Analyzing Your Vulnerability Assessment Reports

Dale Meredith

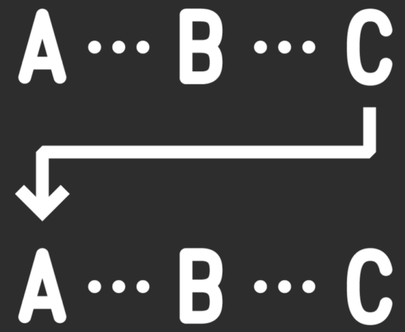
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith

Interpreting Reports

Scan

CVSS Score



Prioritize

Review

Identify

Investigate

Interpreting Reports

Reconcile the results

Identify unknown devices

Verify results

Correlate results

Compare best practices

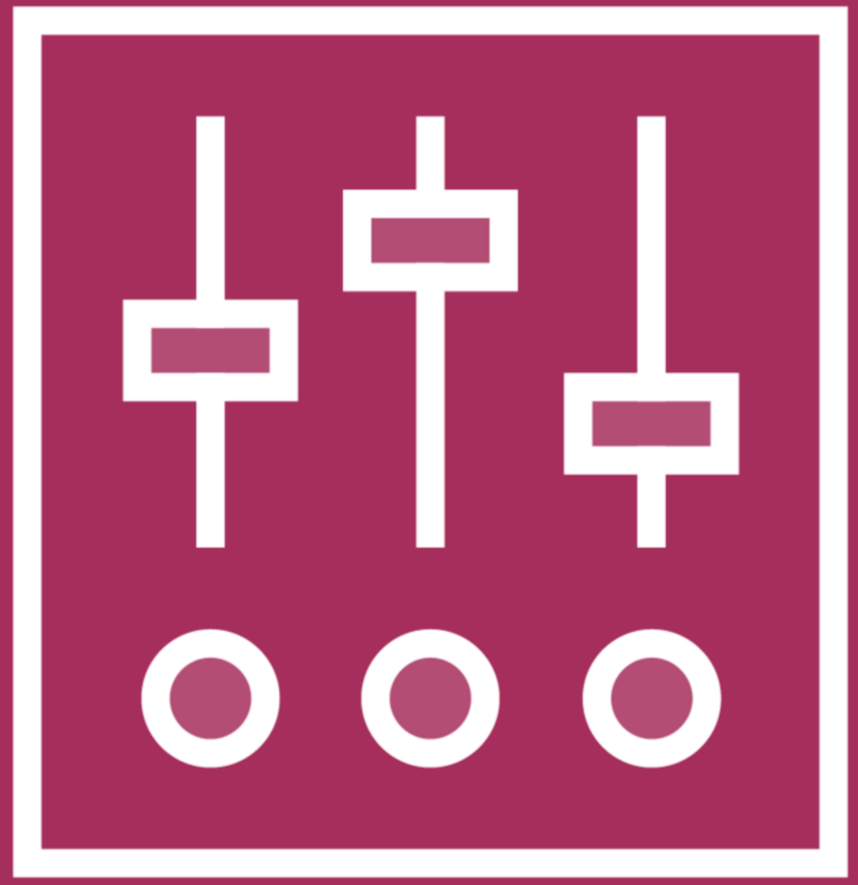
Interpreting Reports

Recognize inaccurate compliance scans

Identify solution for inaccuracies

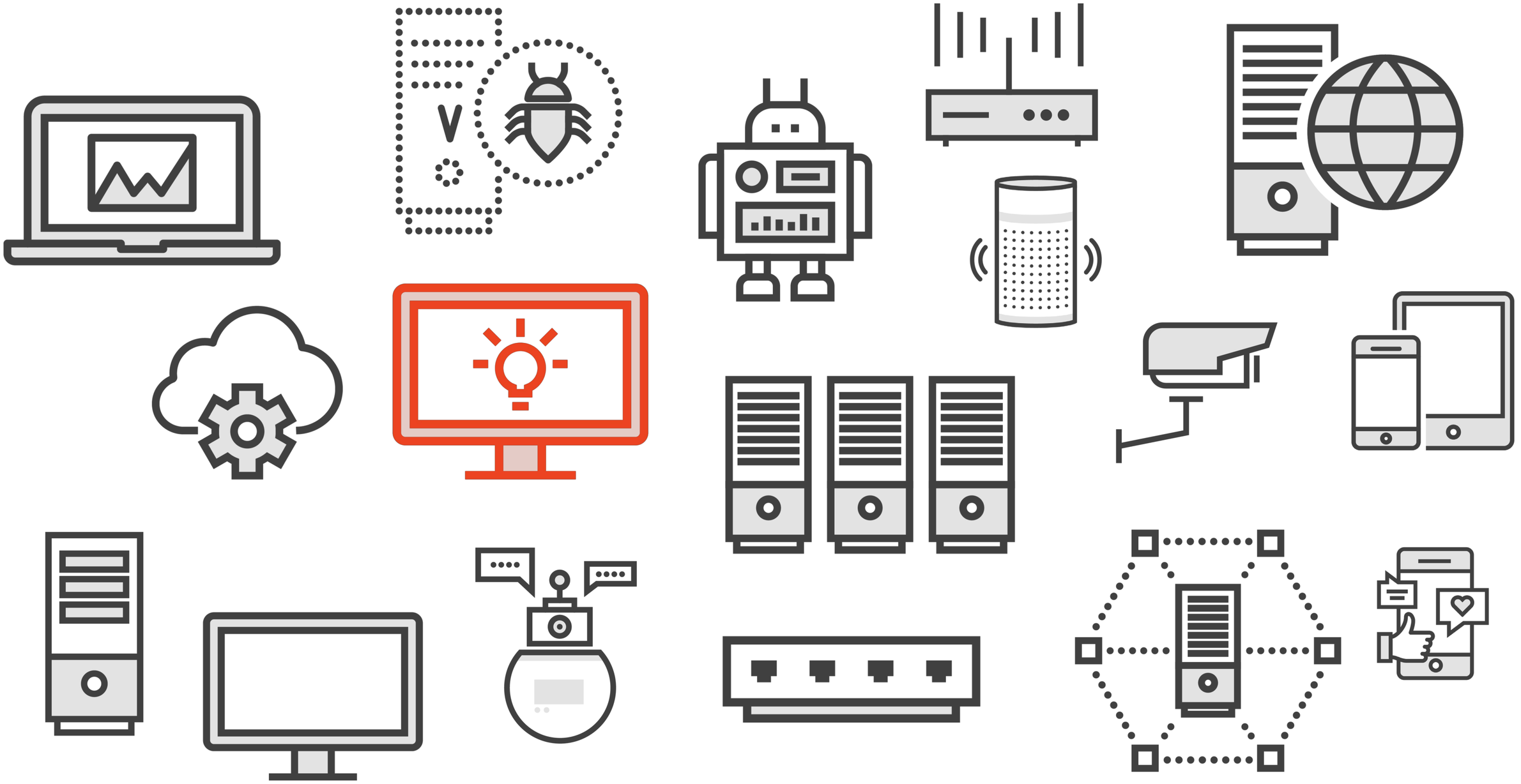
Implement needed solutions

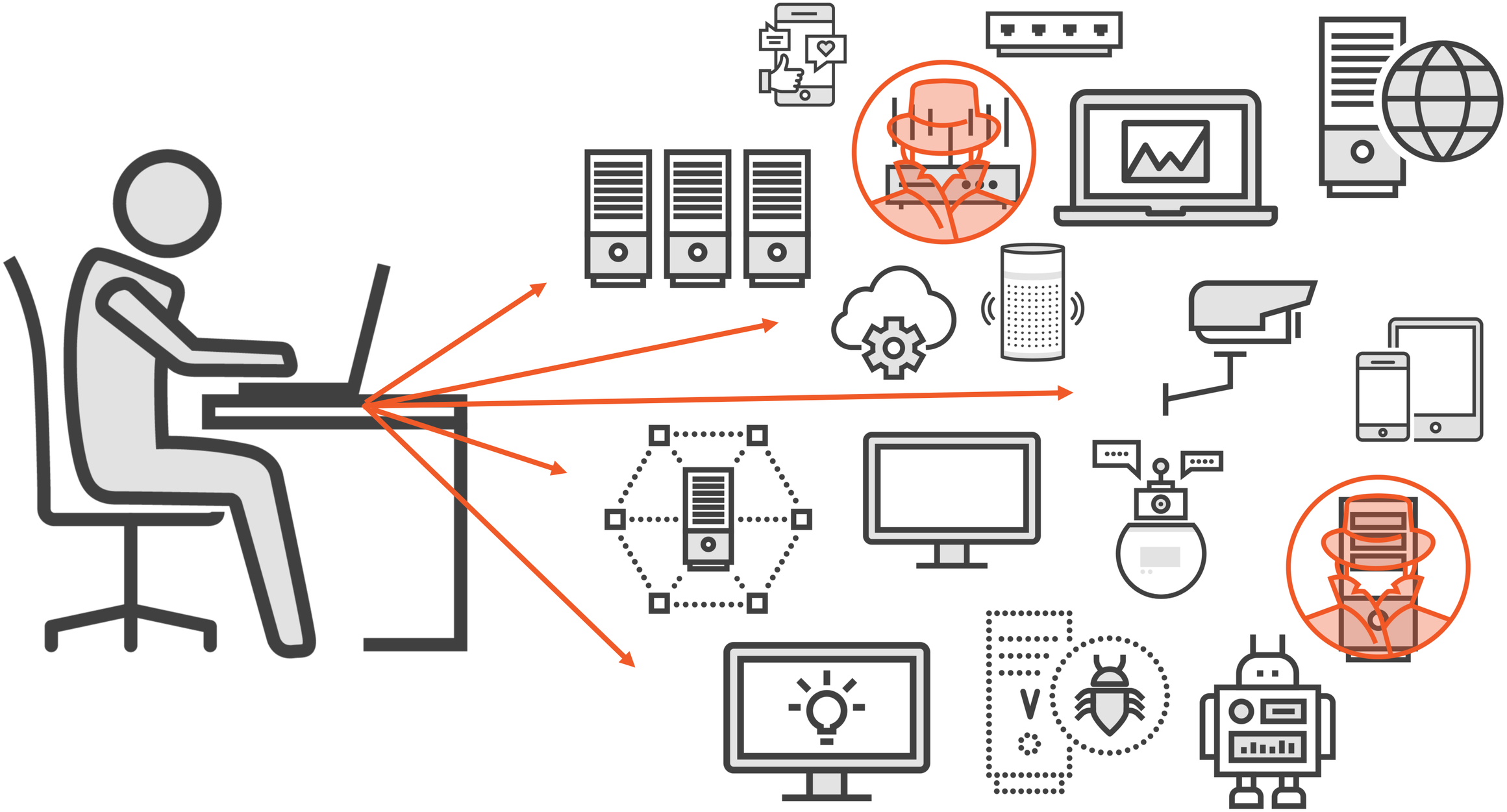
False Positives and Exceptions

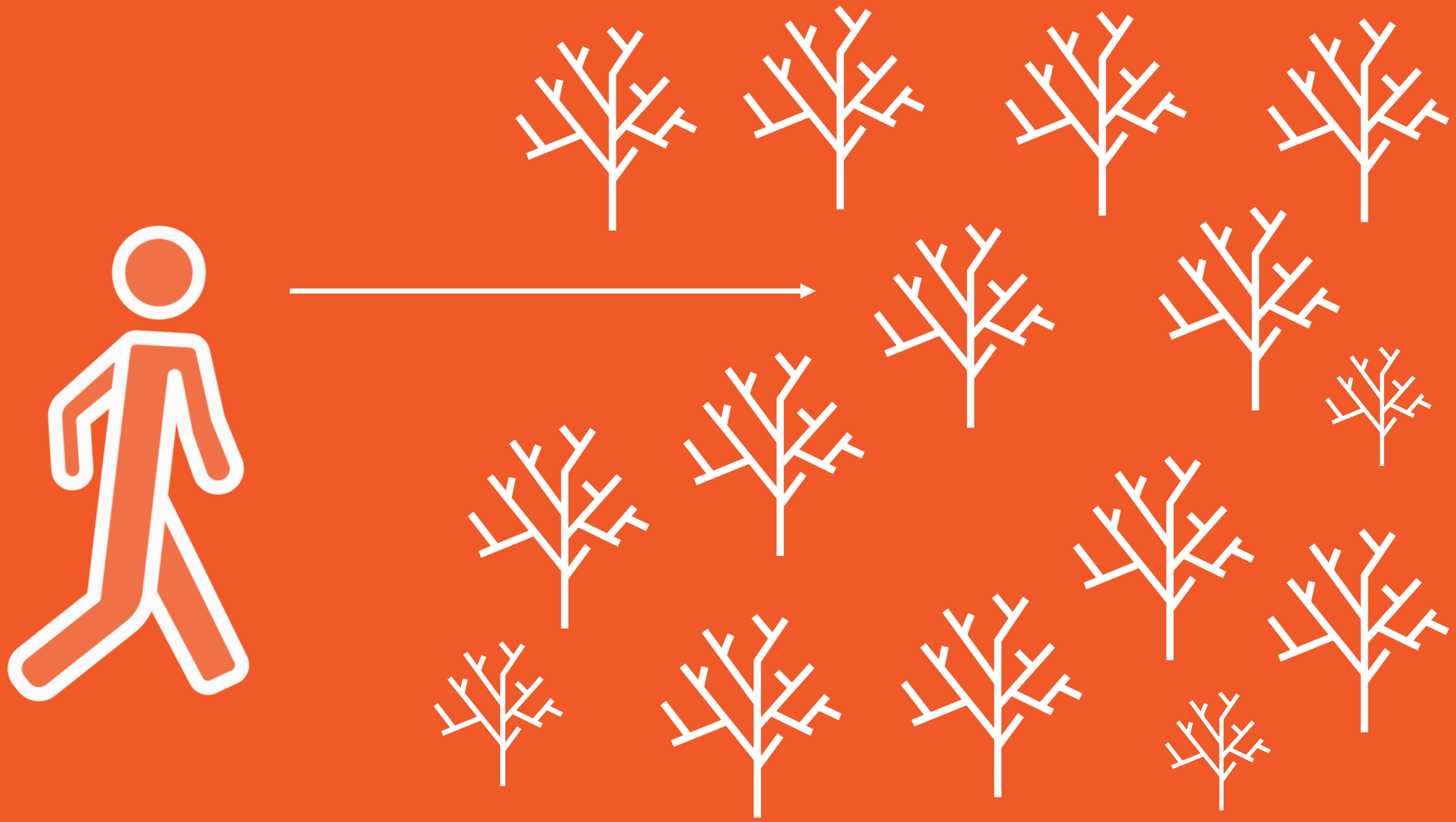


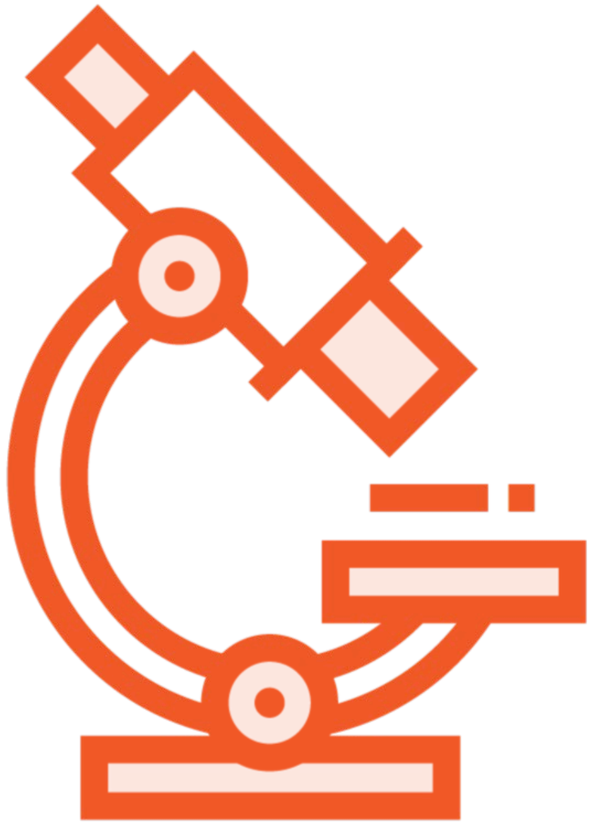
- Validate applications
- Establish new baselines if needed
- Recognize inappropriate scans
- Adjust the scan scope as needed
- Identify if vulnerabilities are exploited by administrative privileges
- Reduce incidences of false positives
- Monitor systems that can’t be remediated

Keeping up with the Trends









Prioritizing Importance

Monitor the number of incidences, detections and the response time

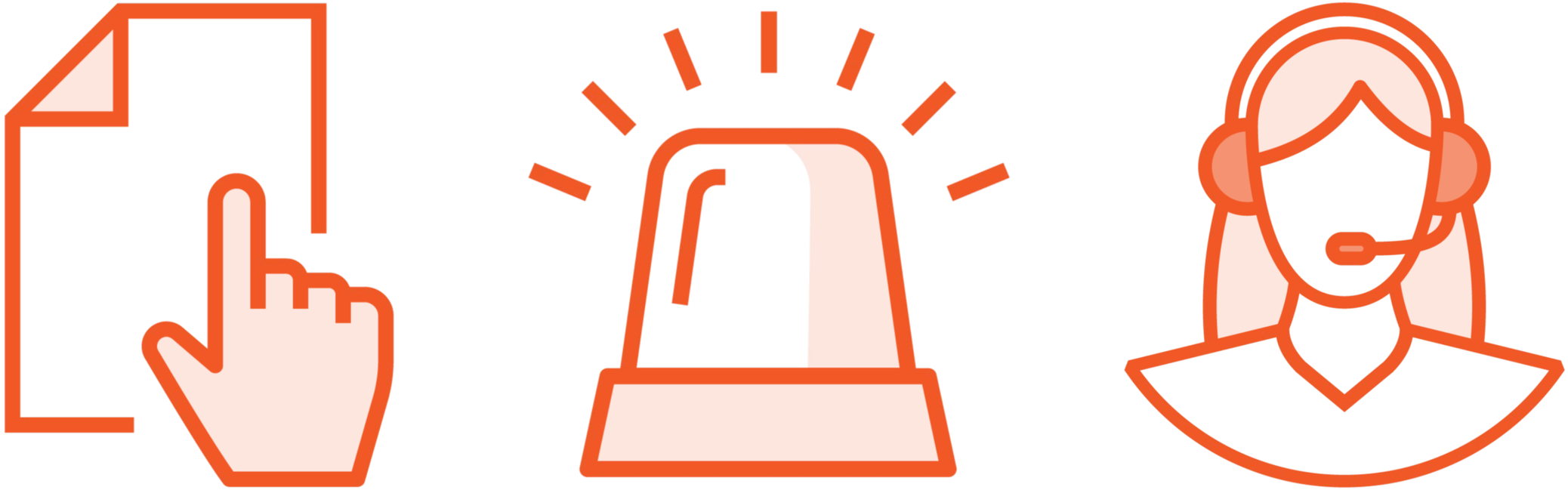
Explore financial impact

Recognize internal and external traffic volume and active ports

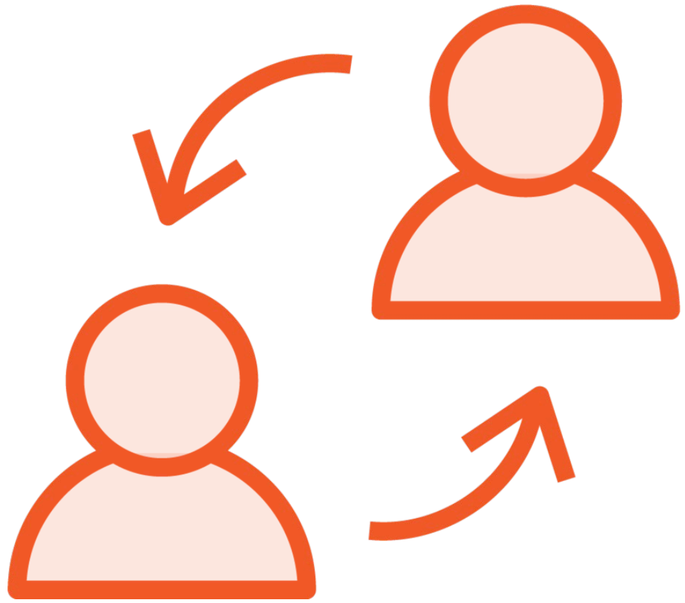
Observe the number of logins and failed logins

Examine unauthorized software and unauthorized devices

Training and Awareness



Compliance



External Awareness

Daily Education

SANS Institue

FireEye

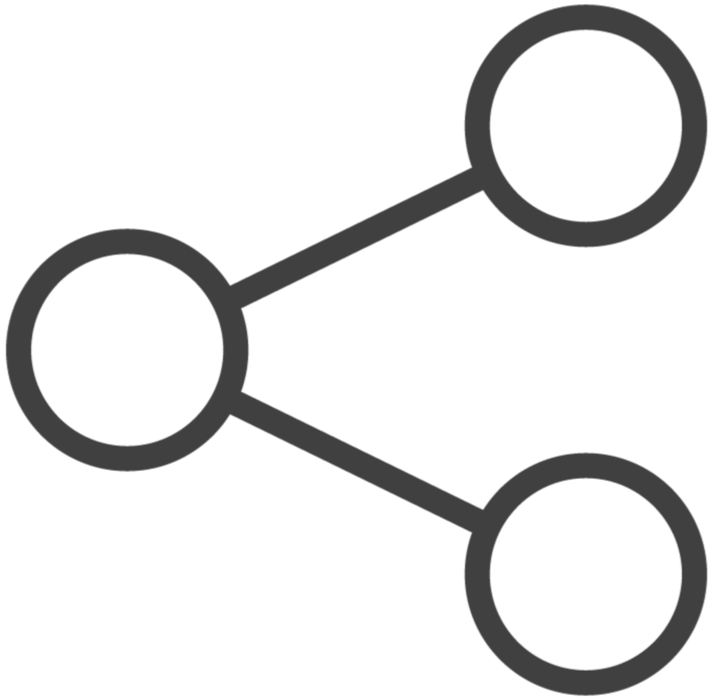
Dark Reading

Zero-day exploits

Defender Security Intelligence

AlienVault

Connect and Share



Dale Meredith

www.daledumbsitdown.com

Learning Check

Learning Check

- CVSS
- Compliance
- Add to exceptions
- User training