

Q&A?