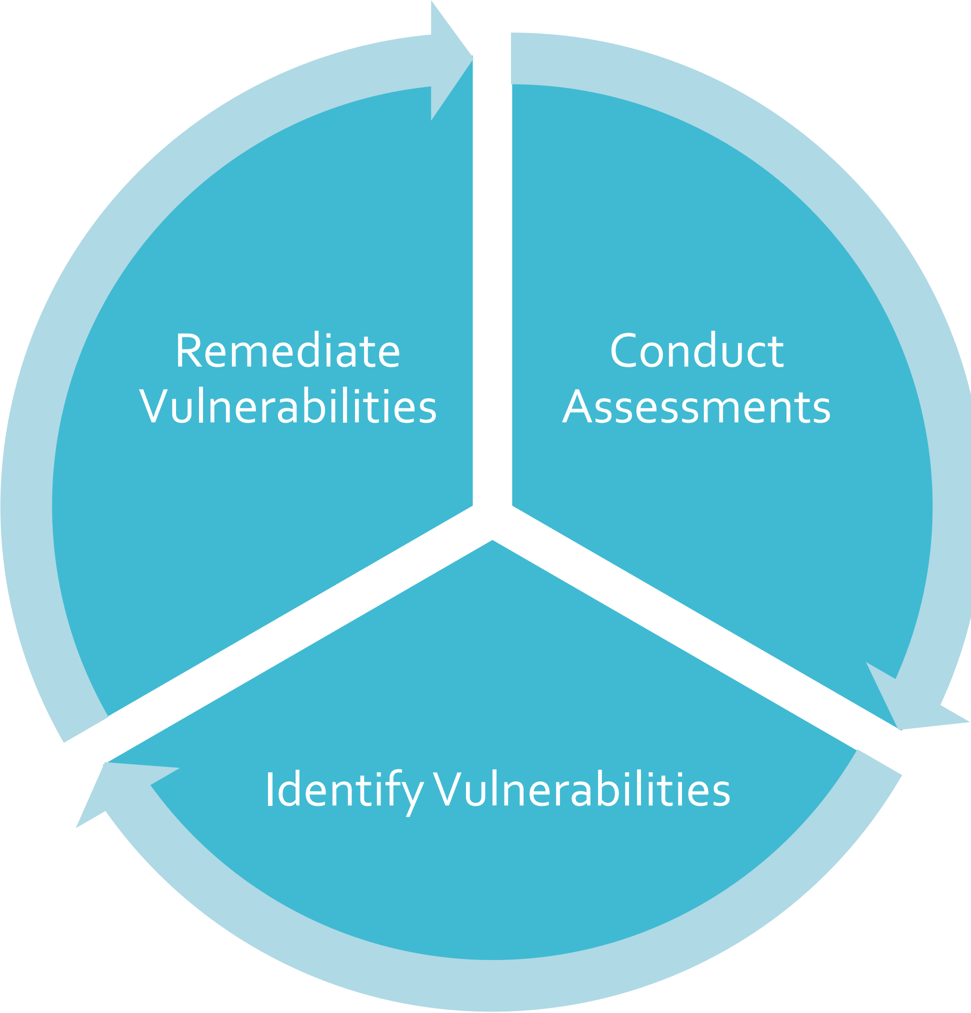
Process of VA & DF

Presented by Isuru Tharanga Malawige

Vulnerability Management Process

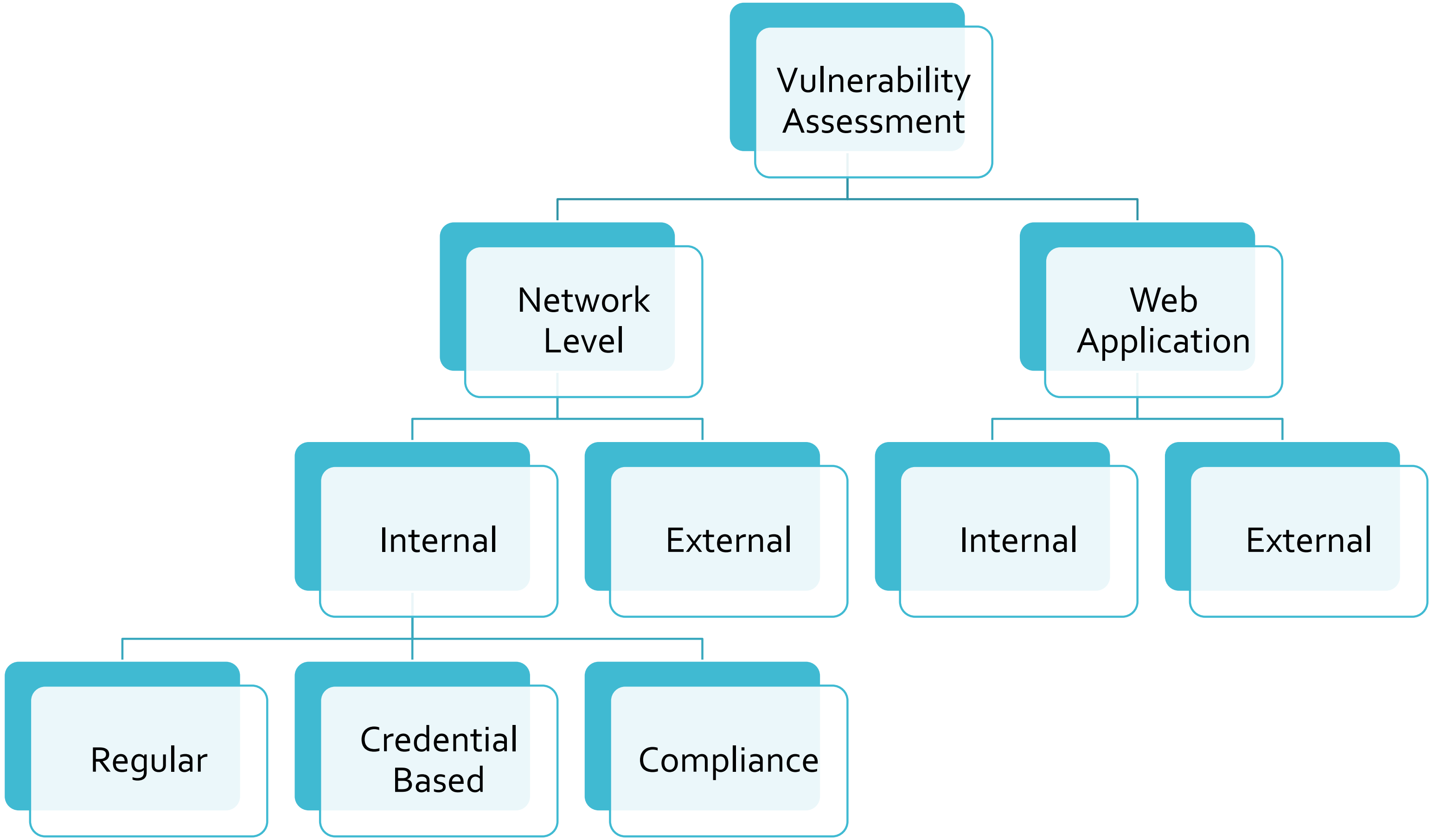


Remediate Vulnerabilities

Conduct Assessments

Identify Vulnerabilities

Vulnerability Assessment Types



Assessment Plan

Bi-annual

2X

Quarterly

4X

Monthly

12X

Credential Based Vulnerability Assessments

Regular VA

- Reconnaissance done via network
- Vulnerabilities identify depend on the port enumeration
- Might be **False Positive**

Credential Based VA

- Reconnaissance done on the Host (No disruption on the network)
- Identify list of missing patched
- Identify client-side installed software vulnerabilities (AV Software included)
- Tests for default credentials on the system/services
- More **Accurate**

Compliance Assessments

- Filesystem Configuration
- Password Policy
- User Account Policy
- Access Control
- Audit Policy
- Logging
- Network Configuration
- Firewall Configuration

Security Configuration checks may vary based on the services running on the system

Operating Systems

- Windows
- Linux
- Unix

Server Software

- Microsoft IIS
- Vmware
- Apache
- IBM DB2
- BIND
- Docker
- MySQL

Network Devices

- Palo Alto
- Cisco

Desktop Software

- Microsoft Office
- Google Chrome
- Mozilla Firefox
- Microsoft Exchange

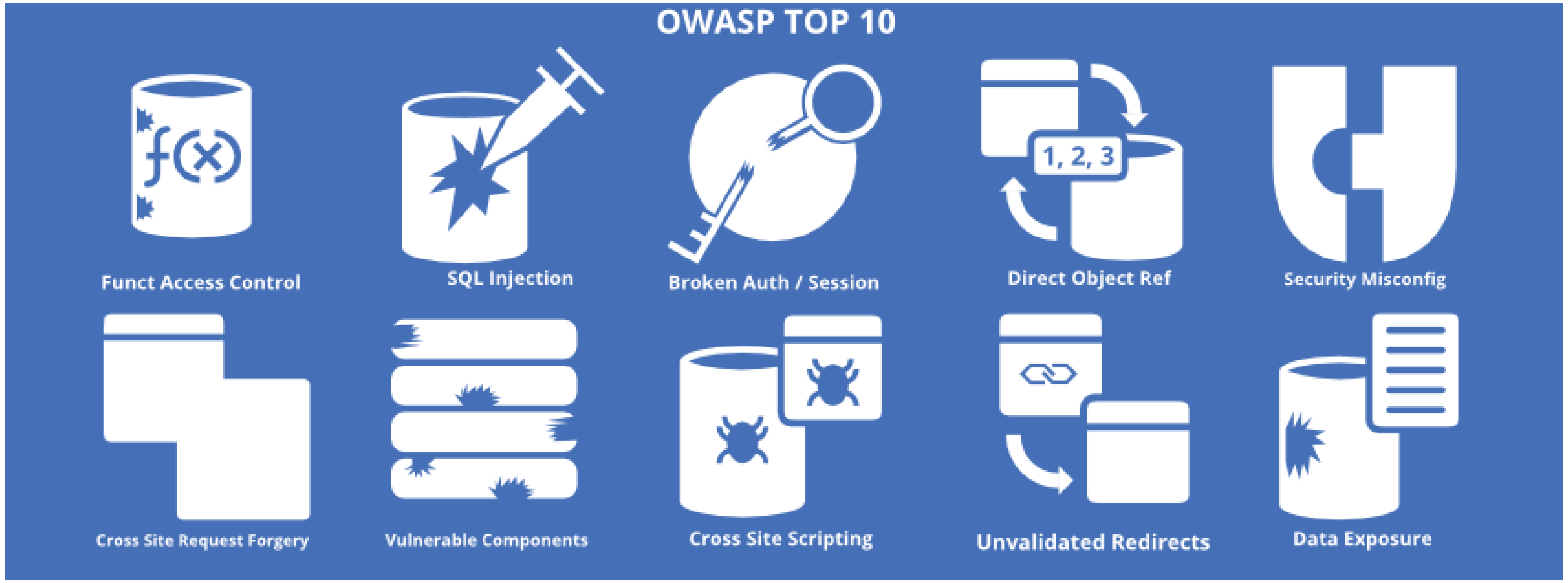
Mobile Devices

- Apple IOS
- Google Android

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

CIS. Center for Internet Security®

Web Application Security Assessments



- SQLi (Blind/Boolean)
- XSS (Blind/DOM Based)
- CSRF
- Command Injection (Blind)
- File Intrusion (Local/Remote)
- HTTP/Email Header Injection
- RCE (Remote Code Evaluation)

OWASP
Open Web Application
Security Project

Tools

Vulnerability

- **Nessus**
- **Qualys**
- **Nexpose**
- OpenVAS
- Nikto

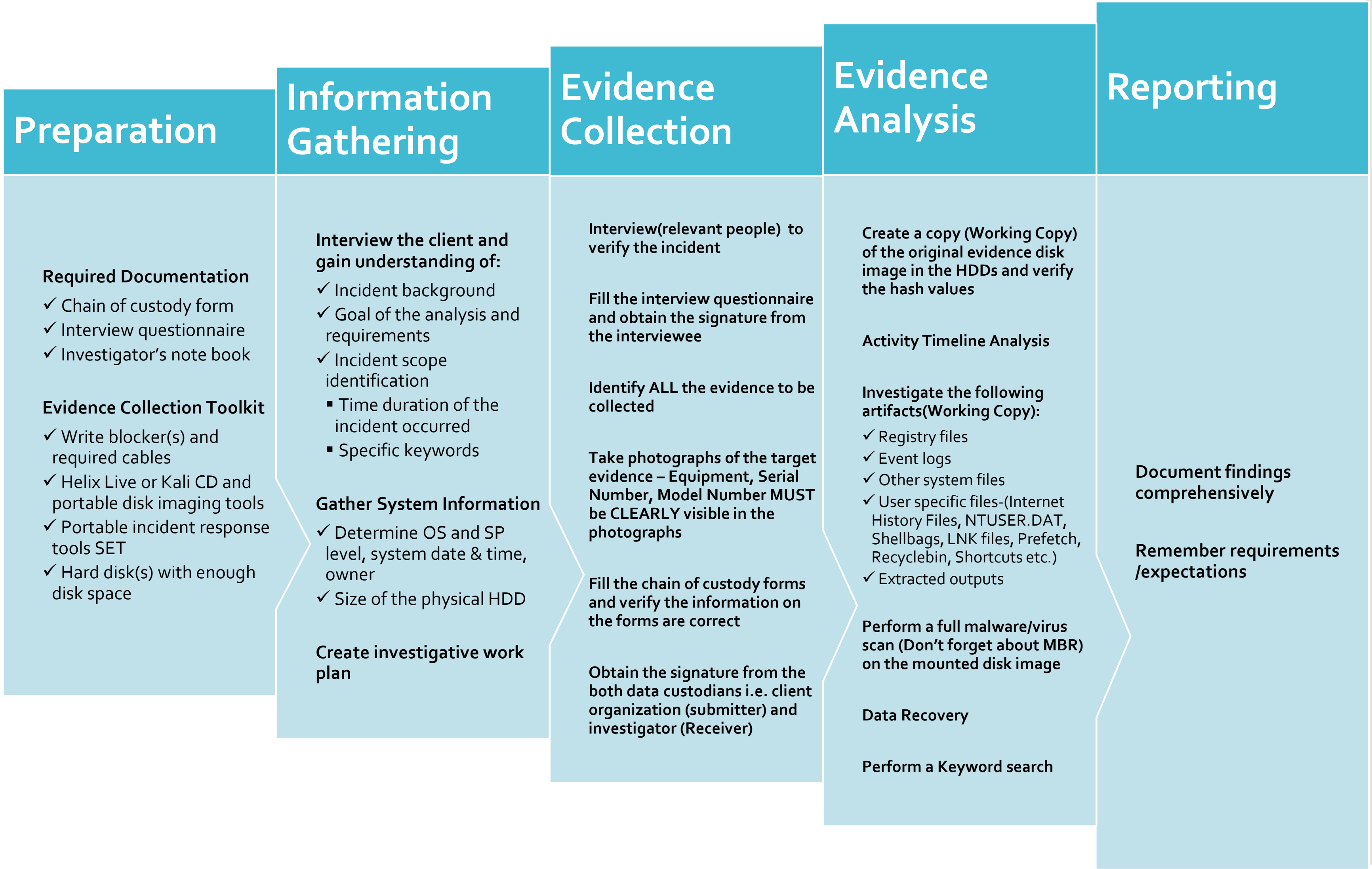
Web Application

- **Acunetix**
- **Netspaker**
- **Nessus**
- **Qualys**
- **Nexpose**
- **Detectify**
- Burpsuit
- Arachni
- Wapiti

Compliance

- **Nessus**
- **Qualys**
- **Nexpose**
- SCAP Workbench
- Lynis

Digital Forensic Investigation Process



Preparation

Required Documentation

- ✓ Chain of custody form
- ✓ Interview questionnaire
- ✓ Investigator’s note book

Evidence Collection Toolkit

- ✓ Write blocker(s) and required cables
- ✓ Helix Live or Kali CD and portable disk imaging tools
- ✓ Portable incident response tools SET
- ✓ Hard disk(s) with enough disk space

Information Gathering

Interview the client and gain understanding of:

- ✓ Incident background
- ✓ Goal of the analysis and requirements
- ✓ Incident scope identification
  - ▪ Time duration of the incident occurred
  - ▪ Specific keywords

Gather System Information

- ✓ Determine OS and SP level, system date & time, owner
- ✓ Size of the physical HDD

Create investigative work plan

Evidence Collection

Interview(relevant people) to verify the incident

Fill the interview questionnaire and obtain the signature from the interviewee

Identify ALL the evidence to be collected

Take photographs of the target evidence – Equipment, Serial Number, Model Number MUST be CLEARLY visible in the photographs

Fill the chain of custody forms and verify the information on the forms are correct

Obtain the signature from the both data custodians i.e. client organization (submitter) and investigator (Receiver)

Evidence Analysis

Create a copy (Working Copy) of the original evidence disk image in the HDDs and verify the hash values

Activity Timeline Analysis

Investigate the following artifacts(Working Copy):

- ✓ Registry files
- ✓ Event logs
- ✓ Other system files
- ✓ User specific files-(Internet History Files, NTUSER.DAT, Shellbags, LNK files, Prefetch, Recyclebin, Shortcuts etc.)
- ✓ Extracted outputs

Perform a full malware/virus scan (Don’t forget about MBR) on the mounted disk image

Data Recovery

Perform a Keyword search

Reporting

Document findings comprehensively

Remember requirements /expectations

Tools

- Integrated Acquisition -Smartphone, Computer
- View File System
- Registry Viewer
- Keyword Artifact Searching
- Connections for relationship linking
- Mobile Artifacts
- Internet and Email Artifacts
- Recover Deleted Files and Folders
- SQLite Databases Viewer

ACCESSDATA

EnCase Endpoint Investigator

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

MAGNET FORENSICS

Q & A

Thank You