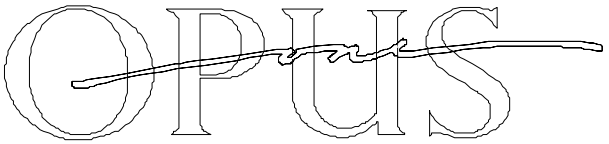
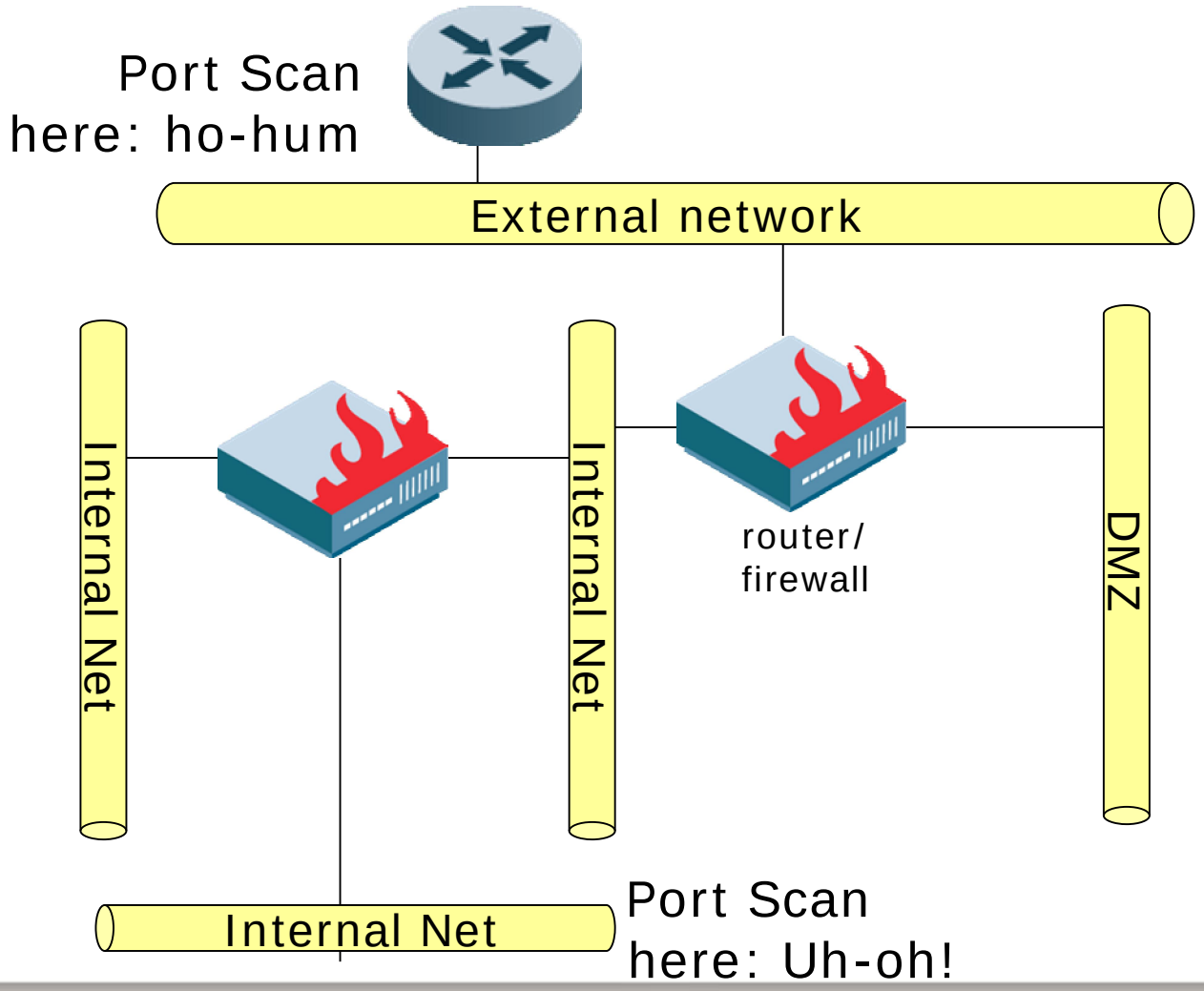
How to Make

Joel M Snyder
Senior Partner
Opus One
jms@opus1.com



Agenda: IDS

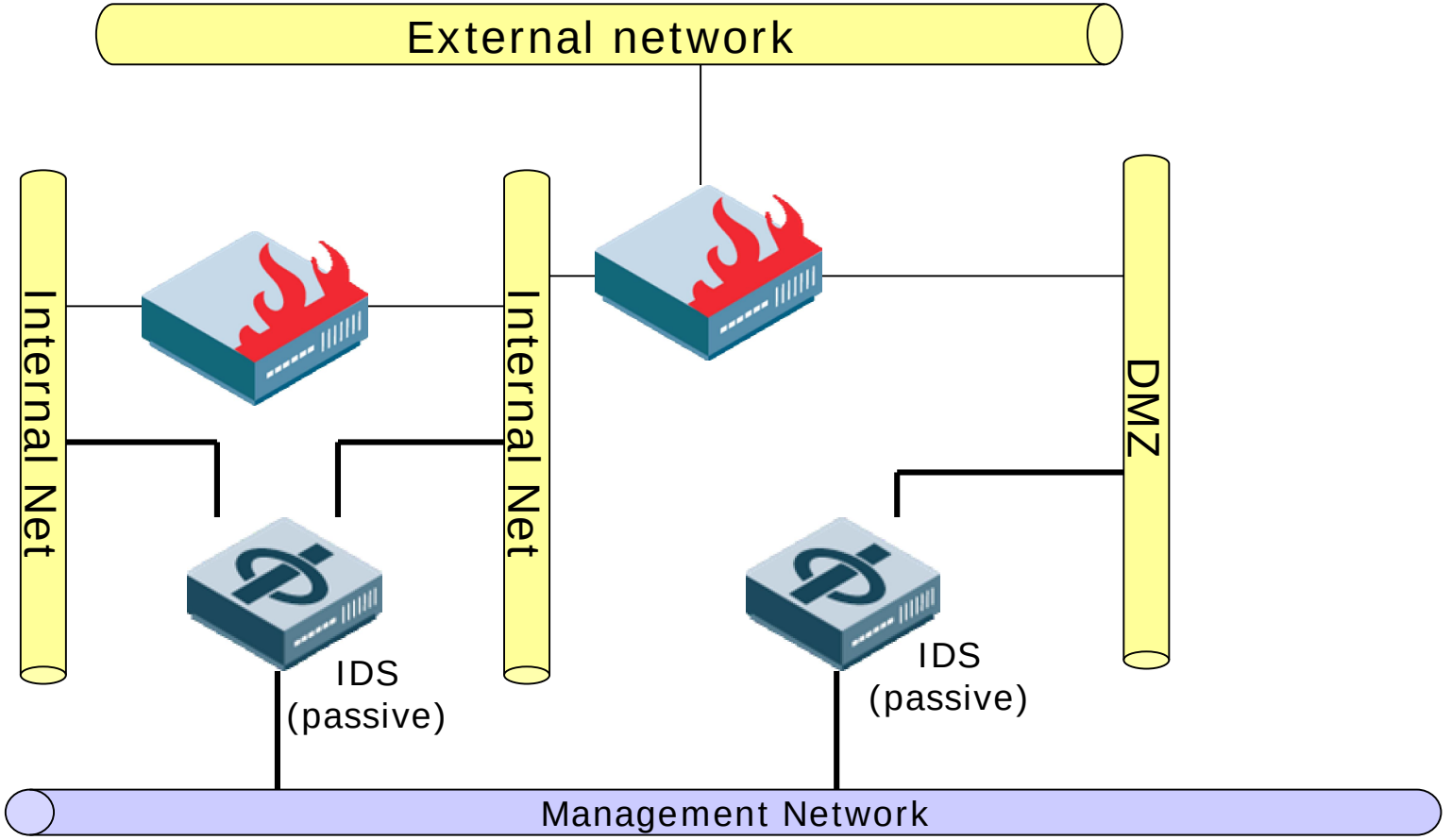
- Why are we looking at IDS?
- The 5 “Ws” of IDS Analysis
- The IDS Analysis Cycle



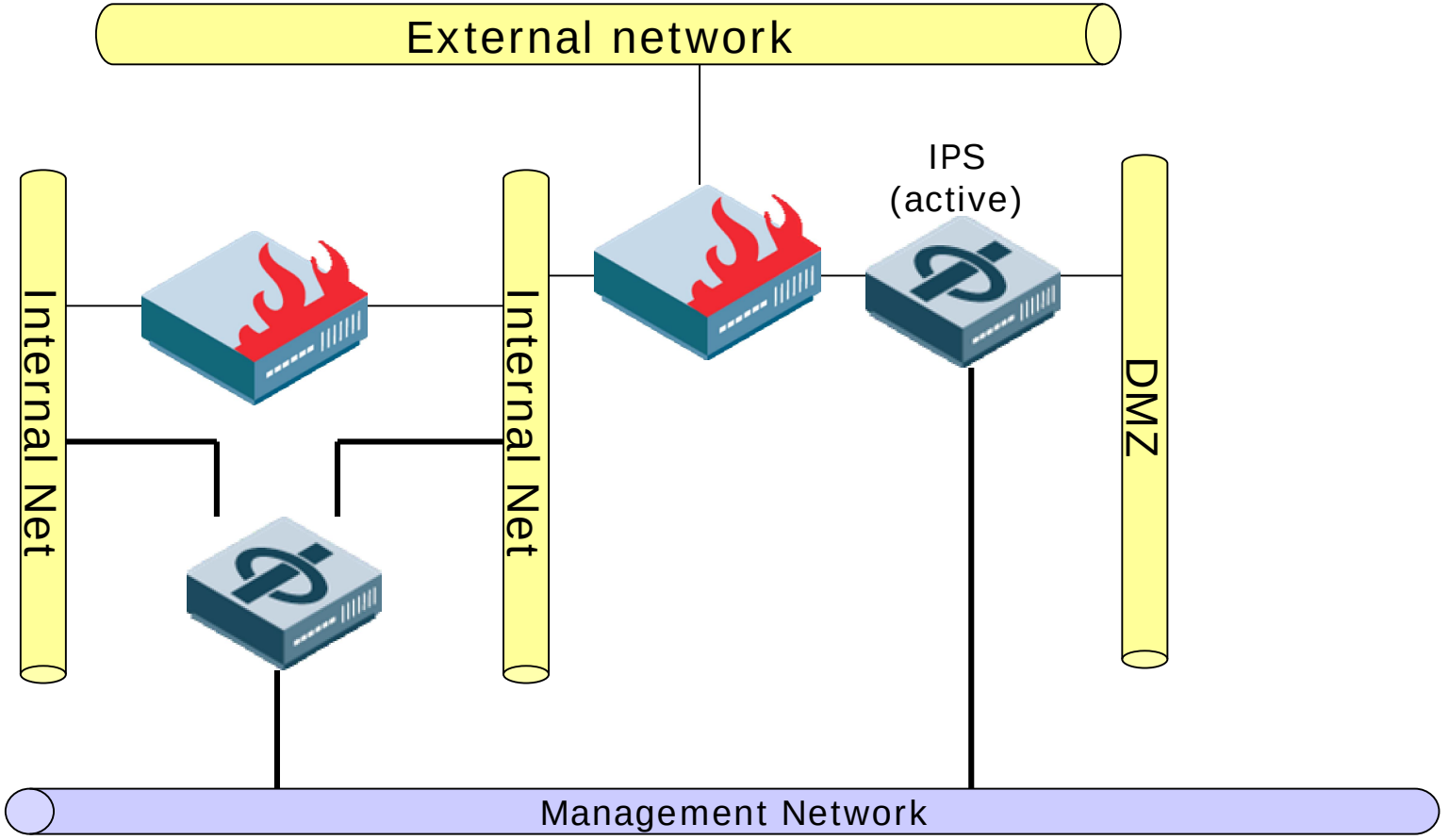
Enterprises want to understand and block security problems on their networks.

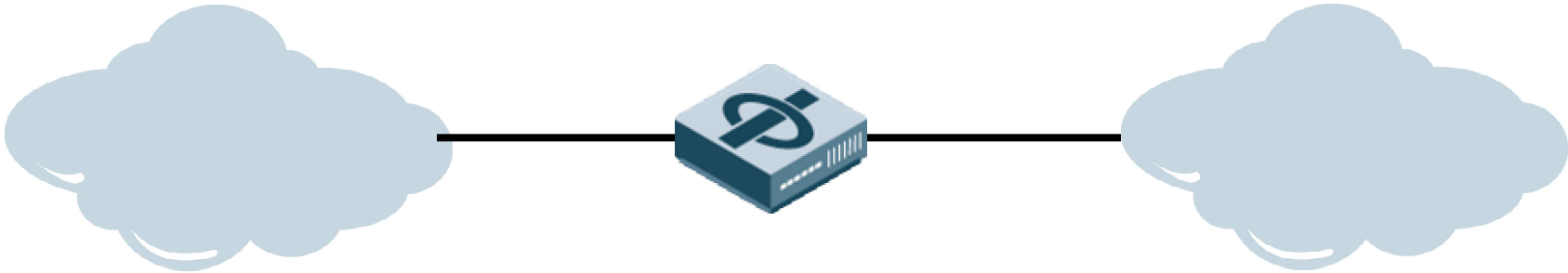
On each network, “intrusion” can mean something very different

Intrusion Detection Systems
Identify Security Problems on Nets



Intrusion Prevention Systems *Block* Security Problems on Nets





Signature-based: look for specific traffic that matches specific descriptions, or is “out of spec” in some particular way

Anomaly-based: observe deviations from “baseline” normal traffic and block or alert

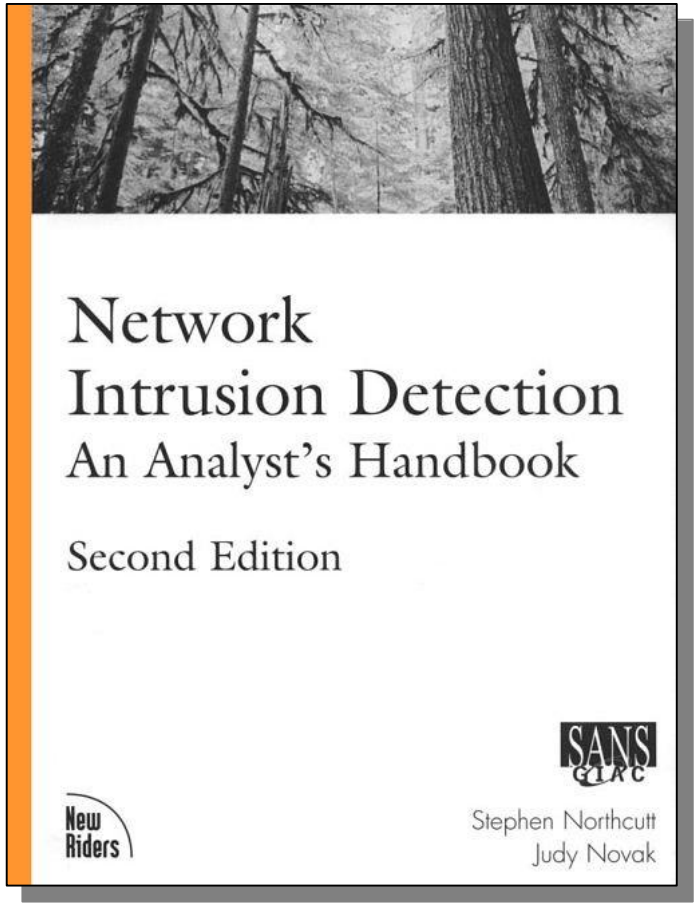
Niche:

Wireless: have specific knowledge of RF and RF behaviors; looking for wireless-specific issues

Rate-based: watch flows and connections and limit or modify TCP/UDP to pre-determined norms or to guarantee response time

Technology With Methodology

- You must have some of both before you can even start
- Suggested reading: "Network Intrusion Detection, 3/e" by Northcutt & Novak



Five *W*s

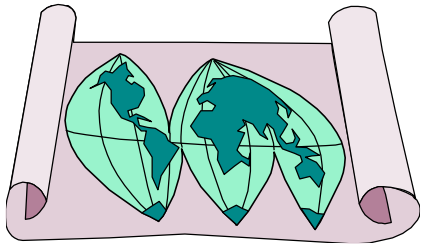
- Where is everything?
- What do I care about?
- Who is responsible? Who do I tell?
- When do we do analysis?
- Why are we doing this?

Yes, this sounds dull and uninteresting.

But if you don't do it, then you'll never know what to do with the data your IDS gives you

Network?

- You can't watch all ports on all devices connected to the network
  - Even if you had infinite CPU time...
- So you need to know what each device is doing and who is taking care of them



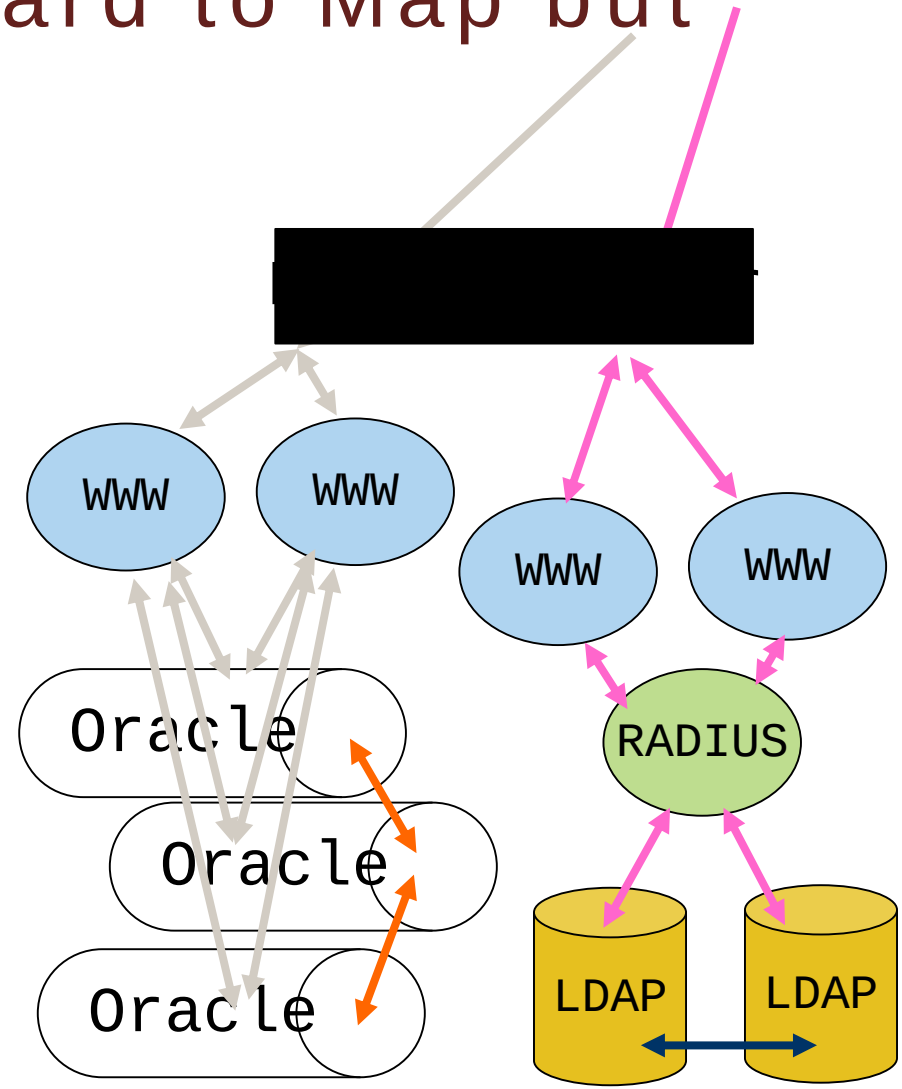
- Mapping your network is part of your preparation for IDS analysis

- Physical layer topology helps to understand what wires and bridges go where
- Network layer topology

  paths
- Application layer topology shows you what business-critical resources are present

Applications Are Hard to Map but

- Physical layer topology helps to understand what wires and bridges go where
- Network layer topology identifies systems and routing paths
- Application layer topology shows you what business-critical resources are present



- Once you have mapped your network, you have two main questions to ask:

What is visible to my IDS/IPS?	Which network elements are important to me?
• Generally, certain inside-to-inside flows will not be visible • Also, certain outside-to-inside flows might not pass a sensor • That whole encryption thing	• Physical • Network • Application

Spend Time on Critical and Important Systems

Quick: Your IPS says that

attacks on “imprimo.”

Do you care?

- Answer: No.
- It’s a printer.
- It doesn’t run SQL.
- No one cares about it anyway.

Quick: Your IPS says that someone is trying SQL attacks on system “repono.”

Do you care?

- Answer: Yes!
- It’s an SQL server.
- It’s behind the firewall.
- It generates my paycheck.

Who Is Responsible?

System Mgmt Responsibility	Incident Responsibility
• Who takes care of the network? • Who takes care of the servers and routers? • Who takes care of the applications?	• Who do I tell? • What are they responsible for doing? • What if they don't do it? • Then what do I do?

When Do We Do Analysis?

- Immediately?
  - Are we concerned about catching someone in the act?
- Daily?
  - Do we want to know quickly if there is a problem on our net?
- Weekly? Monthly? Quarterly? Annually?
  - Are we looking for long-term trends?
- Never?
  - Do we do this for forensics and tuning ?

- You must be doing Intrusion Detection analysis and

- What is it?

What did your business case say?

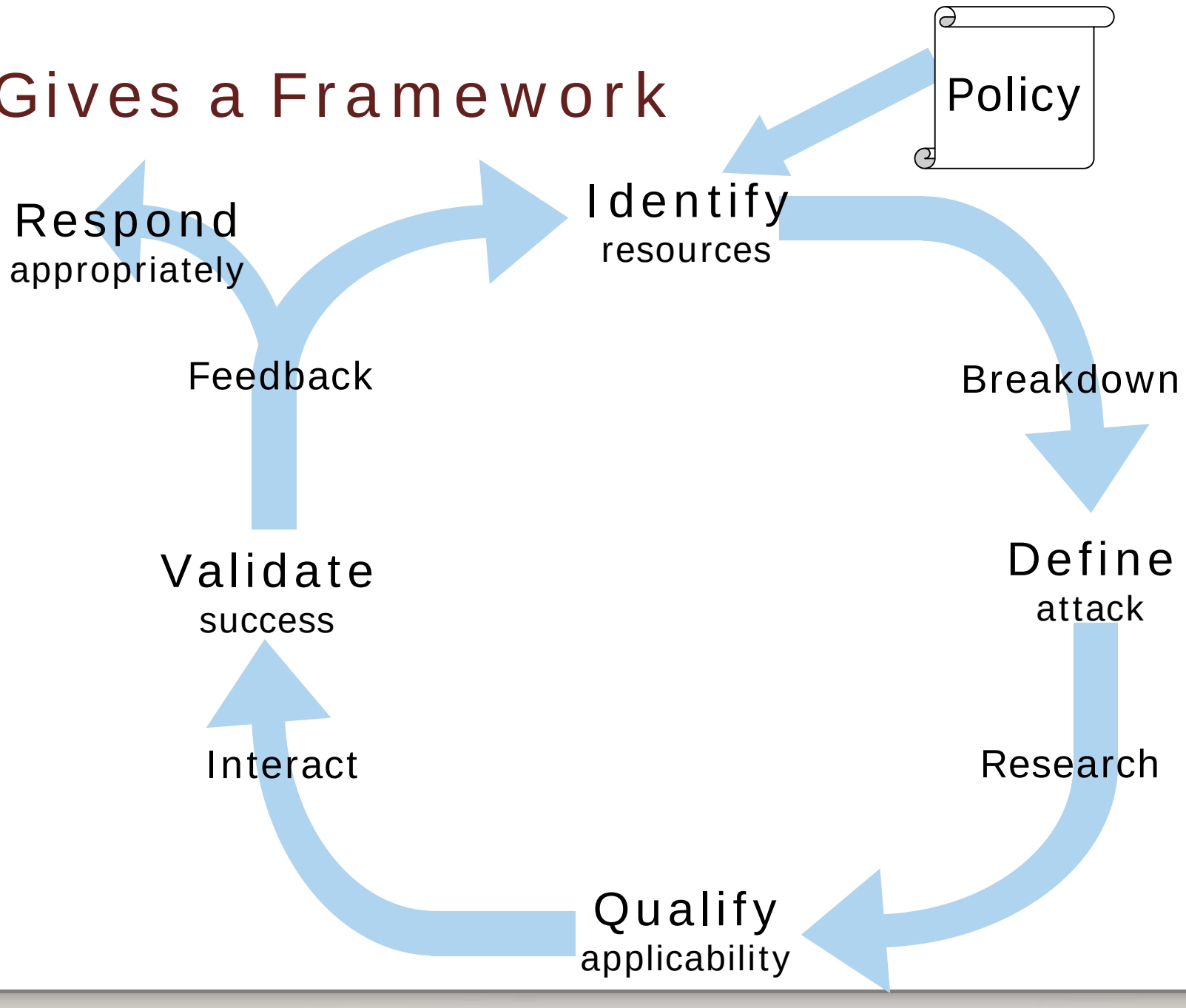
- Avoid common exploits? Look for internal worms and malware?
- Discover misbehaving users and systems?
  - Find out how you were broken? Who? Why? When?
    - Tool for your application and network managers? Tool for security manager?

and You Need a Policy

- This is even more important than the policy that you didn't write to go along with your firewall

- Where is everything?
- What do I care about?
- Who is responsible? Who do I tell?
- When do we do analysis?
- Why are we doing this?

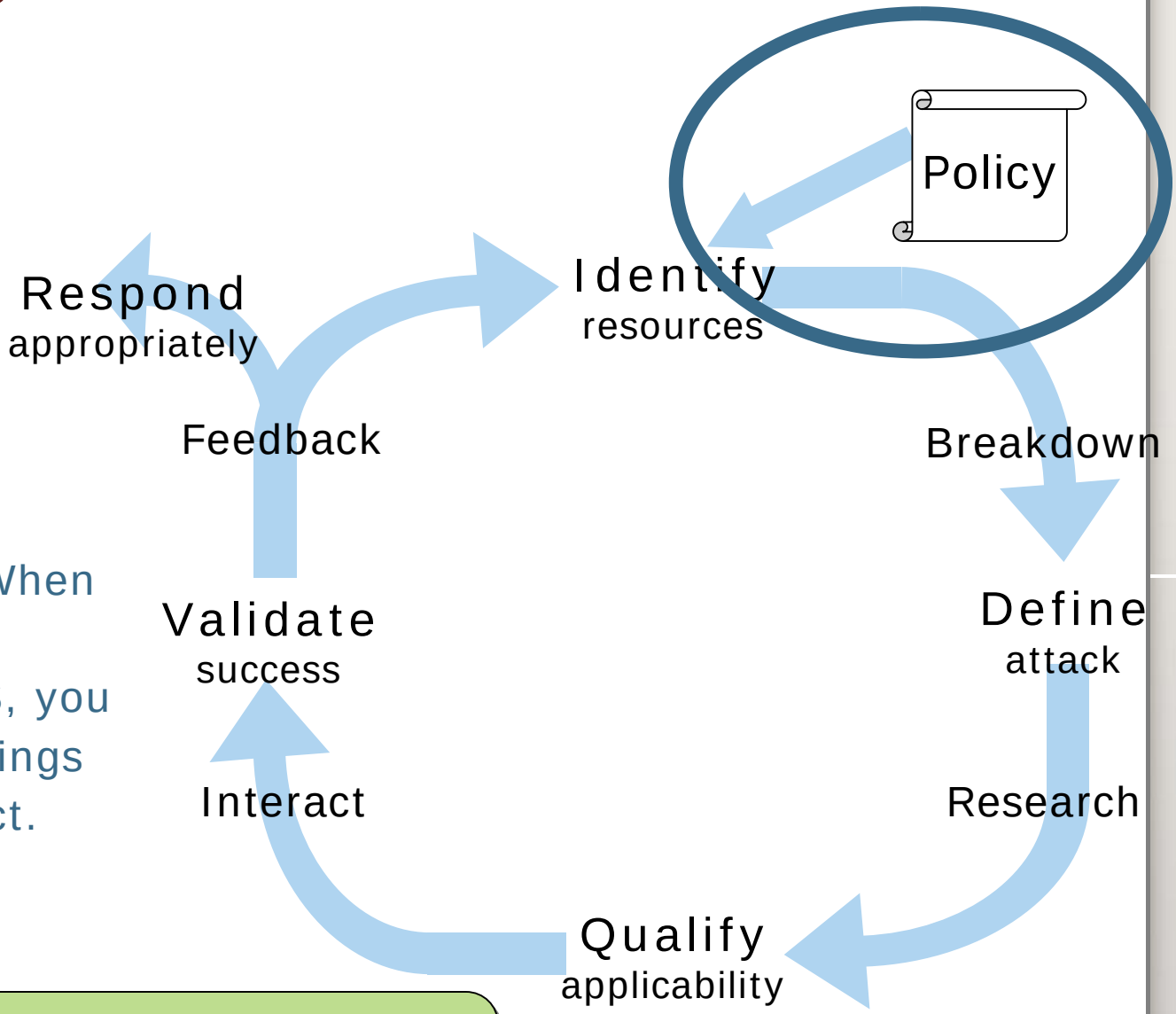
Gives a Framework



Analysis Is

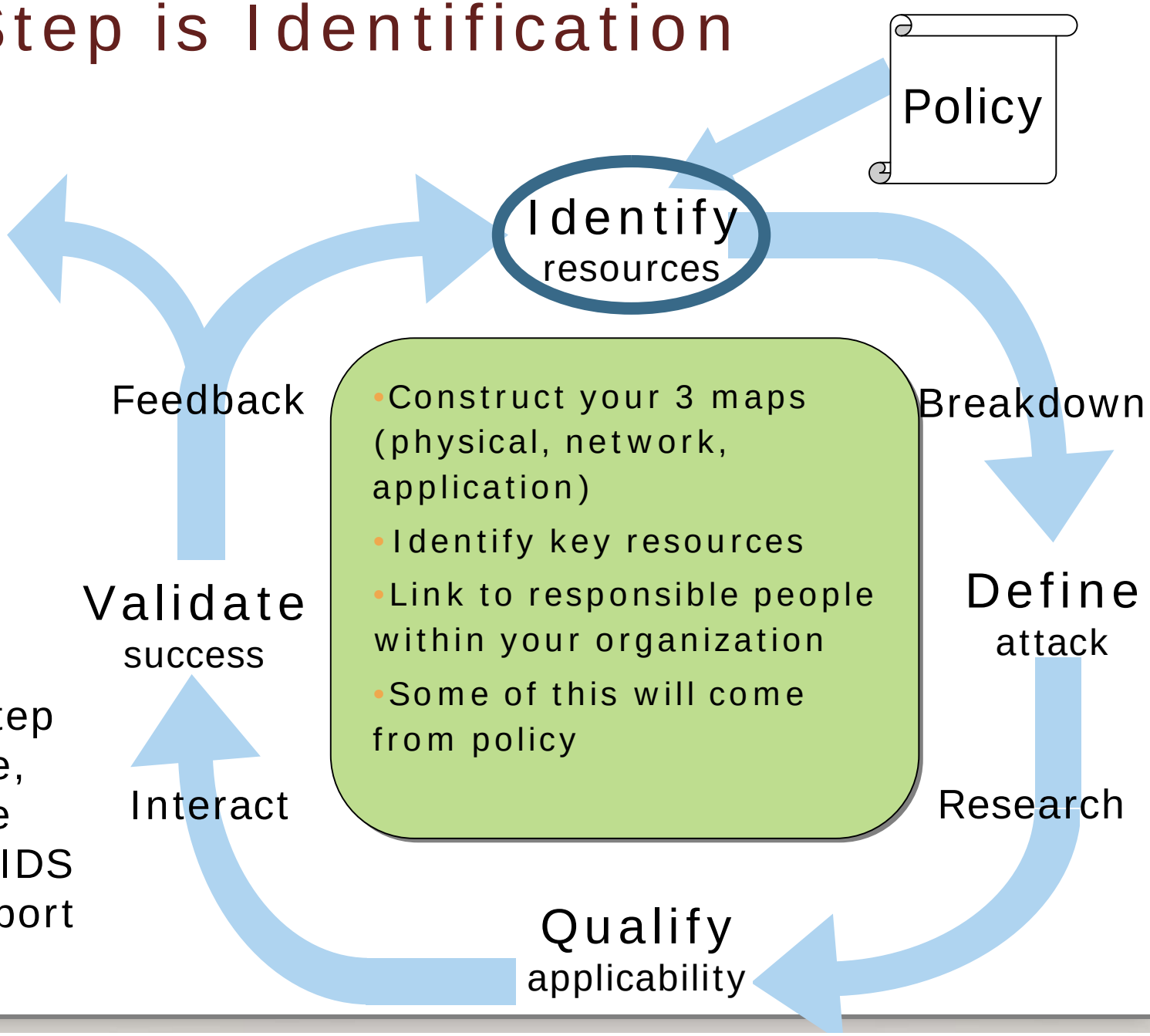
Policy

- As you dive in, remember Paul Proctor's rule: "When you first start operating an IDS, you will find many things you do not expect. Be prepared."



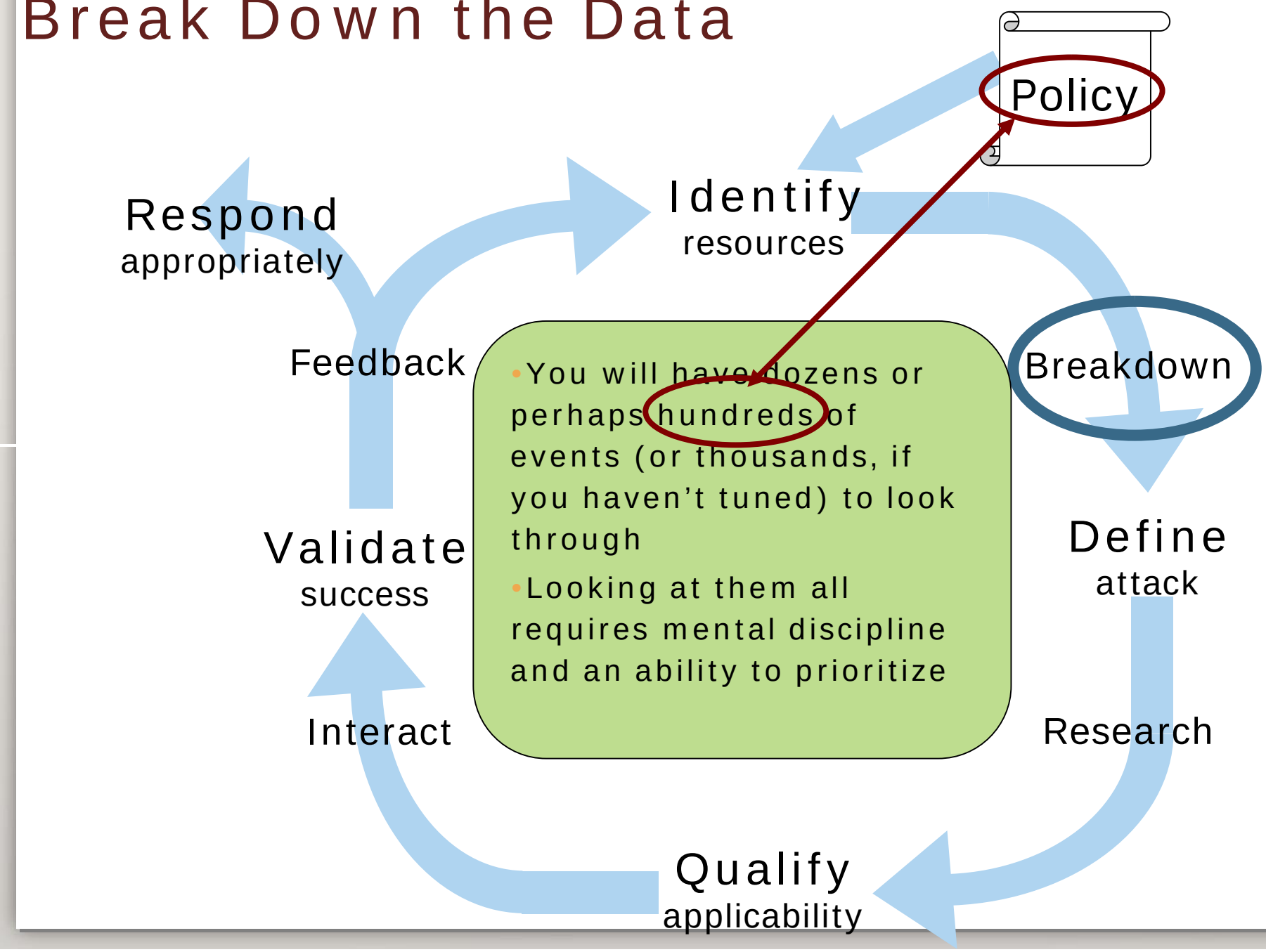
Which implies, perhaps, that policy is also grounded in analysis

First Step is Identification

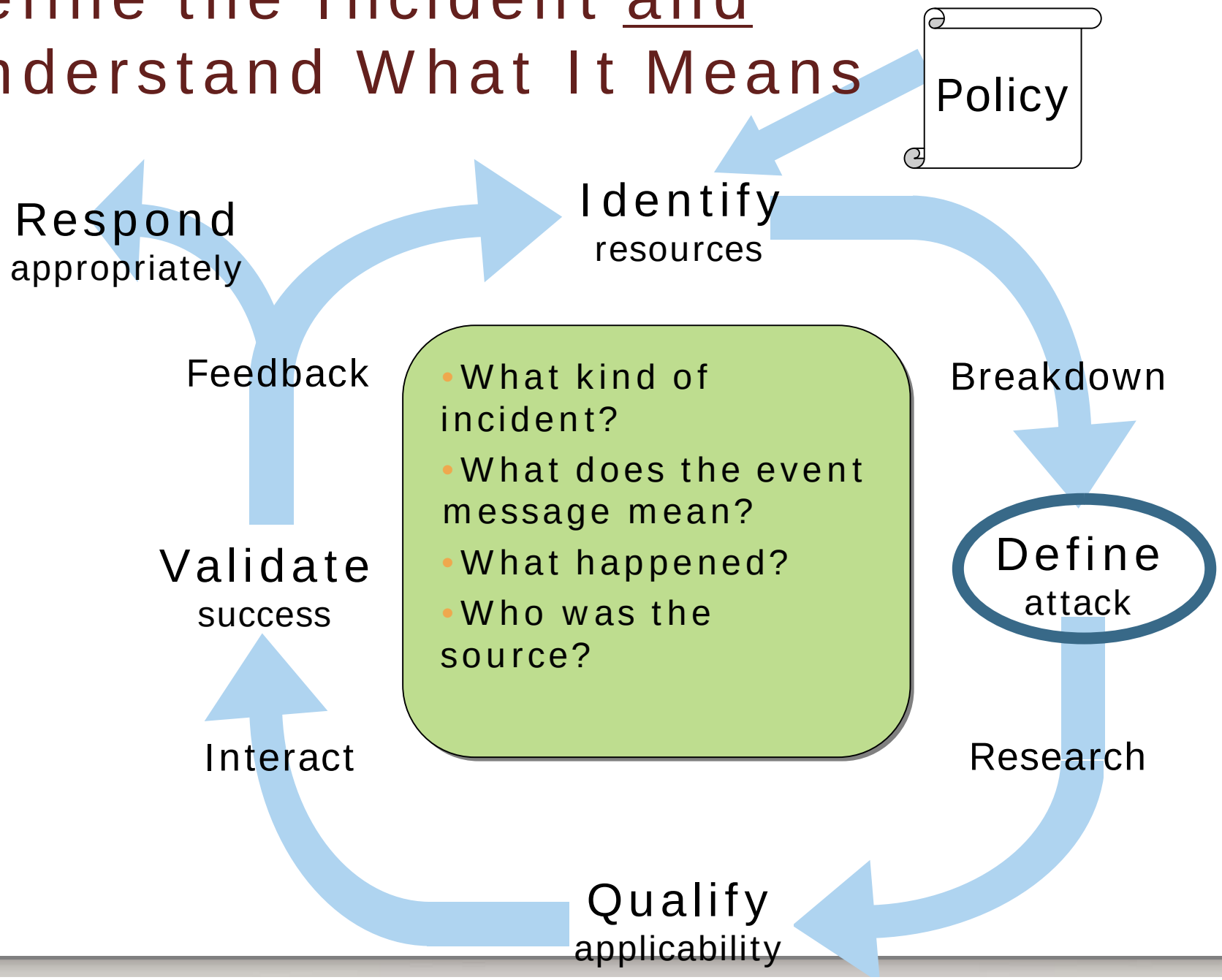


For each step in the cycle, identify the tools your IDS has to support this step

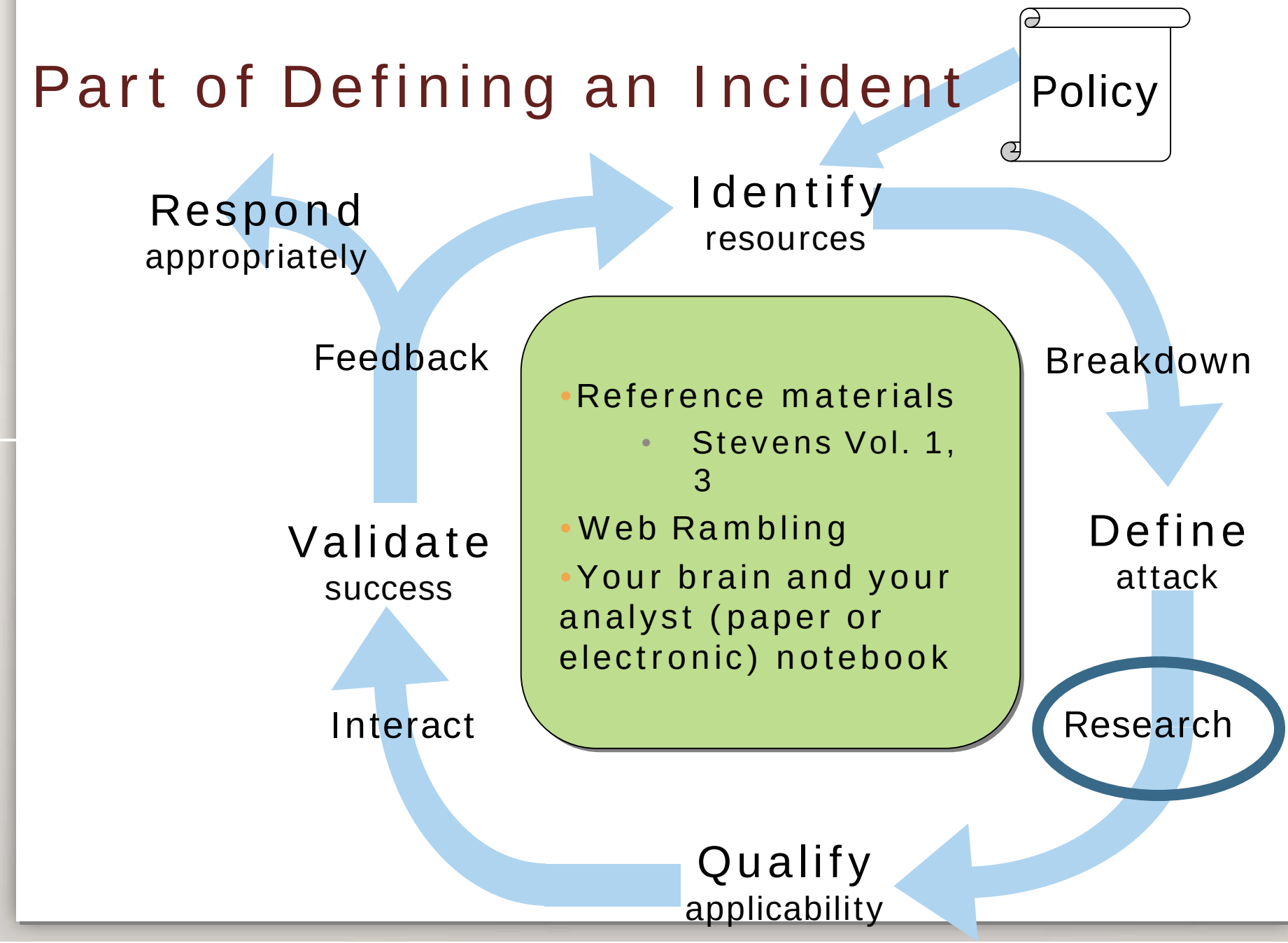
Break Down the Data



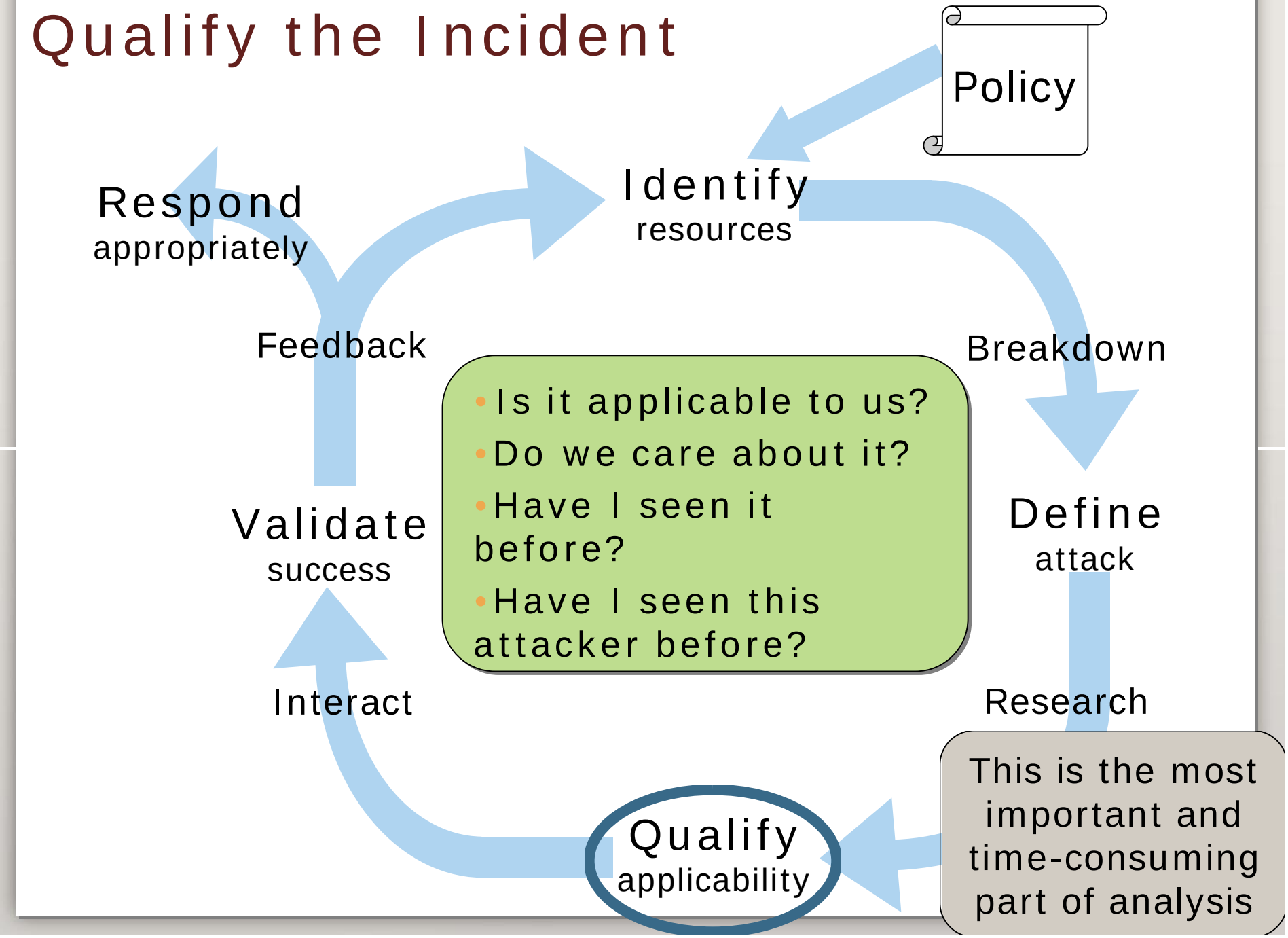
Define the Incident and Understand What It Means



Part of Defining an Incident



Qualify the Incident



Answering a Lot of Questions

- Does this host actually exist?
  - Attacks on non-existent hosts are pretty low priority
- Is this host vulnerable to the attack?
- Go back to your "Identify Resources" maps and start talking to the responsible people

Key conclusion: Without a comprehensive map, you cannot do useful analysis. *Information gathering is painful, but there are tools to help.*

Your Incidents and Events

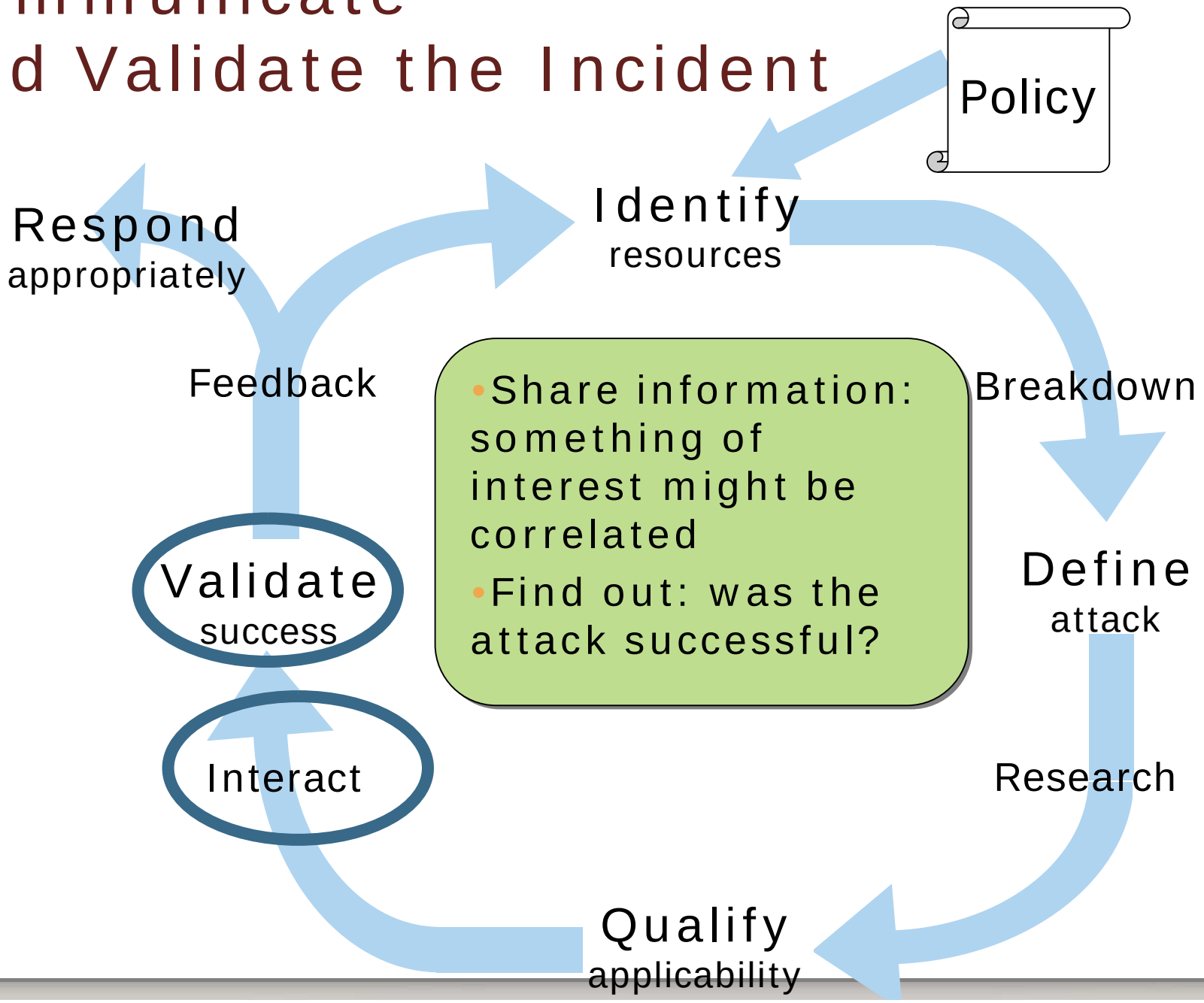
–
(sys + net countermeasures)

- Criticality: How bad will it hurt?
  - 5: Firewall, DNS, router
  - 4: Email gateway/server
  - 3: Executive's desktop
  - 2: User desktop
  - 1: MS-DOS 3.11 on soda machine
- Lethality: How likely to do damage?
  - 5: Multi-system root access
  - 4: Single-system root
  - 3: DoS total lockout
  - 2: User-level access
  - 1: Unlikely to succeed
- System Countermeasures
  - 5: Totally patched, modern O/S, internal firewall
  - 3: Older O/S, partially patched
  - 1: Unpatched/Unmanaged
- Network Countermeasures
  - 5: Validated, restricted firewall
  - 4: Firewall, plus some unprotected connections
  - 2: Permissive firewall
  - 1: No firewall

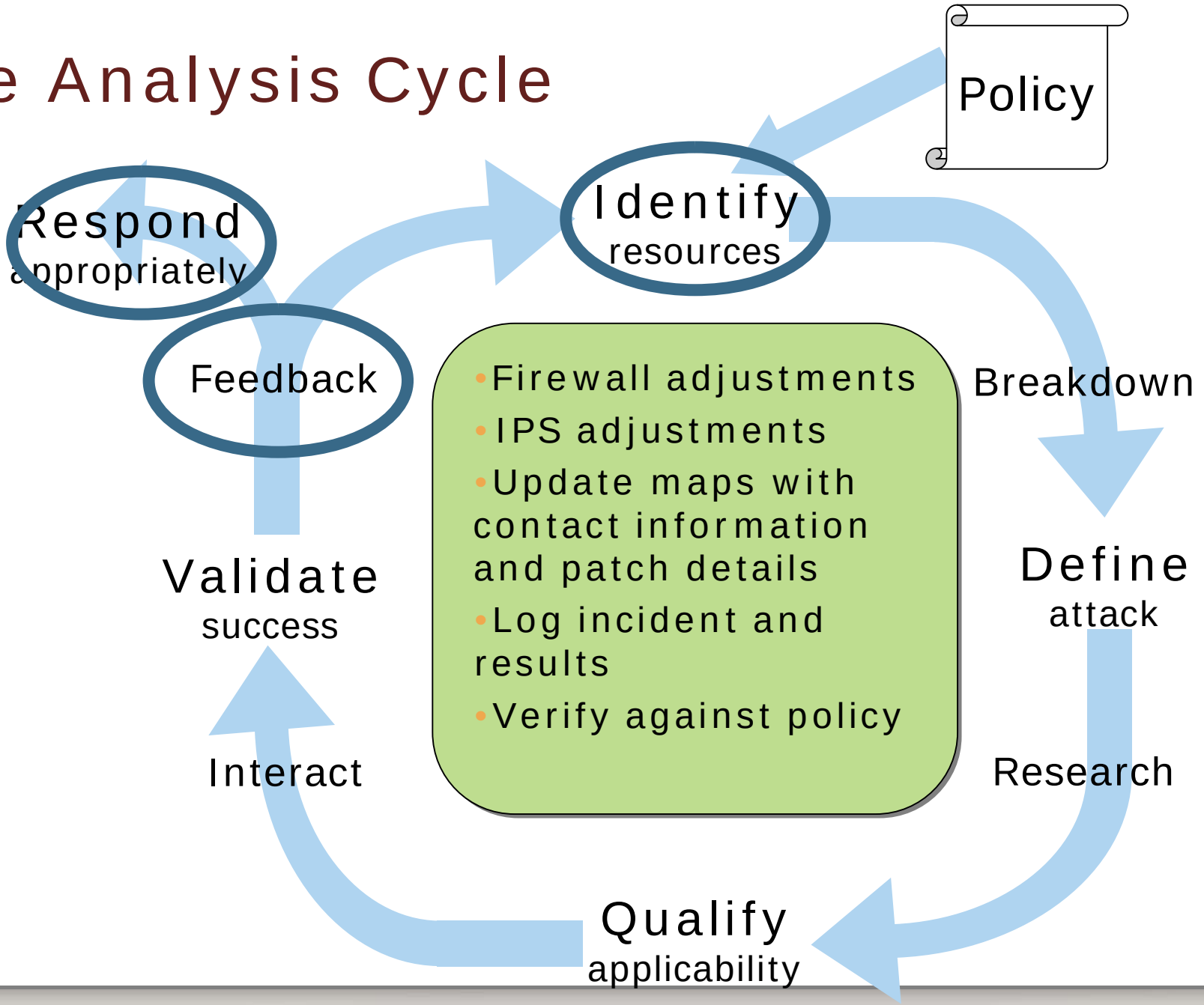
Two More Questions

“Did the event cause a state change?”	“Is there something else going on here?”
• Is the behavior of the target system different after the event than before the event?	• What other correlation can we make between this attacker, the attacked system, and the type of incident with past incidents?

Communicate and Validate the Incident



the Analysis Cycle



Useful

- Follow the “5 Ws” and prepare background information on the network
- Identify tools within your IDS to help each step in the Analysis Cycle
- Set aside 2 to 3 hours each week to practice and

Thanks!

Joel Snyder
Senior Partner
Opus One