SOCSoter

BERRY SOLUTIONS GROUP

Vulnerability Management System

Always On Continuous Monitoring

Threat Hunting

SOCSoter

Part 1 Agenda

- Intro – Melissa Kaiser
- Old scanning vs Always On
- How it works
- Benefits

BERRY SOLUTIONS GROUP

Stay Ahead of Vulnerabilities

BERRY SOLUTIONS GROUP

BEFORE:

Monthly Scans

Wait 30 days to see problems…talk about reacting…and then try to solve the problems before the next report.

NOW:

Always On

See a problem, react immediately…
problem solved.

The combination of always on detection of vulnerabilities plus SOC expertise helps organizations close the gap on security weaknesses quicker than ever before.

Routine Scans Miss Vulnerabilities

Always On Continuous Monitoring is the KEY to fast & reliable remediation for vulnerabilities.

SIMPLE → SECURE → CONSTANT

- Faster Notification & Remediate closer to detection times
- Real Time Updates
  - Vulnerabilities are continuously added to the VMS data feed as they are published.
  - No need to sync or update.
- Always On Vulnerability Scanning consists of one full scan of each connected endpoint a day; meaning a host fingerprint and credentialed vulnerability scan daily.

Evolve Your Network Security

Always on + Security Operations Center (SOC) helps organizations reduce the timeline for security weaknesses quicker than ever before.

- Installed as a virtual machine or dedicate any windows device as a scan sensor.
- Newly identified devices are scanned first to shorten the time from detection to getting a full security assessment of a device and the risks it poses to the network.
- Prioritize refresh of older scan data to ensure a full 24 hour cycle.

Close vulnerabilities before exploitation

BERRY SOLUTIONS GROUP

Risk

- Prioritize remediation based off vulnerability criticality and the value of assets
- Operationalize remediation based off organizational risk tolerance and project plan requirements
- Monitor the effectiveness of patch management programs and tools

Compliance

- Always On Vulnerability is CVSS Version 3.0 Compliant
- Compliance frameworks require scans when new vulnerabilities are identified and remediated according to organization policies
- Vulnerability Management is required by most security compliance frameworks

Part 2 Agenda

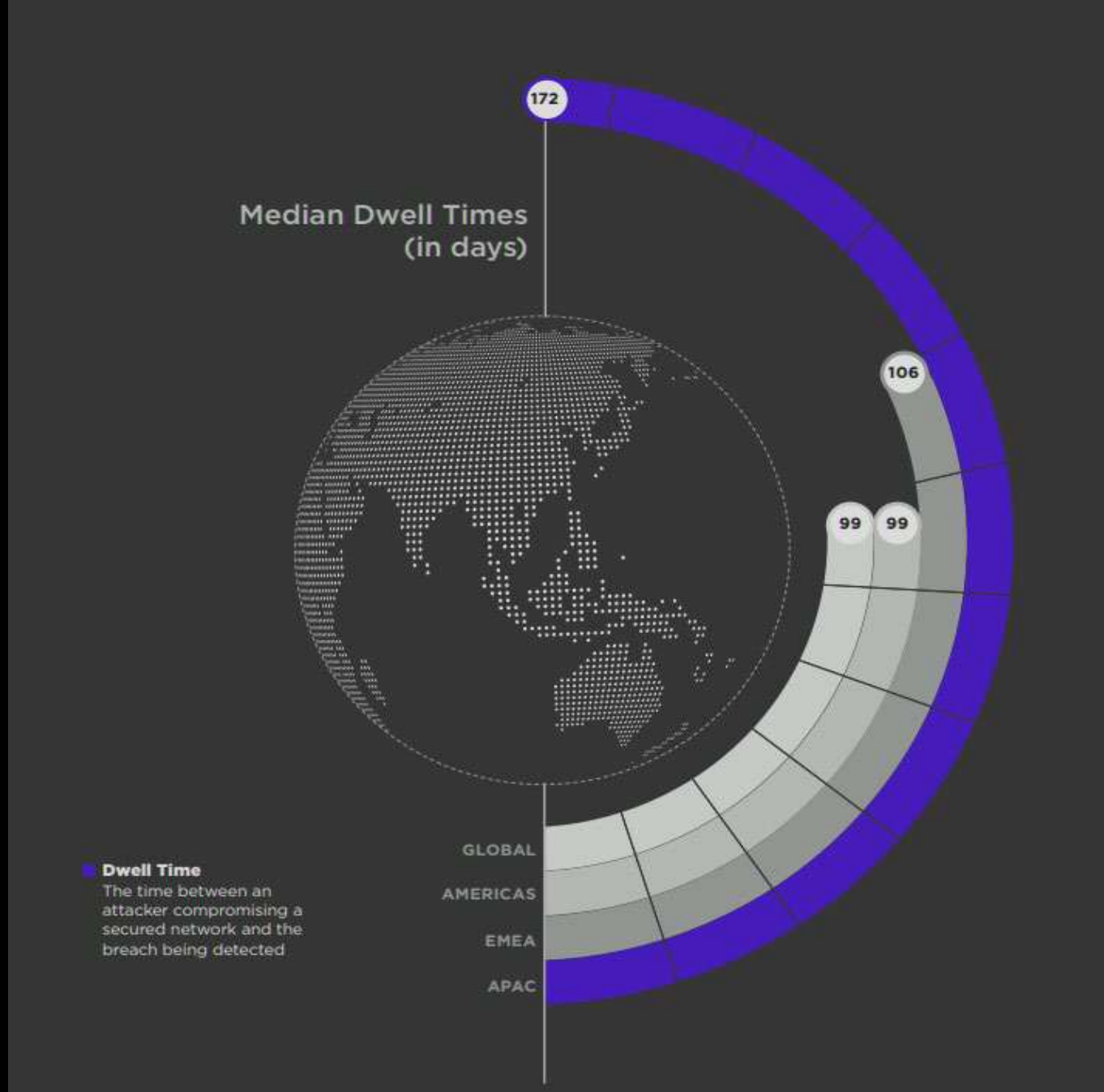
- Intro – Trevin Mowery
  - Background
- What is threat hunting?
- Why is it important?
- Difference between Threat hunting and Vulnerability scanning
- How to pair it with other proactive security measures such as vulnerability scanning

What is threat hunting?

- Called several different names, compromise assessment, threat hunt, etc.
- Searching environment for unknown badness
- No reliance on real-time detection
- Based on anomalies or strange behaviors
- Heavy focus on unusual process behavior
  - Mitre Attack Framework
- Manual process
  - Automated threat hunt = BEWARE
- Generates
  - Tactics, Techniques, and Procedures (TTPs)
  - Indicators of Compromise (IoCs)
  - Confirmed incidents, initiating an incident response

Why should we do threat hunting?

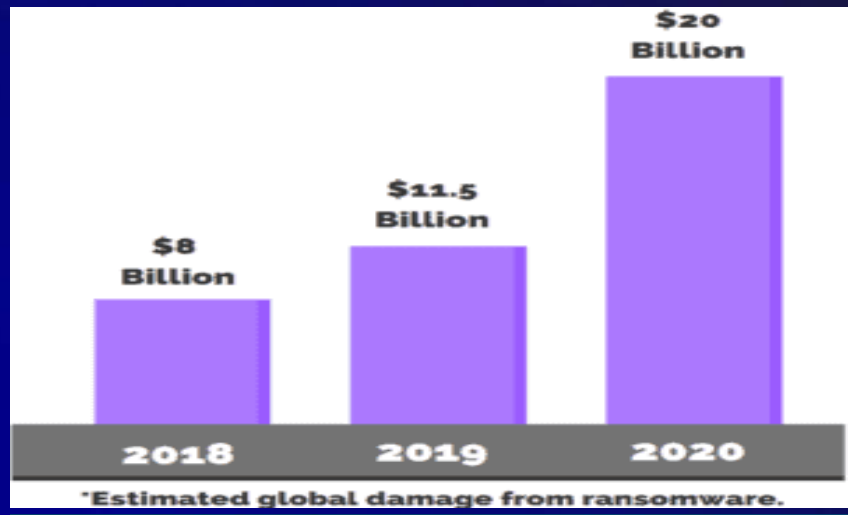
- 2020 Dwell time was 56 days
- 2021 Dwell time is 280 days



Source: Verizon DBIR 2019 report, IBM, FireEye

Industry Stats

- Cybercrime is up 600% due to COVID 19
- 230,000 new malware samples are produced every day
- 18 million websites are infected with malware at a given time each week
- 75% of companies infected with ransomware were running up-to-date endpoint protection
- Average cost of a ransomware attack is $1.85 million
- Credentials are the #1 sought after data followed by PI
- 47% of companies have had at least one employee download malware

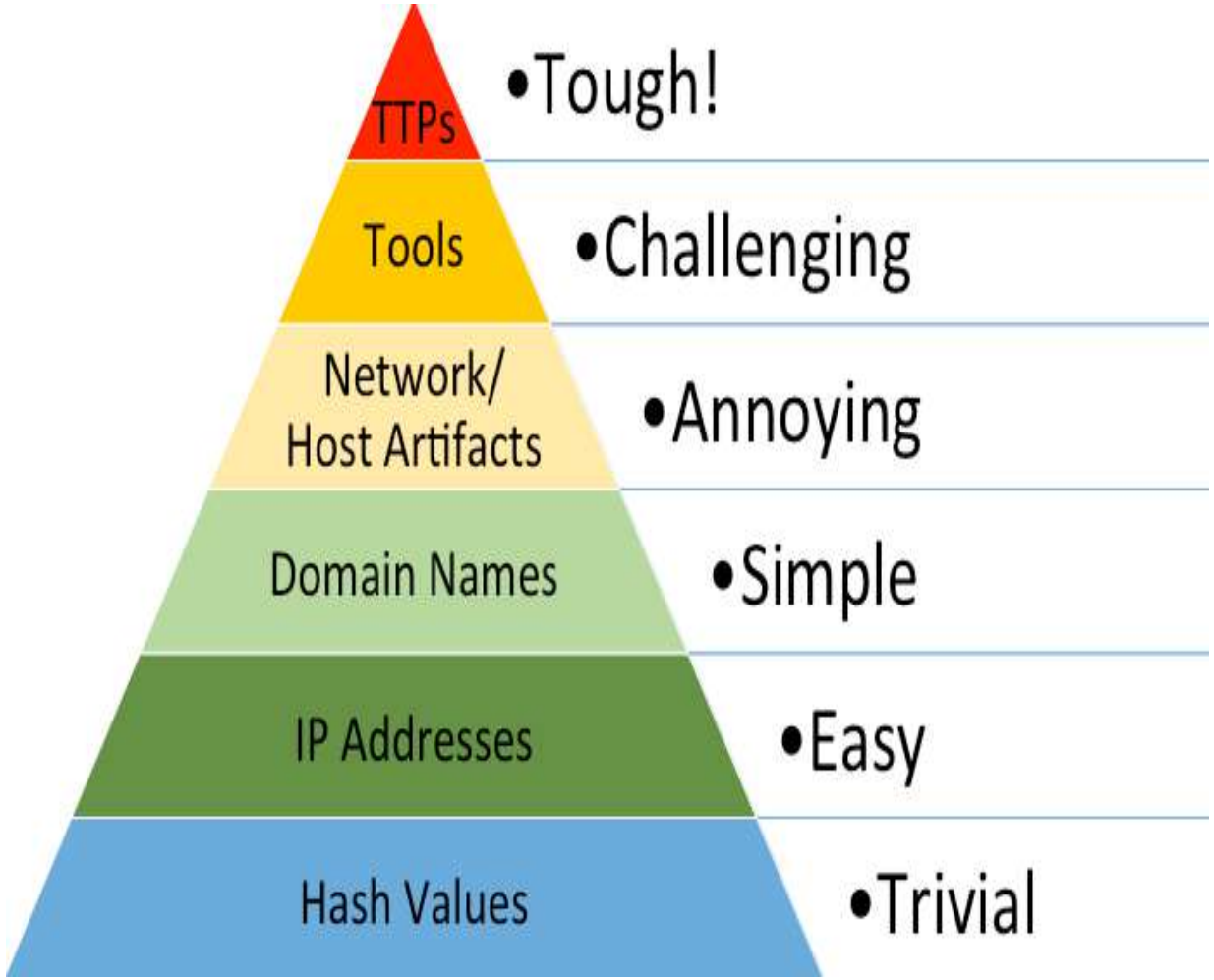


Source: Purplesec.us
Verizon data breach report 2021

TTP's are Better

Comparison between IOCs & TTPs

IOCs	TTPs
Detective in nature	Descriptive in nature and define characterization on abnormal behavior
More false positive alert	Less false positive alerts
Specific to one attack	Covers entire attack family depending on behavior pattern
Reactive	Proactive



OpenText Threat Hunt Case Study

A managed service provider

20,000 endpoints

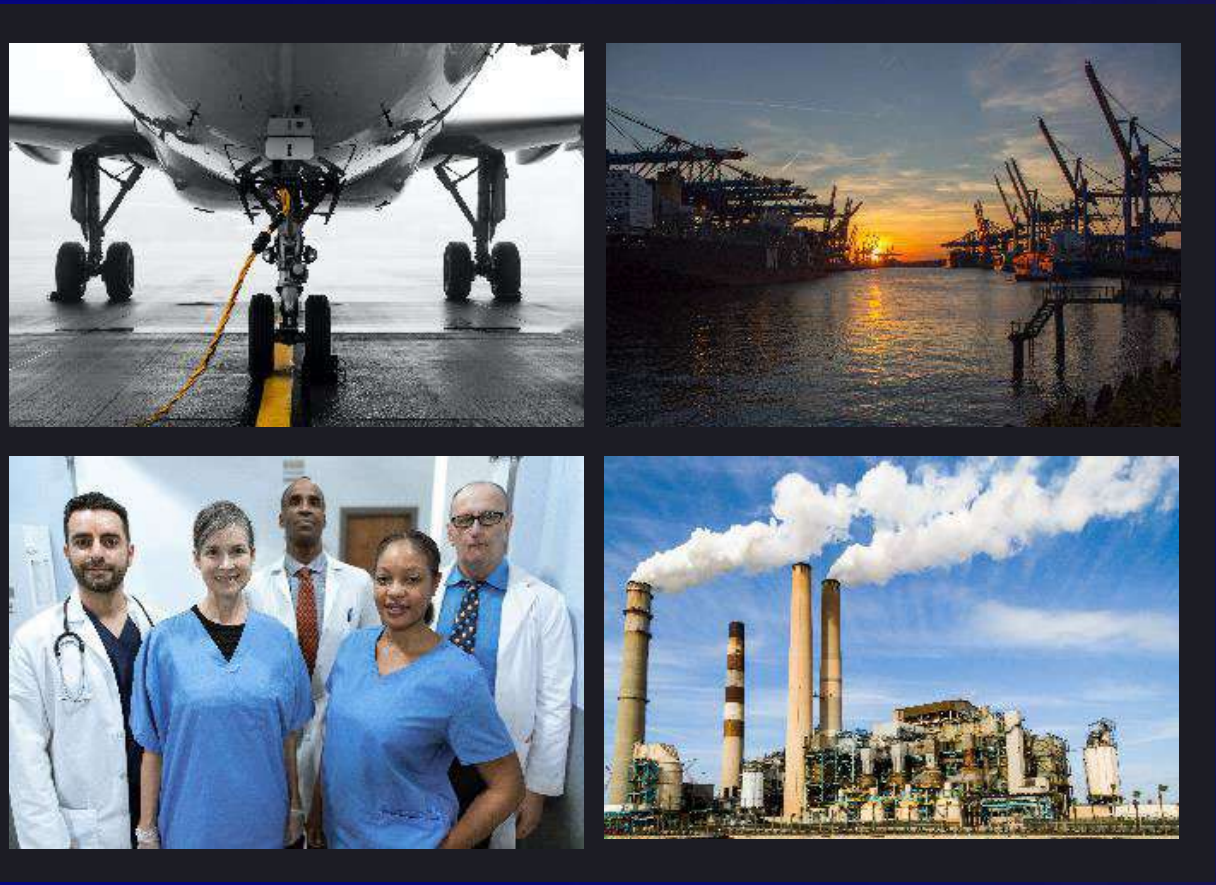
During a Threat Hunt OpenText alerted that the customer had a server with RDP open to the internet

Identified 412 different IP's were performing a brute force on a server

Within 4 hours of installing our EDR Agent:

- Identified lateral movement
- attackers were stealing domain privilege credentials
- Stealing password from more than 30 applications and browsers

OpenText threat hunters were able to work with the customer to remediate these attacks and stop them before any data exfiltration occurred



Threat Hunting vs. Vulnerability Scanning

- Vulnerability scanning identifies vulnerabilities that **could be** exploited
- Threat hunts identify when a vulnerability or misconfiguration **has been** exploited
  - Usually yields more critical findings
- Can use info from vuln scans to see if things have been exploited – Exchange vuln of 2021, Sunspot/Sunburst, log4j, etc.
- Both are important as well as other proactive security activities such as:
  - Penetration testing
  - Threat emulation activities
- Be aware when each is going on.
  - Don't want to sound alarms when a threat hunt identifies mimikatz which is actually a red team engagement
- "According to the cybersecurity resource allocation and efficacy index (Q2 2020), the COVID-19 pandemic greatly increased the use of remote, proactive cybersecurity measures. 66.4% of survey respondents from across North America and Europe increased their proactive risk identification spending shortly after the outbreak, and 76.5% reported an increase in cybersecurity efficacy during the same time." (1)

1. Source:https://www.travasecurity.com/resources/7-benefits-of-proactive-cybersecurity

Thank you

Questions?

Trevin Mowery

tmowery@opentext.com

Melissa Kaiser

mkaiser@socsoter.com