Information Security Controls

Dale Meredith

@dalemeredith | www.daledumbsitdown.com

pluralsight

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

— Malcolm X

pluralsight

Information Security Controls

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

pluralsight

Information Security Controls

- Vulnerability Research
- Data Leakage
- The Role of AI/ML
- Penetration Testing

pluralsight

Necessity of Ethical Hacking

pluralsight

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?

pluralsight

What Skills You Must Have

pluralsight

“I’ve Got Hacking Skills”

O/S Knowledge

Computer professional

Network guru

Security awareness

pluralsight

“I’ve Got Hacking Skills”

Software knowledge

Management skills

Patience

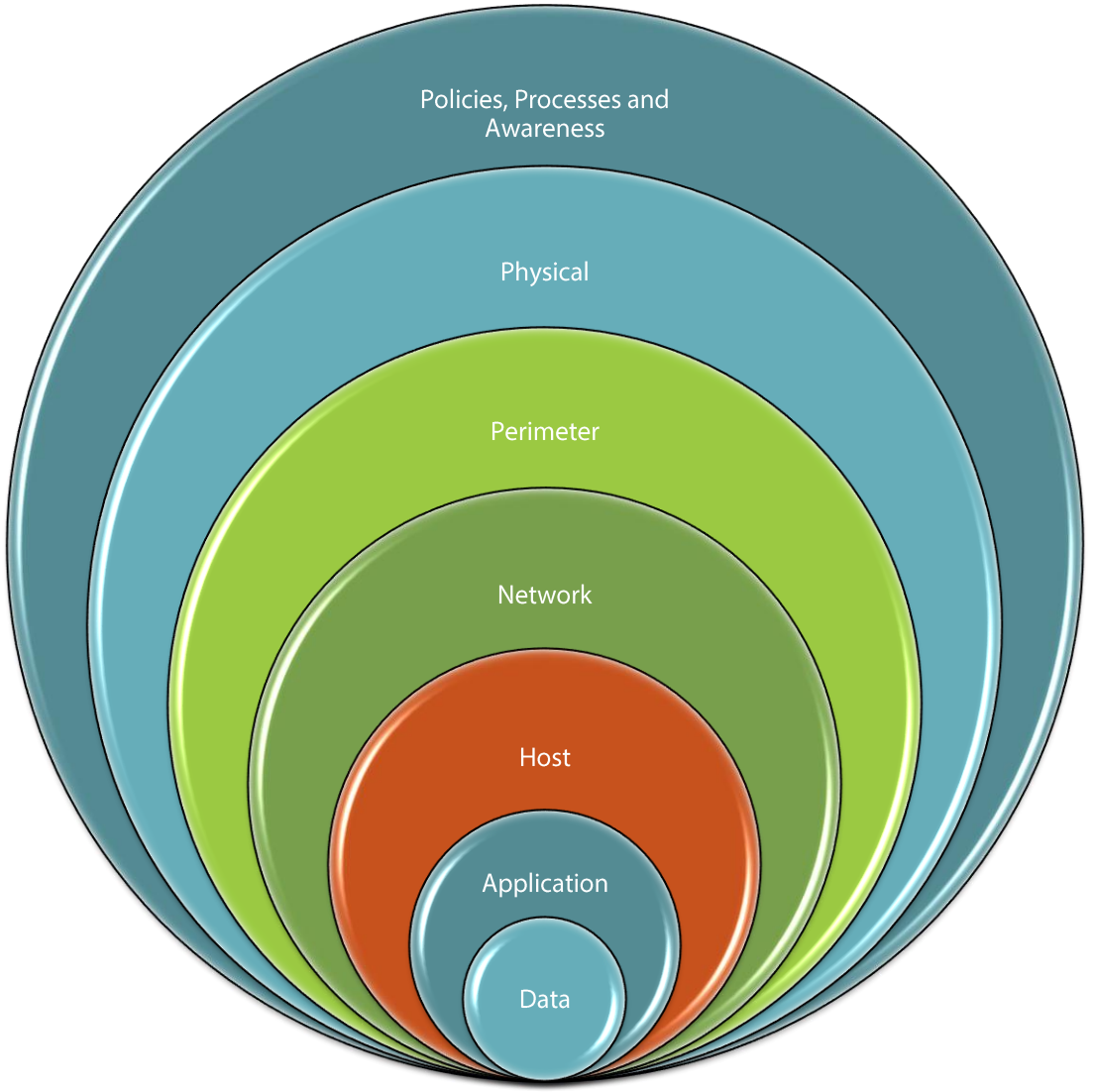
A lot of “Sherlock Holmes”

pluralsight

Multi-layered Defense

pluralsight

“You’ve Leveled Up”

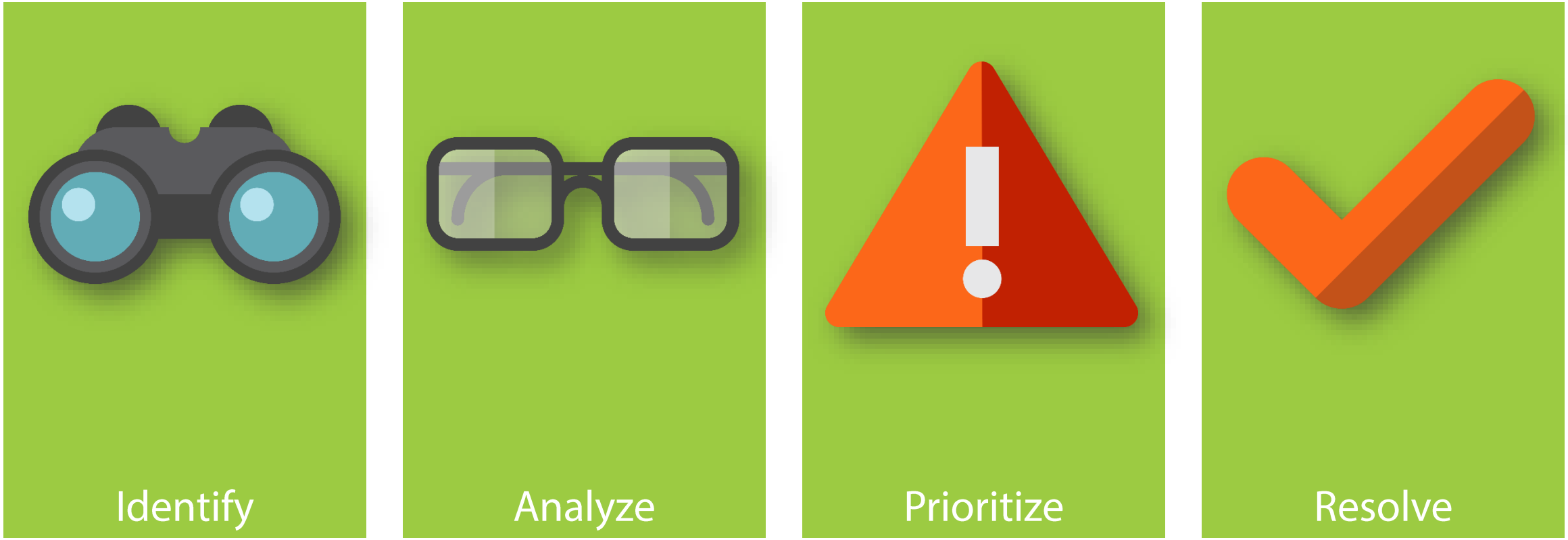


pluralsight

Incident Management

pluralsight

Think Outside the Box



pluralsight

The "Why" of Incident Management

Better service quality

Pro-active

Reduces impact

Meets availability

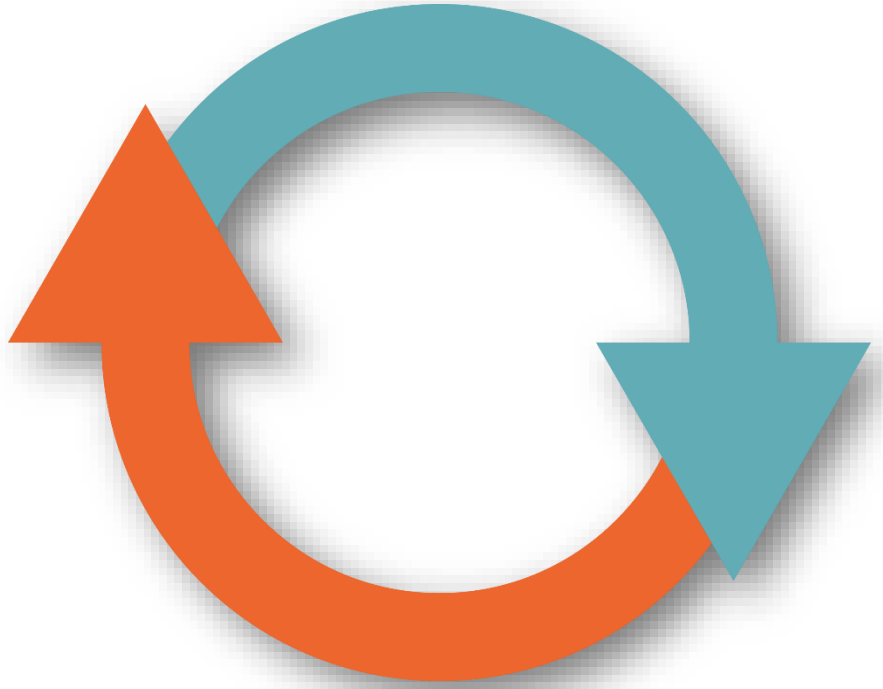
More efficient & productive

Customer/user satisfaction

pluralsight

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



pluralsight

Data Leakage

pluralsight

What The…?

- Major risks to your organization!
- Insider and external threats

pluralsight

It's A Bird, It's A Plane, It's DLP!

- Looks at the data
- Looks at the rules
- Determines what can be done

pluralsight

“Back It Up, Back It Up, My Daddy Taught Me Good”

- ID the data
- Select the technology
- Choosing a RAID

pluralsight

“Back It Up, Back It Up, My Daddy Taught Me Good”

Choose a method

- ❑ Hot
- ❑ Cold
- ❑ Warm

Location:

- ❑ Onsite
- ❑ Offsite
- ❑ Cloud

- ❑ Choose the type
- ❑ Full
- ❑ Incremental
- ❑ Differential

pluralsight

Don’t EVER assume it works!
Validate your process.

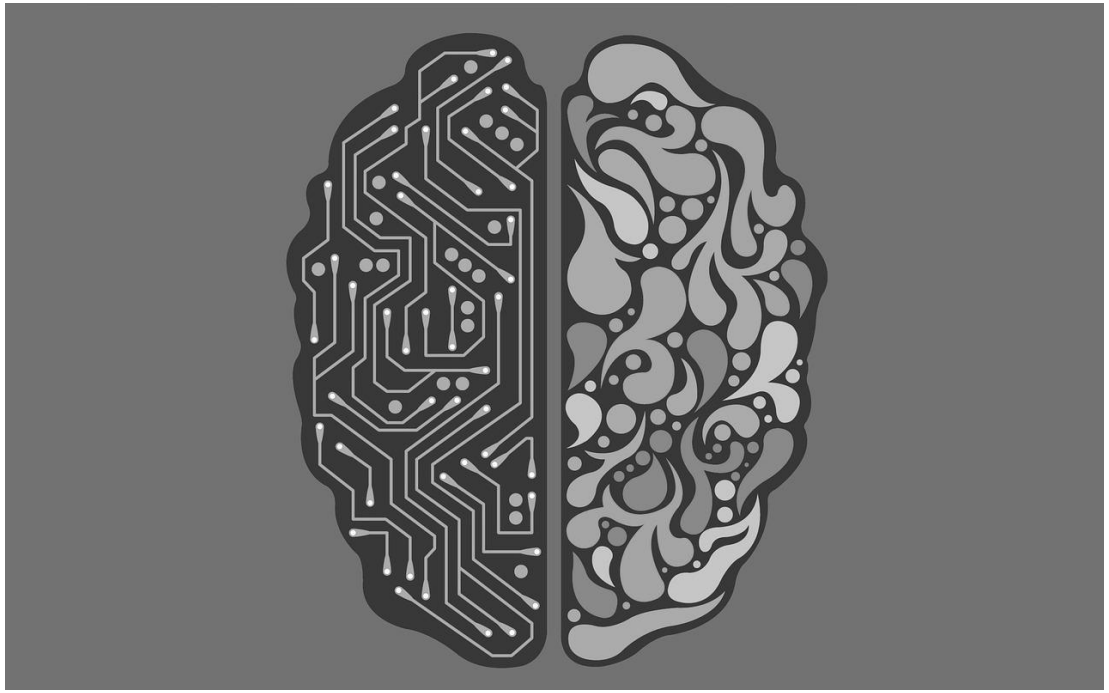
-SuperDale

pluralsight

The Role of AI/ML

pluralsight

I'm Sorry Dale, I'm Afraid I Can't Do That"



- Not just for cars
- Beware
- Machine Learning
- We're #4!

pluralsight

Security Policies

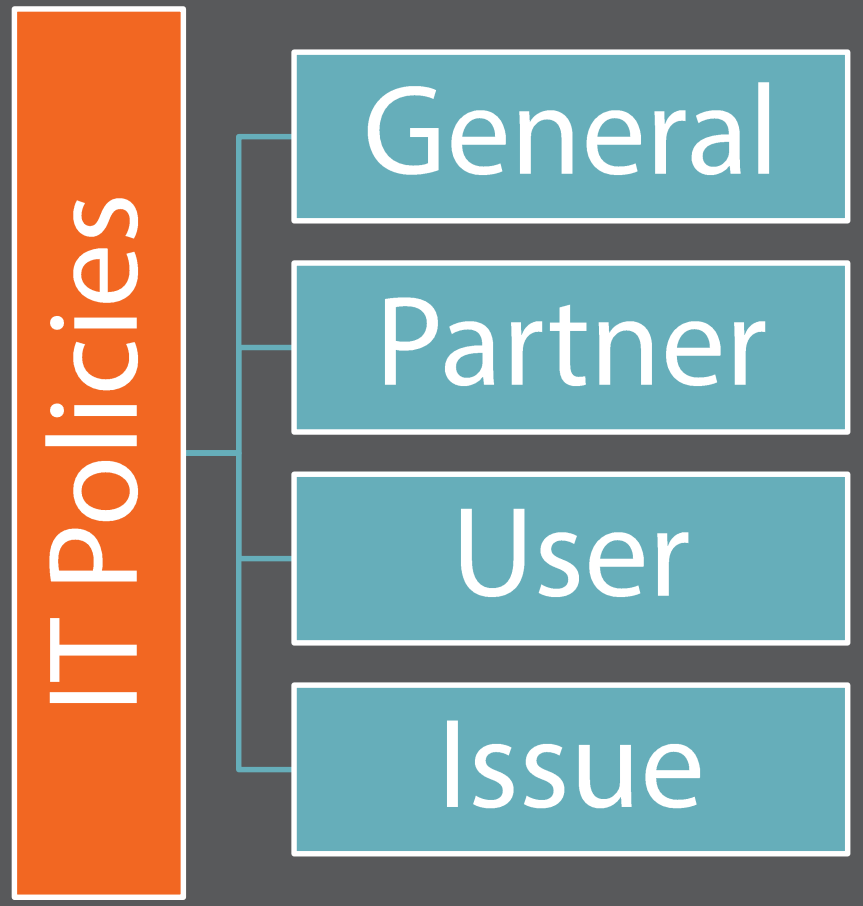
pluralsight

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

pluralsight

Taxonomy of Security Policies



pluralsight

Security Polices Examples

Acceptable-use

Passwords

User account

Email security

Remote-access

Firewall

Information protection

Network connection

Special access

pluralsight

Vulnerability Research

pluralsight

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

pluralsight

Places to Look

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

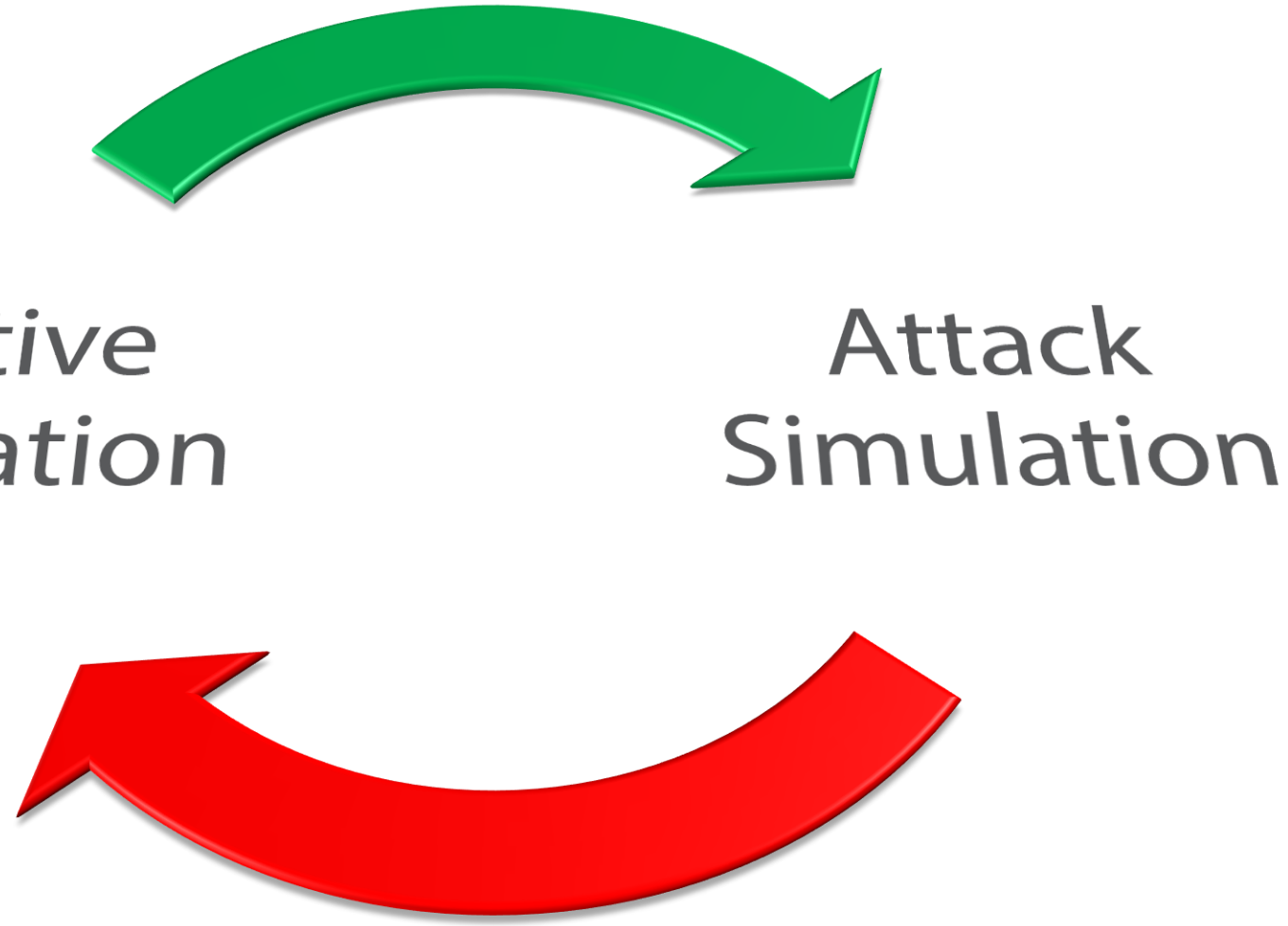
- www.hackerstorm.co.uk
- www.eccouncil.org
- www.securitymagazine.com
- www.securityfocus.com
- blogs.windowssecurity.com
- www.hackersjournals.com
- www.zdnet.com/topic/security

pluralsight

Penetration Testing

pluralsight

Pen-testing - "Not a Job at Bic"



pluralsight

Why?

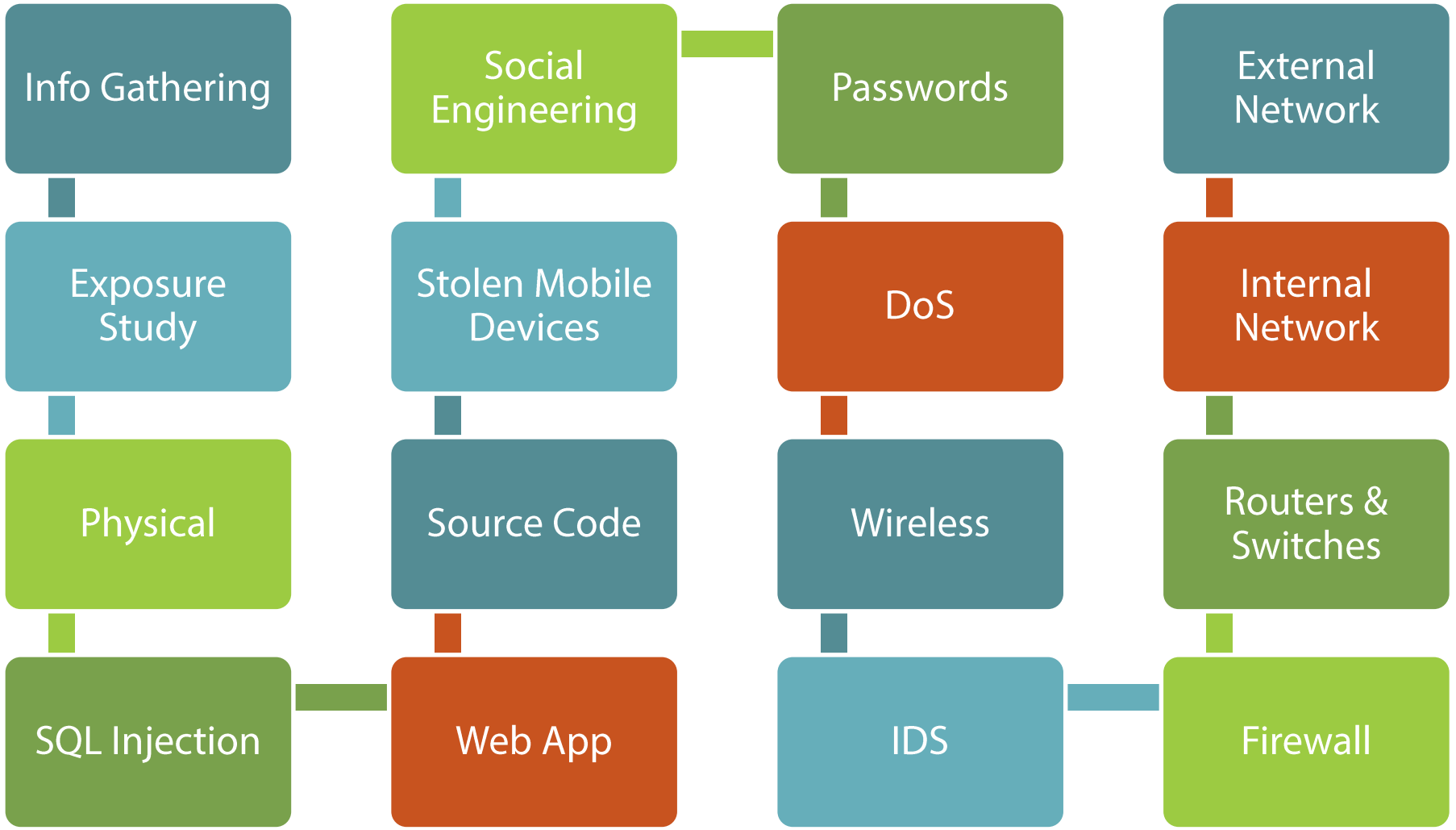
ID threats
Reduce ROSI
Gauge efficiency

Upgrades
Test controls
Maintain standards

Reassurance
Best practices
In-house development

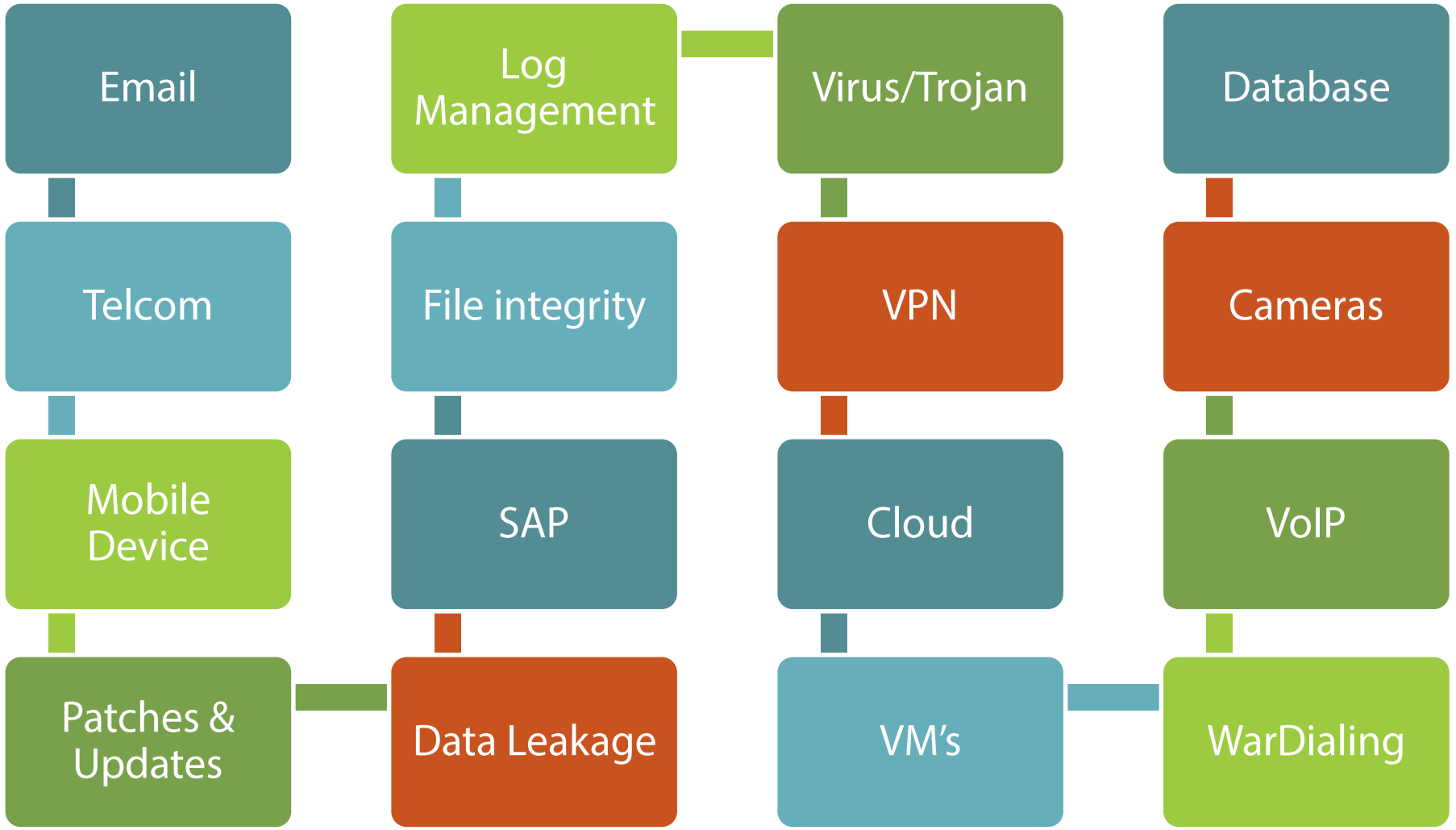
pluralsight

Method



pluralsight

Method



pluralsight

Summary

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

pluralsight

Summary

- Vulnerability Research
- Data Leakage
- The Role of AI/ML
- Penetration Testing

pluralsight