Information Security Controls

Dale Meredith

@dalemeredith | www.dalemeredith.com

I don’t even call it violence when it’s self-defense, I call it intelligence.

— Malcolm X

Information Security Controls

- Necessity of Ethical Hacking
- What Skills You Must Have
- Multi-layered Defense
- Incident Management
- Security Policies
- Vulnerability Research
- Penetration Testing

Necessity of Ethical Hacking

Rapid Growth in Tech = Trouble

What Ethical Hackers do for companies

- ❑ Review systems and infrastructure
- ❑ Test current security
- ❑ Create solution
- ❑ Retest

You HAVE to answer questions like:

- ❑ What can be seen?
- ❑ What is being monitored?
- ❑ What can be done?
- ❑ Is there adequate protection?
- ❑ Are compliances met?

What Skills You Must Have

“I’ve Got Hacking Skills”

O/S Knowledge

Computer professional

Network guru

Security awareness

“I’ve Got Hacking Skills”

Software knowledge

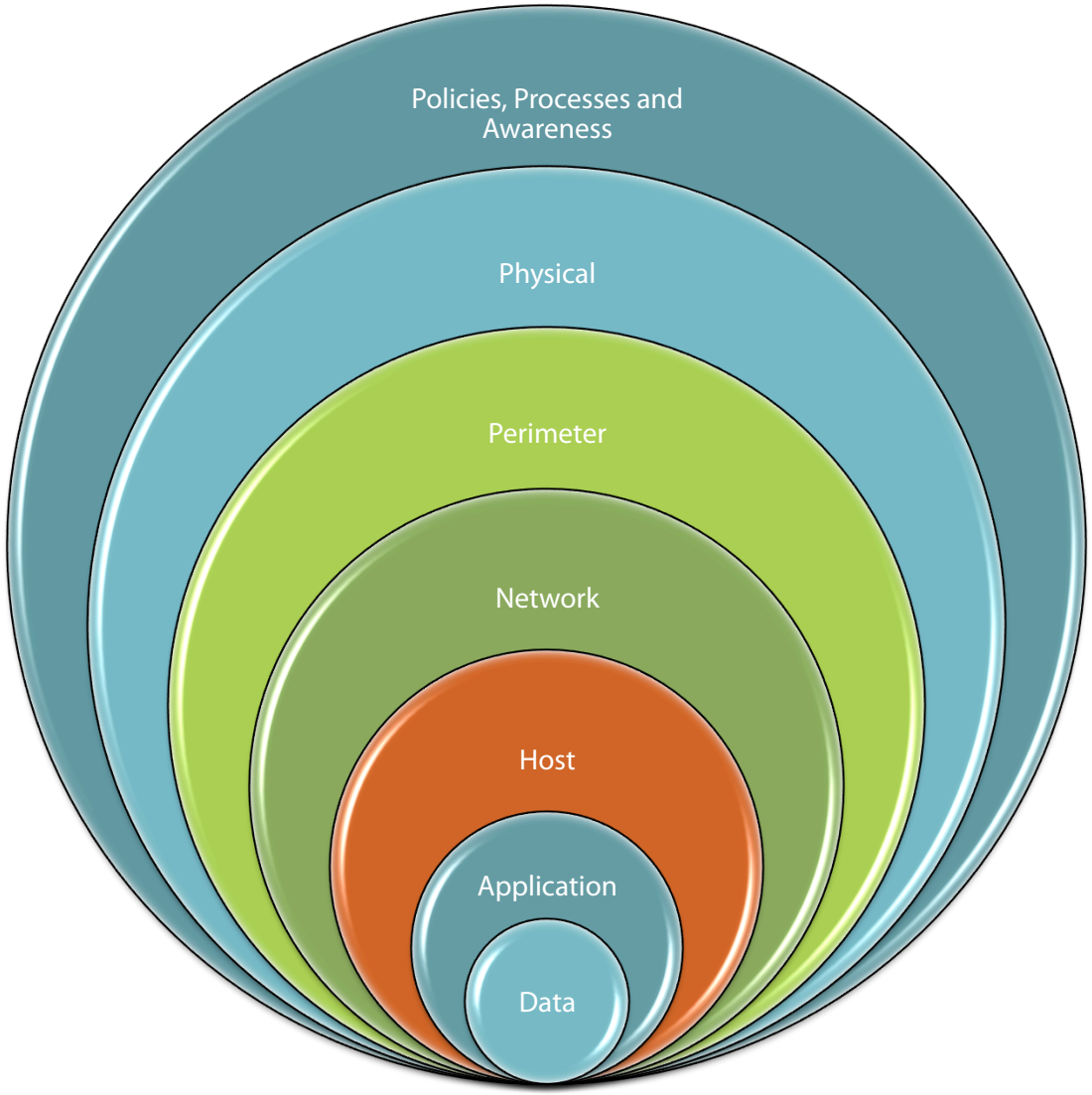
Management skills

Patience

A lot of “Sherlock Holmes”

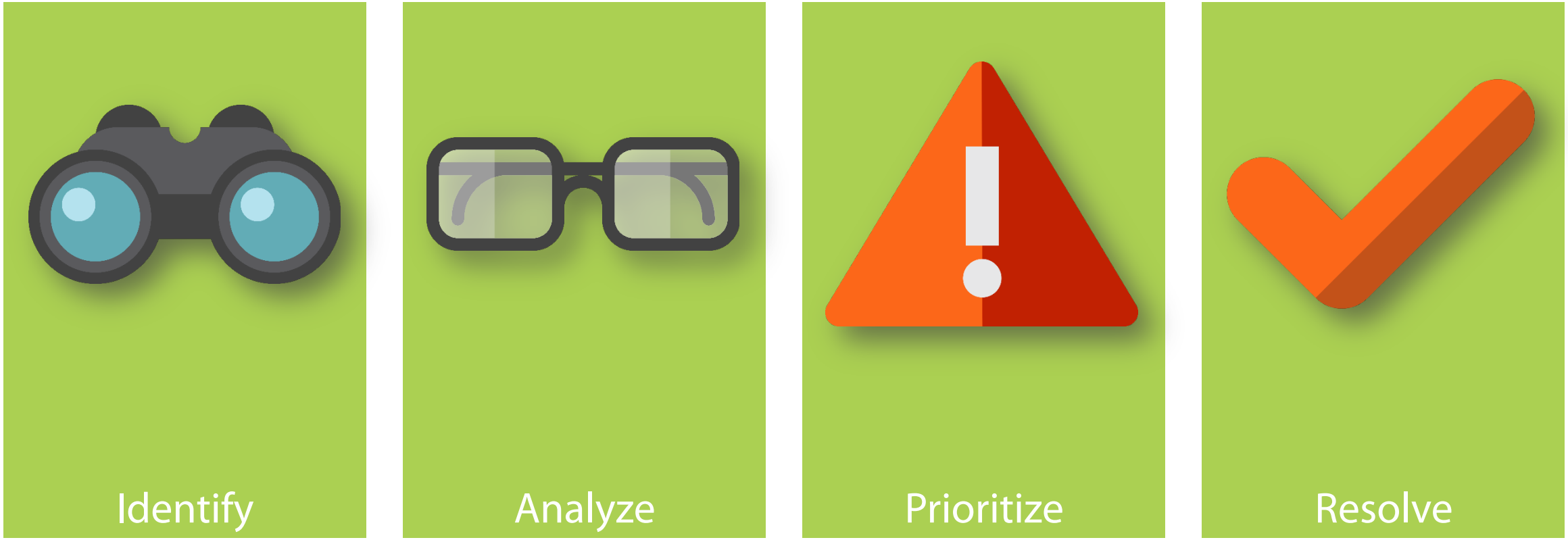
Multi-layered Defense

“You’ve Leveled Up”



Incident Management

Think Outside the Box



The "Why" of Incident Management

Better service quality

Pro-active

Reduces impact

Meets availability

More efficient & productive

Customer/user satisfaction

IM Process

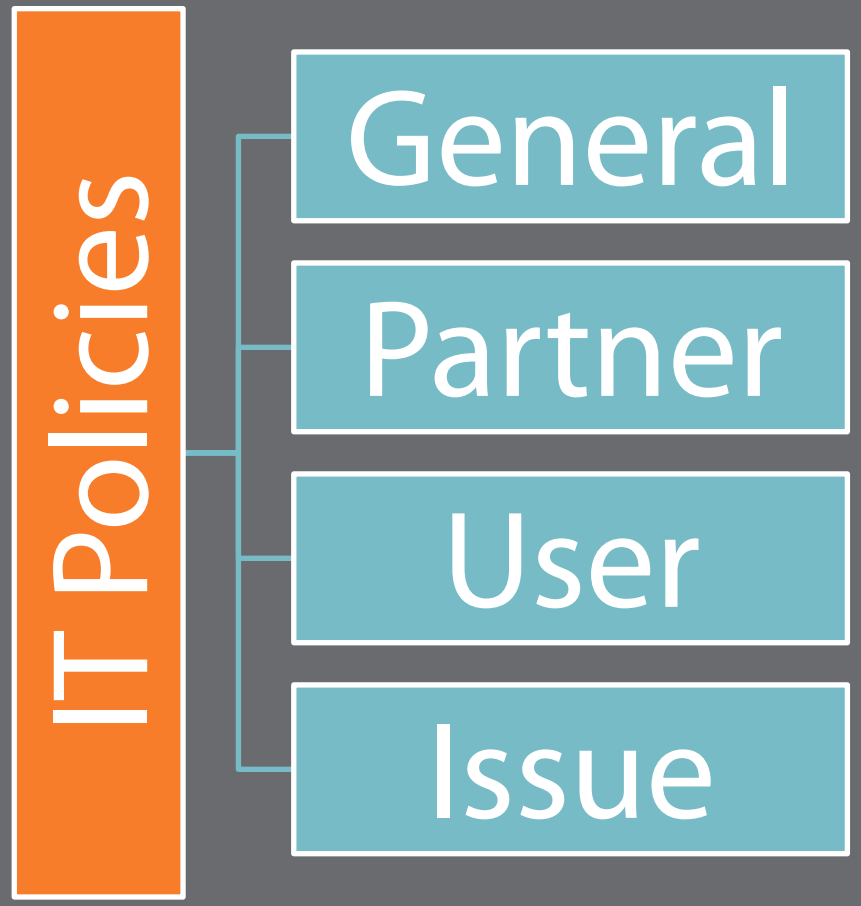
1. Prepare for Event Handling and Reaction
2. Detection & Examination
3. Sorting & Ranking
4. Notification
5. Containment
6. Forensic Examination
7. Purge & Recovery
8. Post-incident Actions

Security Policies

Security Policies

1. Create an outline
2. Protect resources
3. Legal liability
4. Computing resources
5. Unapproved modification of data
6. Loss of private & sensitive data
7. Separate user's access rights
8. Shield from thief, misuse, illegal disclosure

Taxonomy of Security Policies



Security Polices Examples

Acceptable-use

Passwords

User account

Email security

Remote-access

Firewall

Information protection

Network connection

Special access

Vulnerability Research

Knowledge IS Power!

- How often are you checking?
- Where do you check?
- Start thinking like a Hacker
- Collect information about trends in security, attacks, and threats
- Find out how to recover

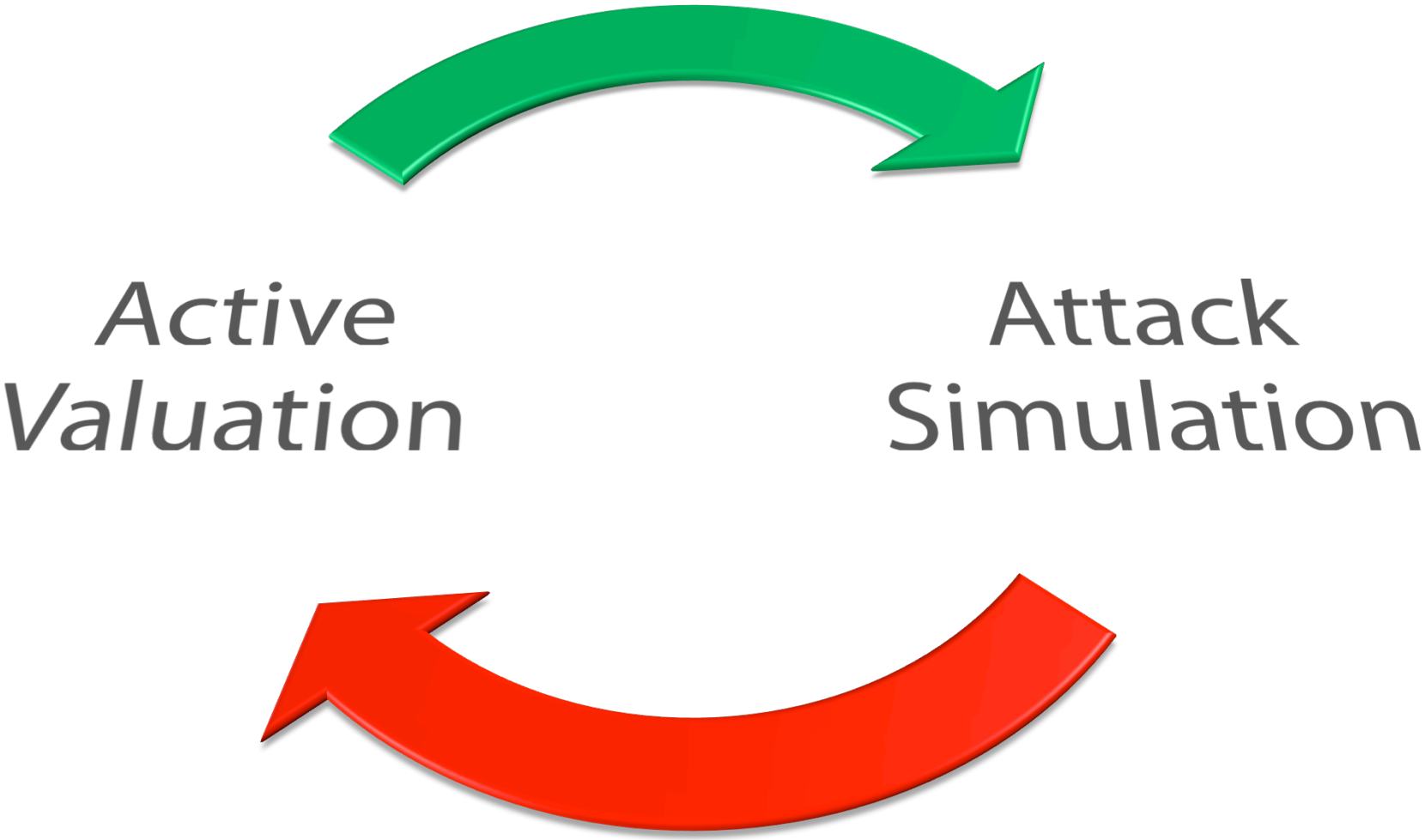
Places to Look

- O/S Vendors
- Application vendors
- Hardware vendors
- Manufacture vendors
- Component vendors
- Security related sites/blogs

- www.hackerstorm.co.uk
- www.eccouncil.org
- www.securitymagazine.com
- www.securityfocus.com
- blogs.windowssecurity.com
- www.hackersjournals.com
- www.zdnet.com/topic/security

Penetration Testing

Pen-testing - “Not a Job at Bic”



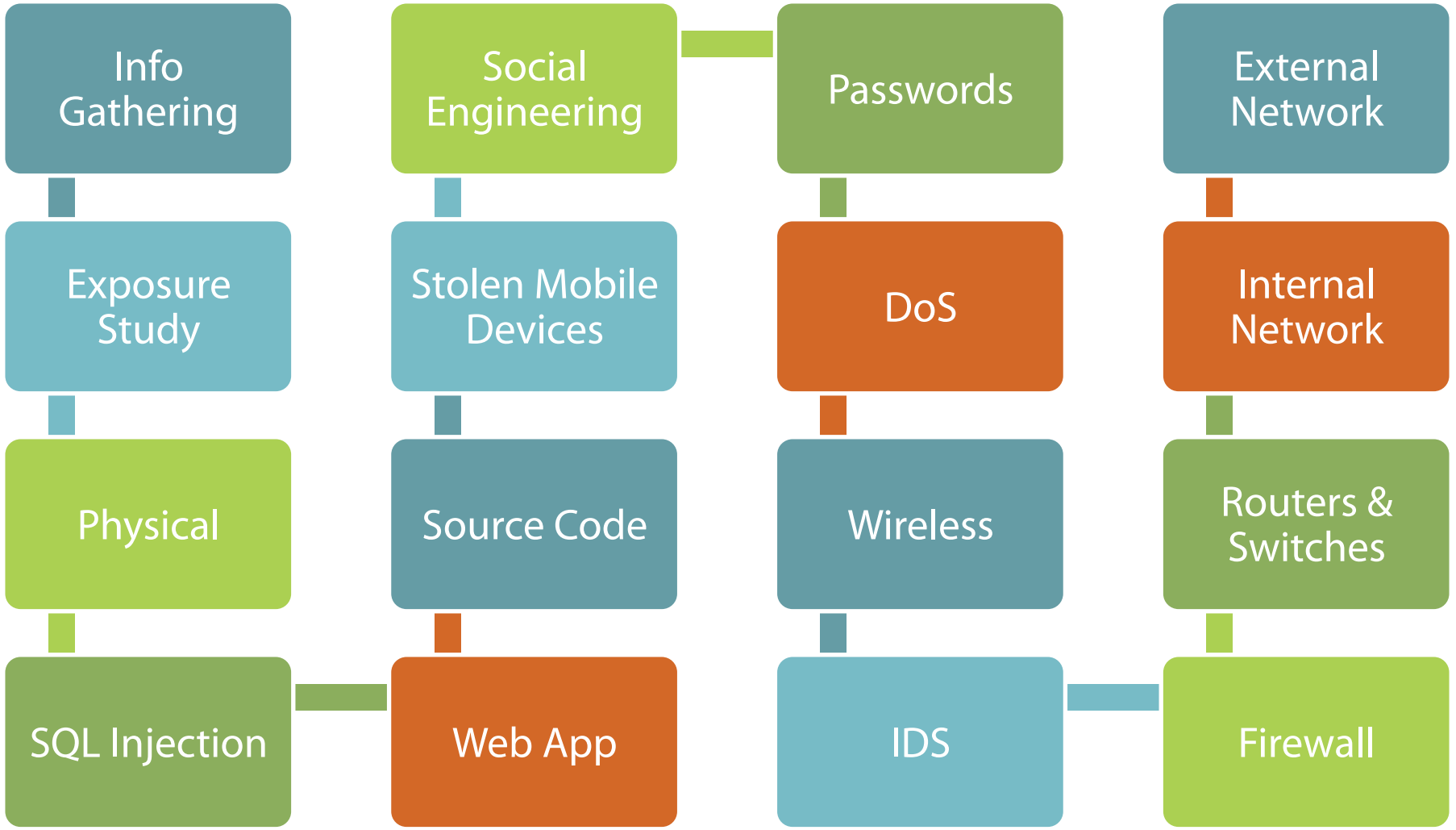
Why?

ID threats
Reduce ROSI
Gauge efficiency

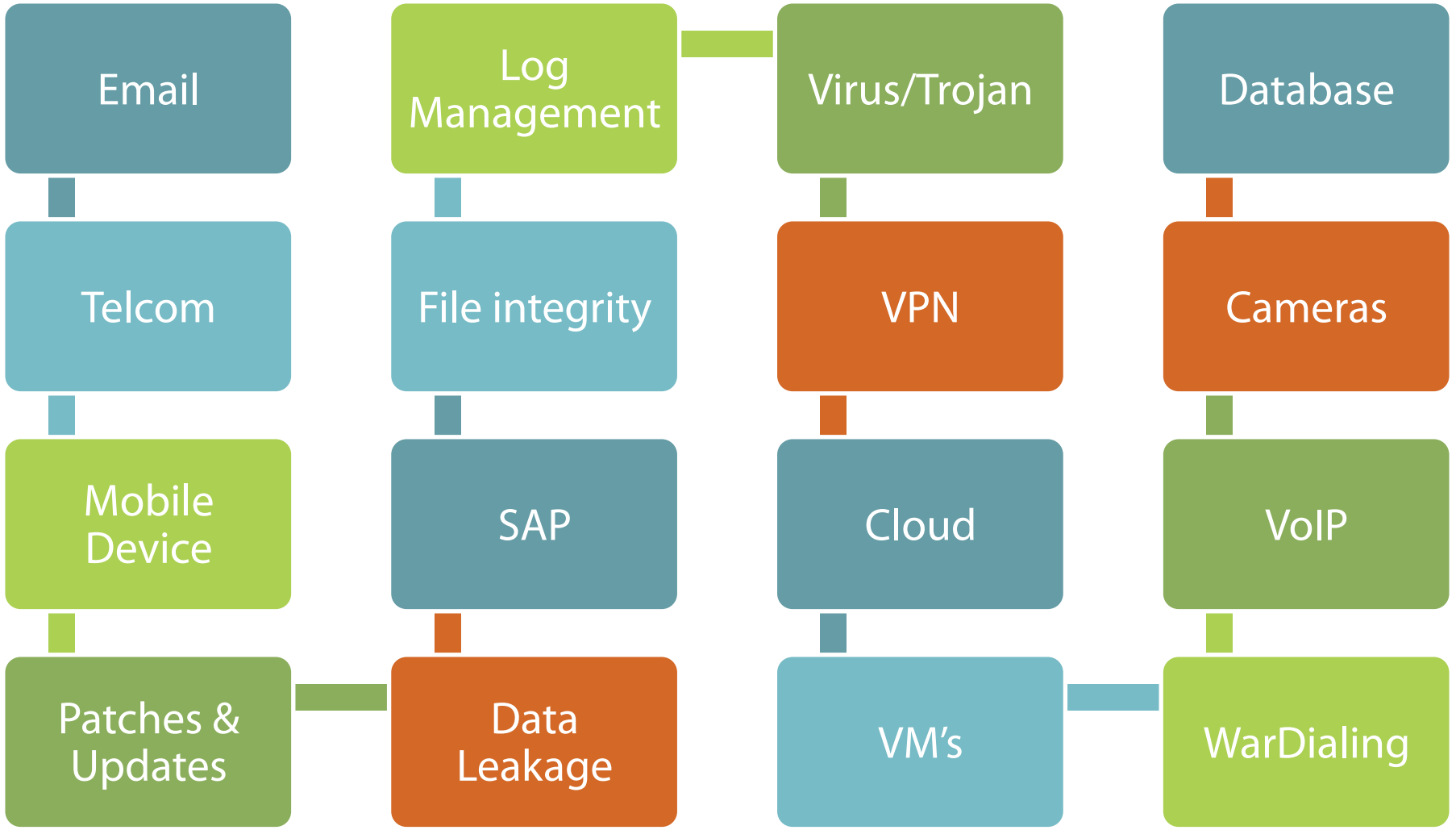
Upgrades
Test controls
Maintain standards

Reassurance
Best practices
In-house development

Method



Method



Summary

- Necessity of Ethical Hacking
- What Skills You Must Have
- Multi-layered Defense
- Incident Management
- Security Policies
- Vulnerability Research
- Penetration Testing