1

Security Fitness - Topics

- Cyber Security Planning for Compliance and Security
- Emerging Technologies
- Security Information Event Management (SIEM)
- Endpoint Detection and Response (EDR)
- Cyber Incident Review of a Real-World Hack

2

Planning for Compliance and Security

CYBERSECURITY CHALLENGES

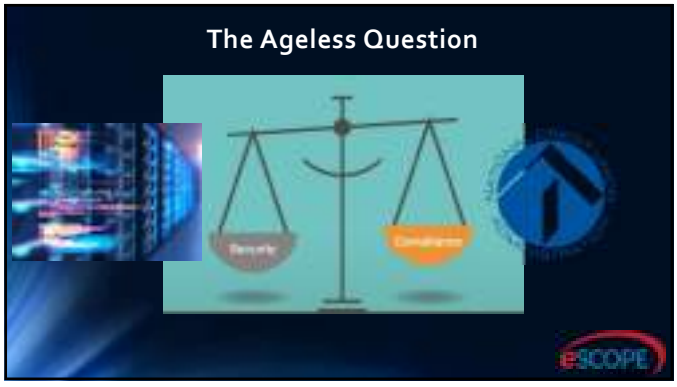
3


Privacy Challenges
110 Million People
Passwords
Regulations
Biometrics
eSCOPE

4


Ransomware:
An Familiar Expensive Threat
Threat Finder
WARNING!
Sunday
Payment
eSCOPE

5

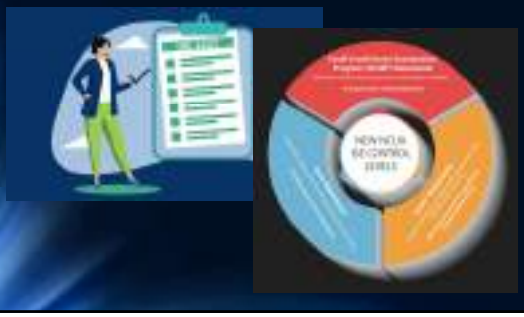

The Ageless Question
eSCOPE

6

It All Starts at the Top!

7

Compliance: IS Exam – *New & Improved*



8

NCUA IS Exam 2024 – Control Levels

9


Emerging Technologies
TODAY'S ENTERPRISES FACING NEW CHALLENGES
eSCOPE

10


Detect
Protect
Enforce
Dropbox
OneDrive
box
slack
zendesk
Cloud Computing in the Enterprise
eSCOPE

11


Cloudy Weather with a Chance of a Breach
What is Cloud Jacking?
Cloud jacking is when an individual or business Cloud Account is taken over by a cybercriminal.
eSCOPE

12


Artificial Intelligence is Here to Stay!
data
hack
hackers
password
AI, friend or foe?
danger
attack
eSCOPE

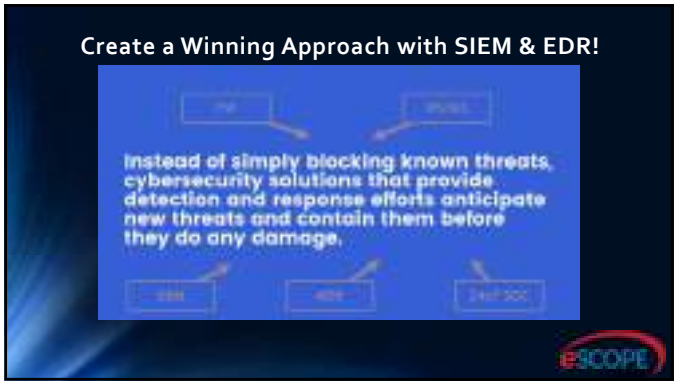
13


ChatGPT & Friends
Generative AI is the new strategic battleground
AI
eSCOPE

14


AI Can Strengthen Risk Management Tools
AI in CyberSecurity
eSCOPE

15


Create a Winning Approach with SIEM & EDR!
Instead of simply blocking known threats, cybersecurity solutions that provide detection and response efforts anticipate new threats and contain them before they do any damage.
eSCOPE

16


Managed SIEM
TIPS FOR SUCCESS
SIEM
eSCOPE

17


What is a SIEM?
Security Information and Event Management
A SIEM works by collecting log and event data generated by an organization's systems, devices, and applications and brings them into the centralized platform for analysis and reporting.
When the SIEM identifies a threat through a set of predetermined rules, an alert is generated for human review.
Why do I need it?
Auditing and Compliance Requirements
Full Visibility of Everything Happening Within the Network
Dramatically Decreases the Time it Takes to Identify Threats
Detailed Forensic Analysis in the Event of Major Security Breaches
eSCOPE

18


Physical Security

19

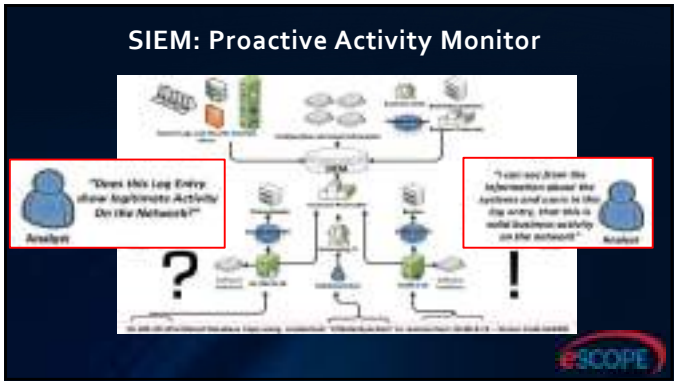

Cyber Security

20


SOC
SIEM Adds Invaluable Compliance Functions

21

SIEM: Proactive Activity Monitor



22

Managed EDR

TIPS FOR SUCCESS

23

What is EDR

- Endpoint Detection and Response works by monitoring endpoint activity and storing the information on a centralized database for analysis, investigation, and reporting.
- This is done through machine learned, behavior-based monitoring in which the software looks for why something is happening on the endpoint, and not just what is happening.

Why Do I Need It?

- Behavior based monitoring of threats.
- Real-time response and remediation.
- Comprehensive endpoint data collection.
- Integration with other security solutions.

24

Why isn't Traditional Anti-Virus good enough anymore?

In short, it comes down to the key differences between the core functionality of traditional AV and an EDR solution.

Traditional AV	EDR
• Can only detect previously known threats • Can't detect unknown threats	• Can detect previously known and unknown threats due to behavioral based monitoring
• Minimal to no data collection	• Complex and detailed endpoint data collection
• Minimal to no added features or benefits	• Added features and benefits including application monitoring, threat hunting capabilities, and advanced reporting.

25

Overnights, Weekends & Holidays?

26

How the eScope MDR Works

Remediation on your behalf

This includes:

- Stopping all processes related to the threat.
- Encrypting and quarantining the threat and its executables.
- Disconnecting the system from the network to prevent spread of malicious activity.
- Deleting files and system changes created by the threat.
- Restoring files and configurations that the threat had changed.

27

EDR & SIEM: Why Together?

- Wholistic, Layered Approach – They are complimentary to each other, not replacements for each other
- A well designed EDR solution SHOULD outperform SIEM in prevention
  - Full & Incremental Scans
  - Simpler to react to events
- A well designed SIEM solution SHOULD outperform EDR in detection
  - Simpler to correlate multiple data sources
  - Yields actionable context and supports log enrichments

28

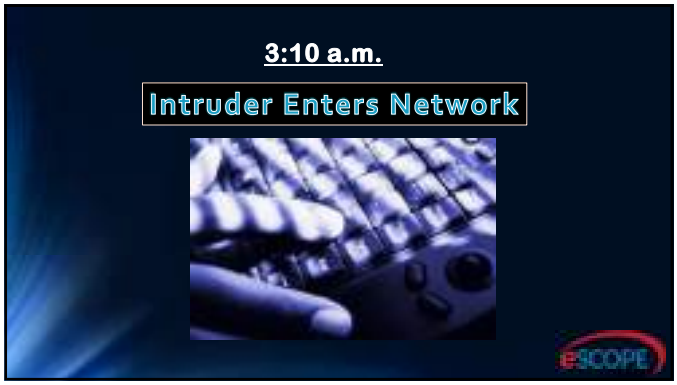
It's Only Friday Night Marshmallows!

29

Anatomy of a Breach

A CLOSER LOOK

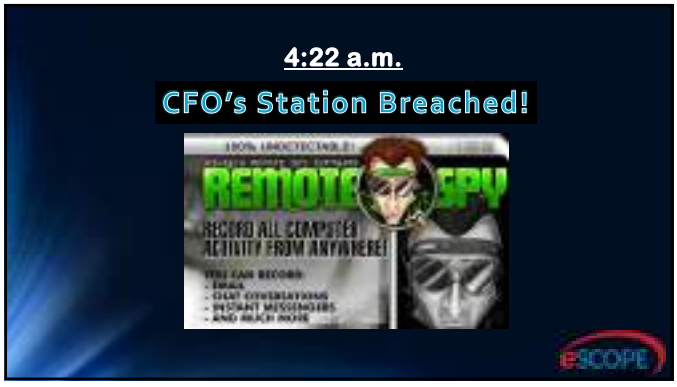
30


3:10 a.m.
Intruder Enters Network
eSCOPE

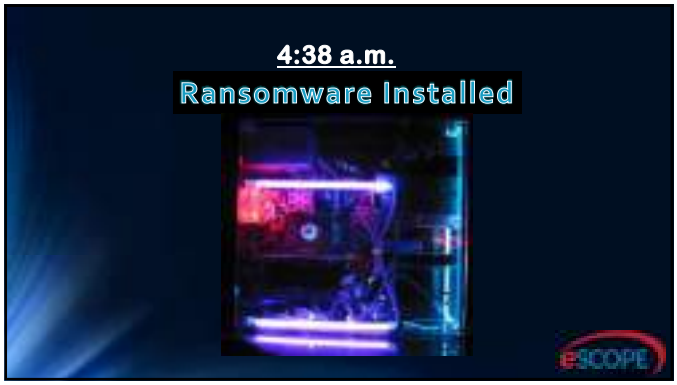
31


3:58 a.m.
Database Files Accessed
Exfiltration Warning
eSCOPE

32


4:22 a.m.
CFO's Station Breached!
eSCOPE

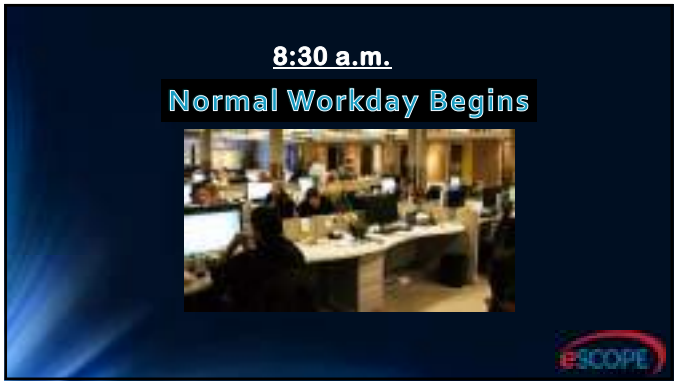
33


4:38 a.m.
Ransomware Installed
eSCOPE

34

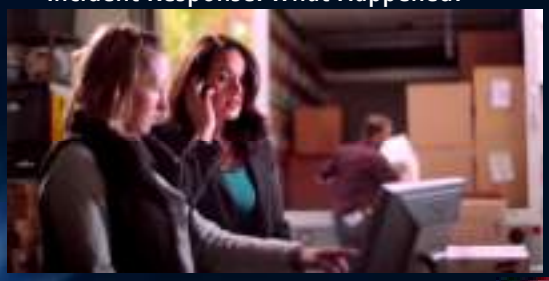

6:04 a.m.
Remote Connection Ends
eSCOPE

35


8:30 a.m.
Normal Workday Begins
eSCOPE

36

Incident Response: What Happened?



37

Incident 1: Facts

- Sensitive Records Accessed: 2,106
- Continued Unauthorized Access: 11 Days
- Breach Discovery: 4 months later (lucky observation)
- Live Network Activity Monitoring: None
- Reports Filed with Insurance, Police & FBI: Required
- Disclosure Notices Sent to Customers: Mandated

38

Live Response: Timely and Effective

39


Security Incident Steps

40


Post-Incident Analysis

41


Incident 2 (Protected): Facts
• Managed SIEM Network Activity Monitoring Installed
• Within 3 Business Days: Suspicious Activity Detected
• Network Traffic to International Network Blocked
• Reported to Credit Union IT Director: 11 Minutes
• Continued Unauthorized Access: 0 Days
• Breach Discovery: Immediate
• Reports Filed with Law Enforcement: None required
• Disclosure Notices Sent to Customers: None

42

eScope Security Suite: Peace of Mind

43

Could Use a Hand?

The Right Partnership Could Make Security Program Oversight A Breeze... Hands Down!

44

Security Fitness - Review

- Cyber Security Planning for Compliance and Security
- Emerging Technologies
- Security Information Event Management (SIEM)
- Endpoint Detection and Response (EDR)
- Cyber Incident Review of a Real-World Hack

45