
YOU BUILD SIEM
memegenerator.net

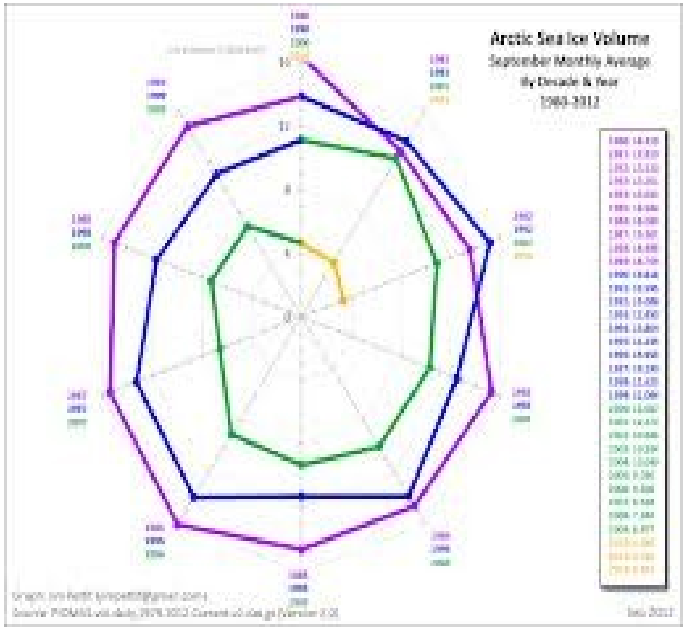

I DON'T ALWAYS LOOK AT DASHBOARDS
BUT WHEN I DO, I NEED PRETTY PICTURES
memegenerator.net

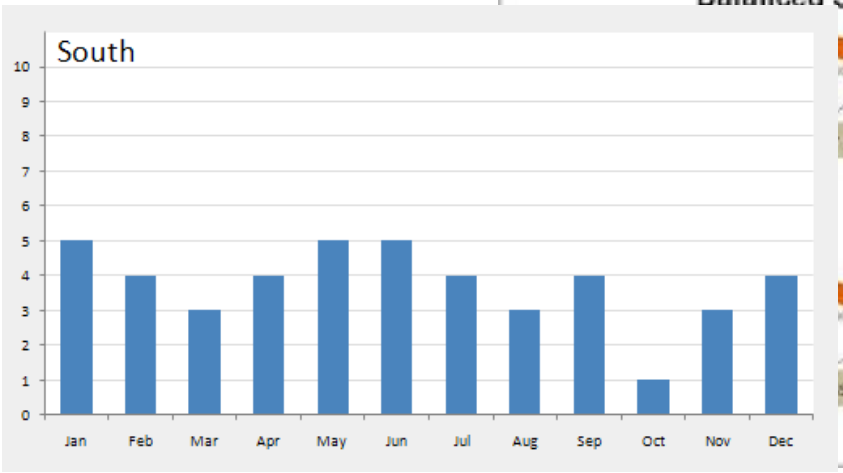
Internet had lots of examples and tutorials for specific or advanced dashboards

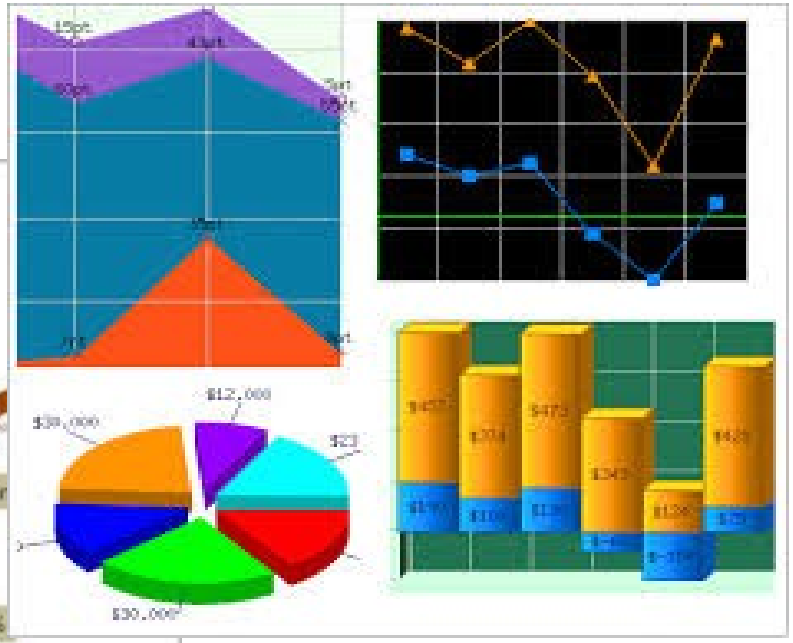
Top 10 lists of other things were easy to find

But no dashboard Top 10 list

Which led to.....







Quick Win, Industry Agnostic, SIEM Dashboards

Craig Bowser

Introduction

15+ years in InfoSec

Worked mainly in DoD with some DOJ and now DOE experience

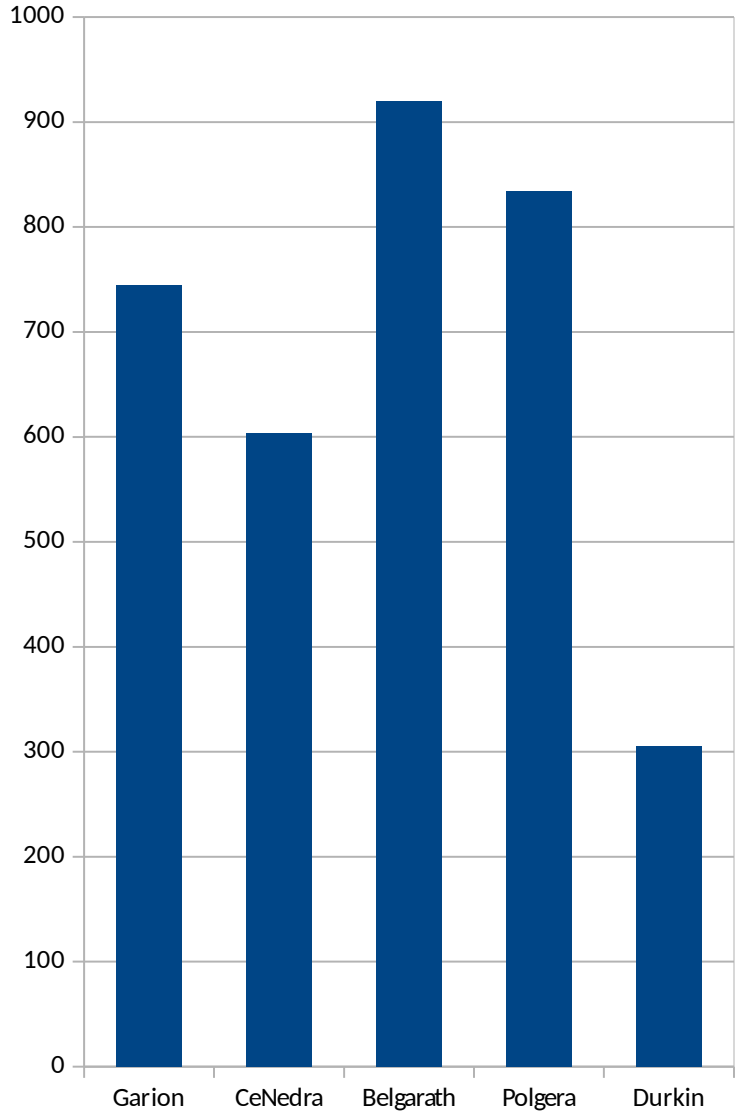
GSEC GCED CISSP, yeah!

Christian, Father, Husband, Geek, Scout Leader who also does some woodworking

To Do List > To Do Open Slots

Criteria for Dashboards

1. Must use data types that a
2. Must use data from types first 'connected' to SIEM
3. Must be simple to create
4. Must be relevant in any S(
5. Must be able to visually cc a way that directs further inve



Dashboard

Impact:

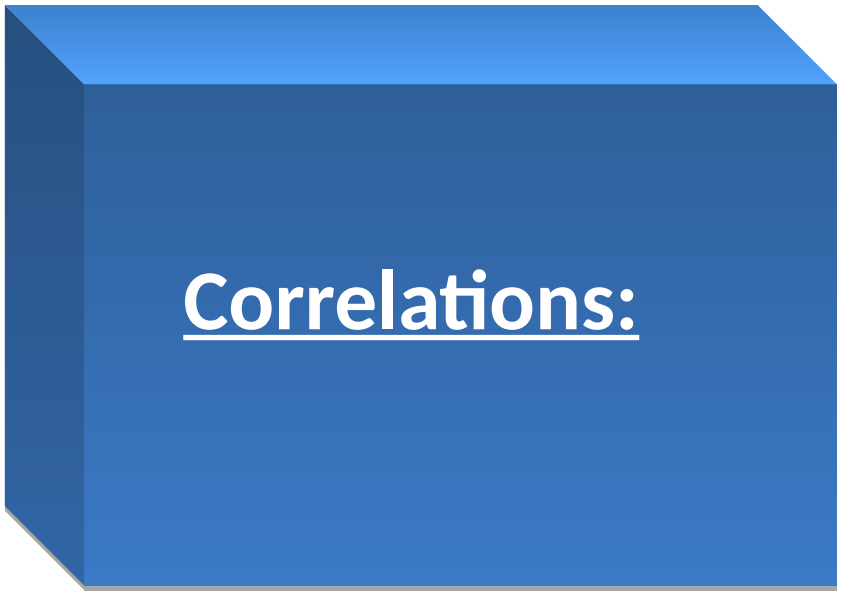
What does this dashboard tell you?

What are the important things you should know when you view this dashboard?

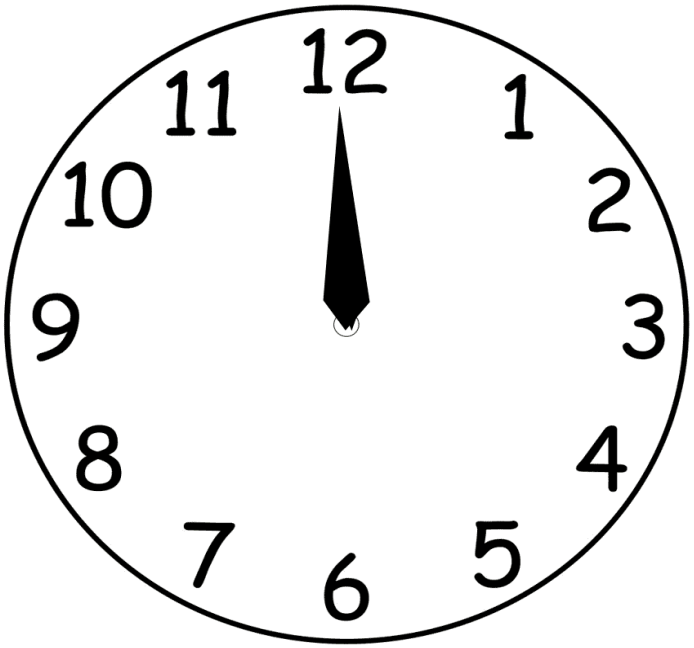
Dashboard

What you can cross reference the data with to determine more about the events?

What other events can you use to make a better decision regarding events seen?



Column A



Column B

Username

IP ⚌ ▭ Hostname

Filename/Hash

Dashboard

Challenge:

What issues are there that make this dashboard hard to use?

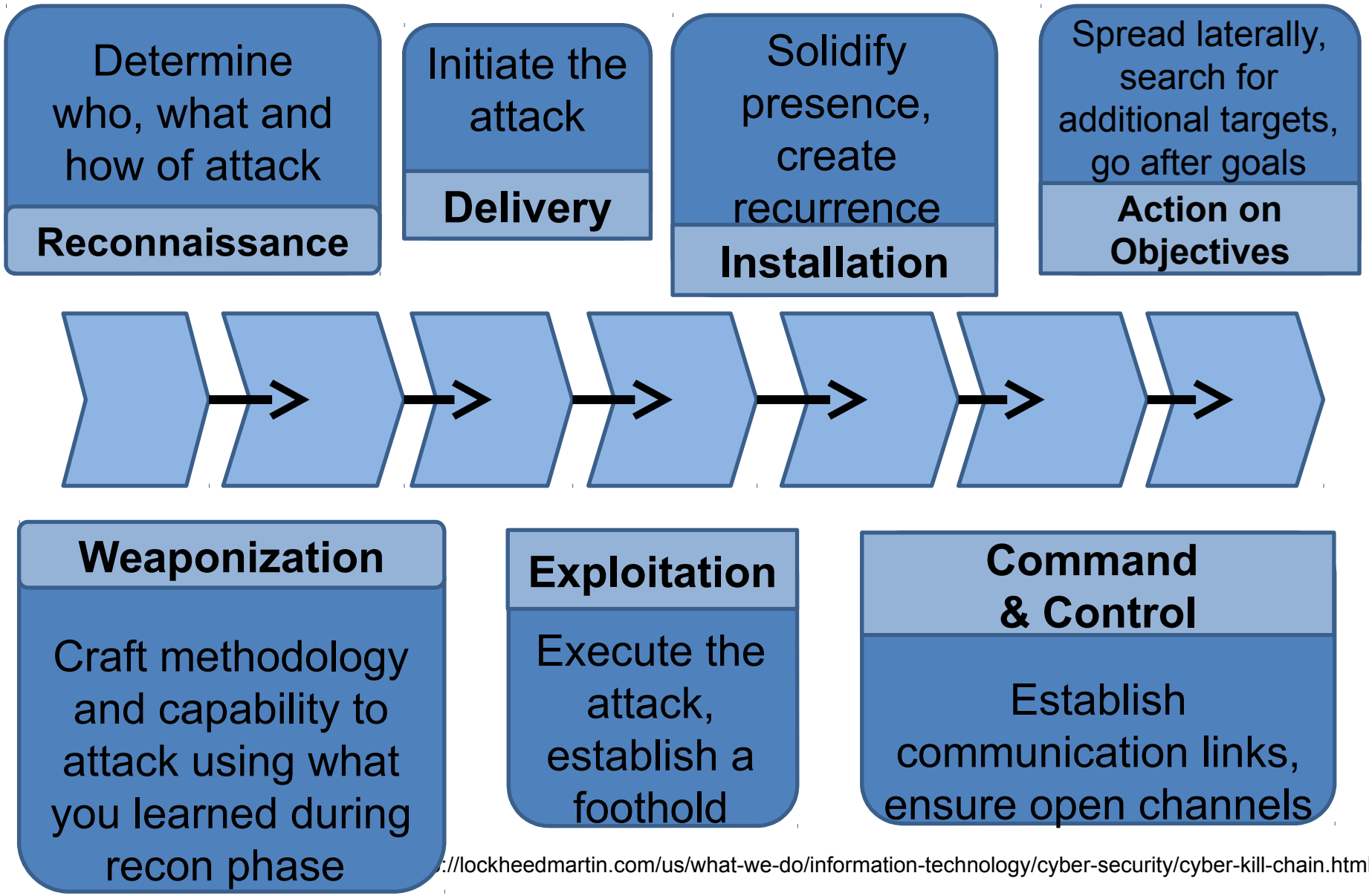
What problems cause the important events in this dashb
missed?

Dashboard

Examples:

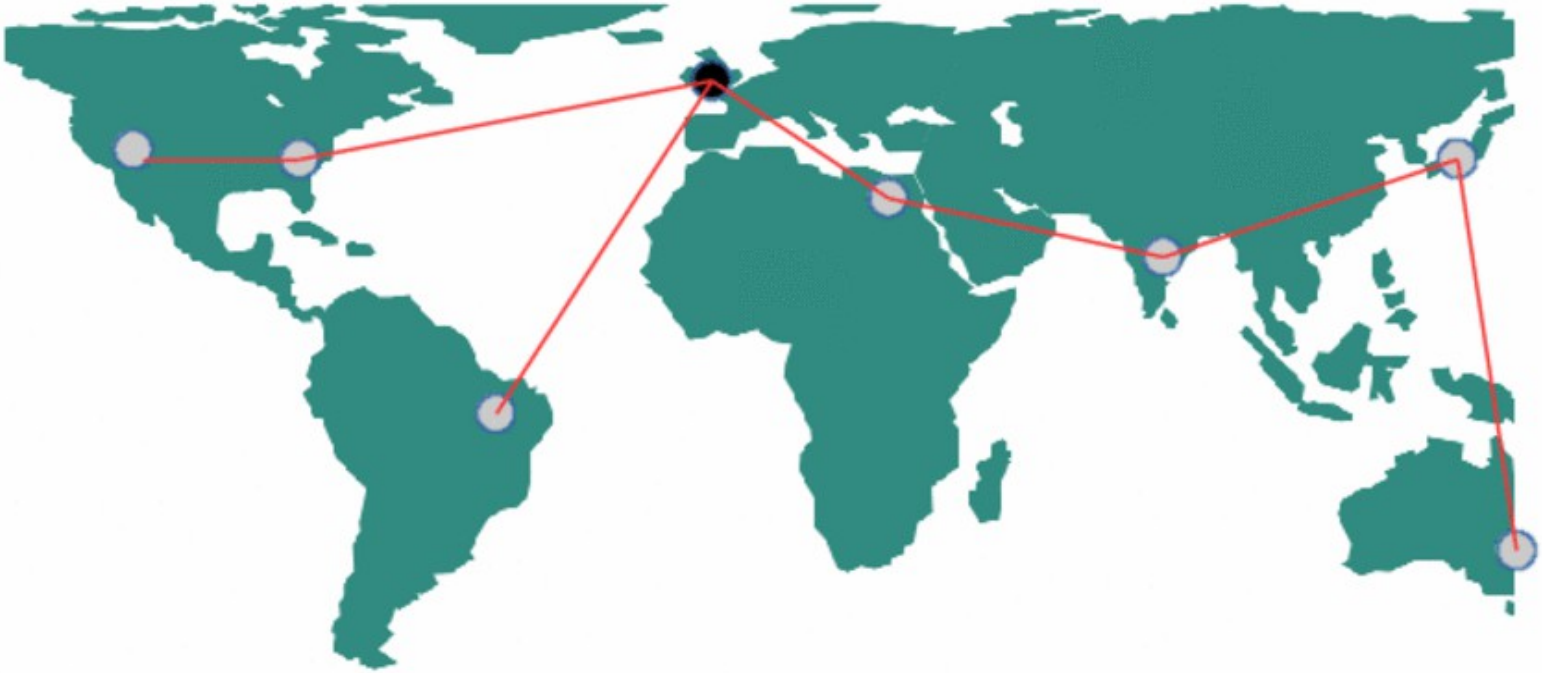
What are examples, from real life if possible, of how this dashboard was used to resolve actual issues?

Cyber Kill Chain ©



://lockheedmartin.com/us/what-we-do/information-technology/cyber-security/cyber-kill-chain.html

Traffic World Map



10
9
8
7
6
5
4
3
2
1

Correlations

Impact

Challenge

Examples

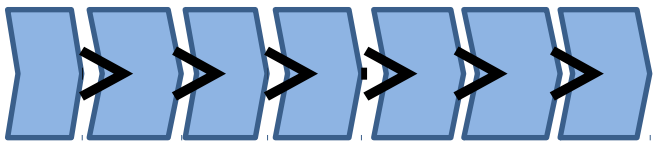
Traffic World Map

10
9
8
7
6
5
4
3
2
1

Impact:
Management Eye Candy. Alert when node is down

Challenge

Examples



Traffic World Map

10
9
8
7
6
5
4
3
2
1

Correlations:
Nagios/OpenView.
Traffic Spikes. High bandwidth usage.

s:

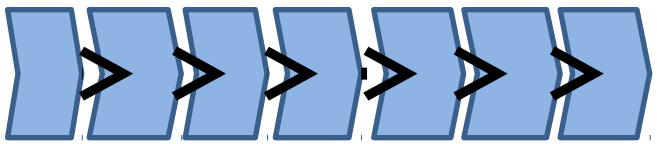
ns:

ions

Impact

Challenge

Examples



Traffic World Map

10
9
8
7
6
5
4
3
2
1

Challenge:
Getting GPS coordinates of sites properly into SIEM

Challenge:

Challenge:

Impact

Examples

Traffic World Map

10
9
8
7
6
5
4
3
2
1

Examples:
DDOS attacks,
Detect new
devices/connections

s:

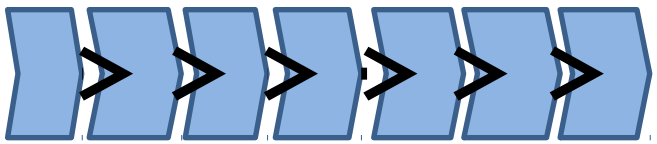
s:

es:

Impact

Challenge

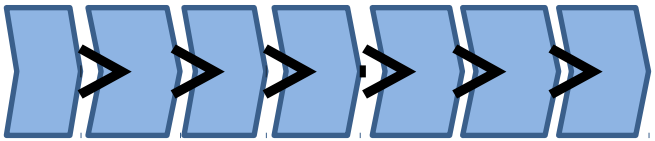
Examples

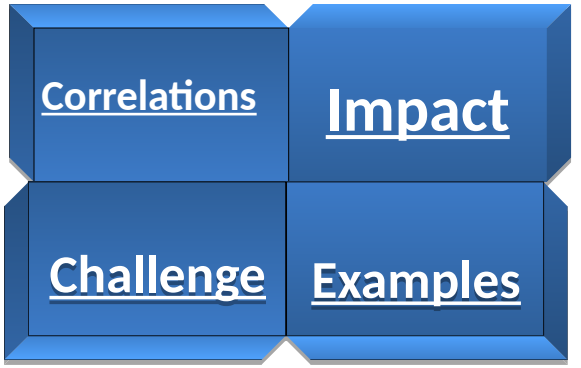


Alerts for New Devices/Software

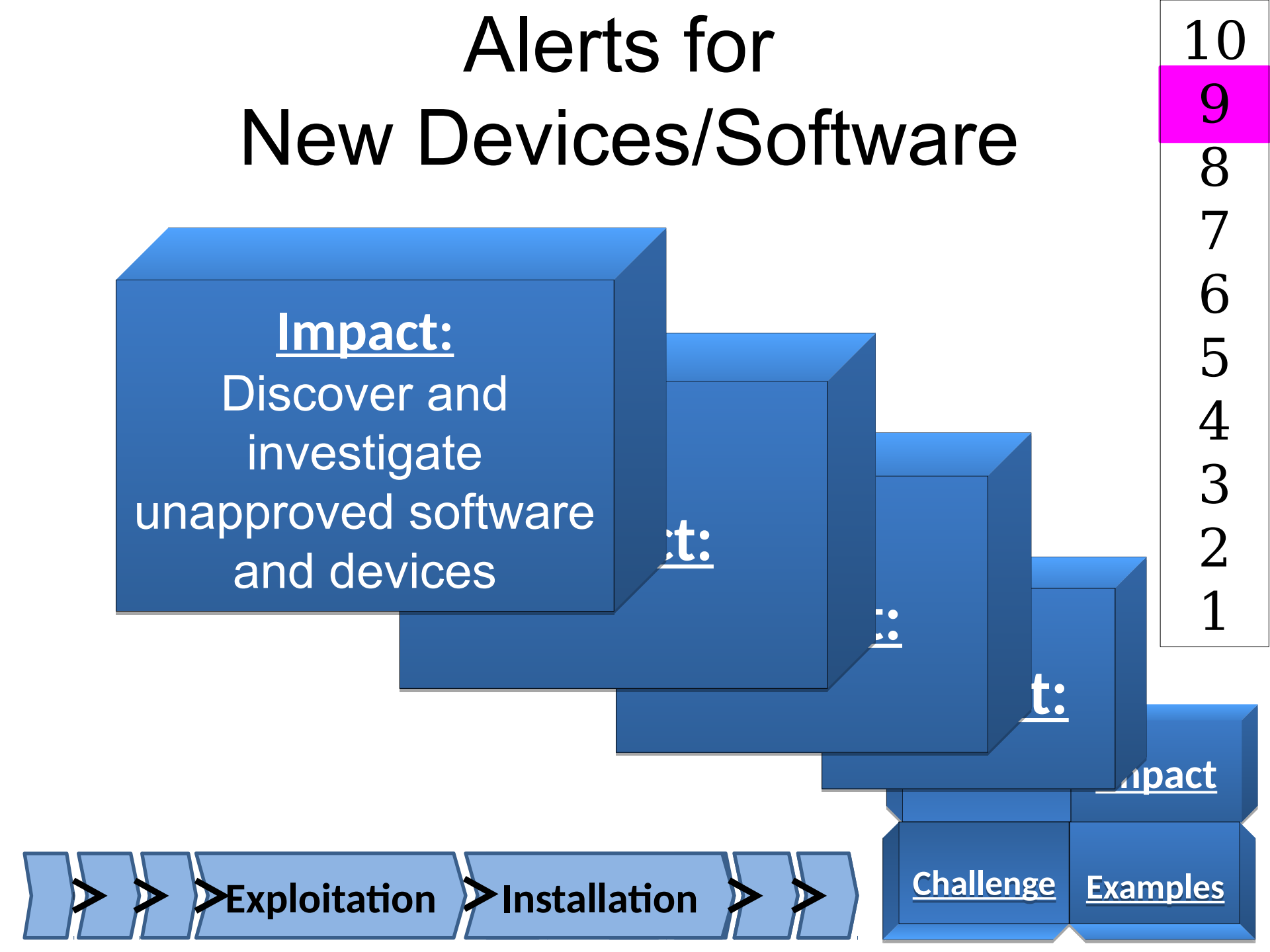
IP	# Times Seen	Date First Seen	Date Last Seen
1.0.0.1	3	26 July 2015	27 July 2015
1.0.0.2	10	20 July 2015	9 Aug 2015
1.0.0.3	1	1 Aug 2015	1 Aug 2015
1.0.0.4	35	5 Aug 2015	11 Aug 2015

10
9
8
7
6
5
4
3
2
1

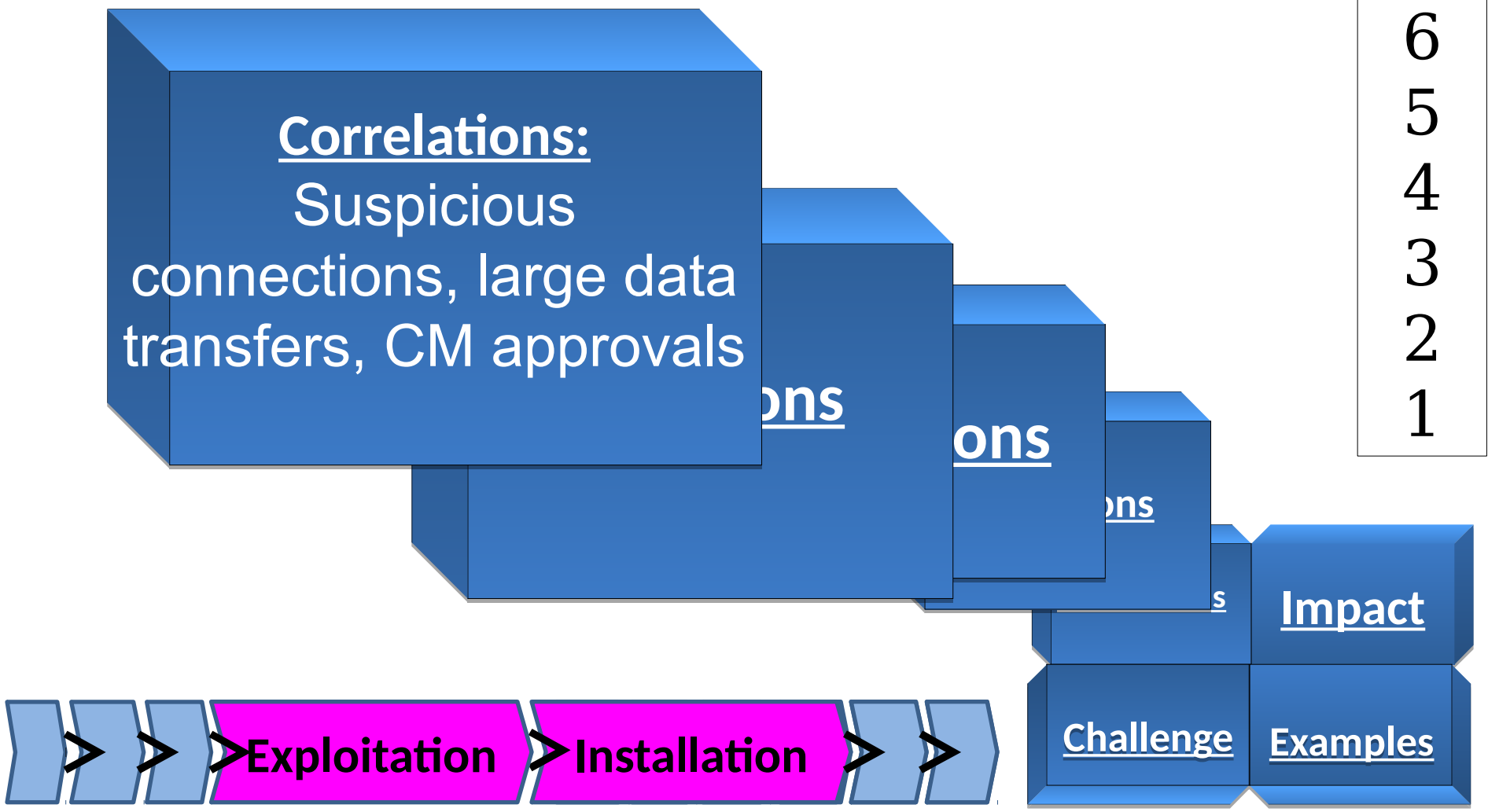




Alerts for New Devices/Software



Alerts for New Devices/Software



Alerts for New Devices/Software

Challenge:
Controlling large and decentralized networks.
Keeping approved list updated

ge:

ge:

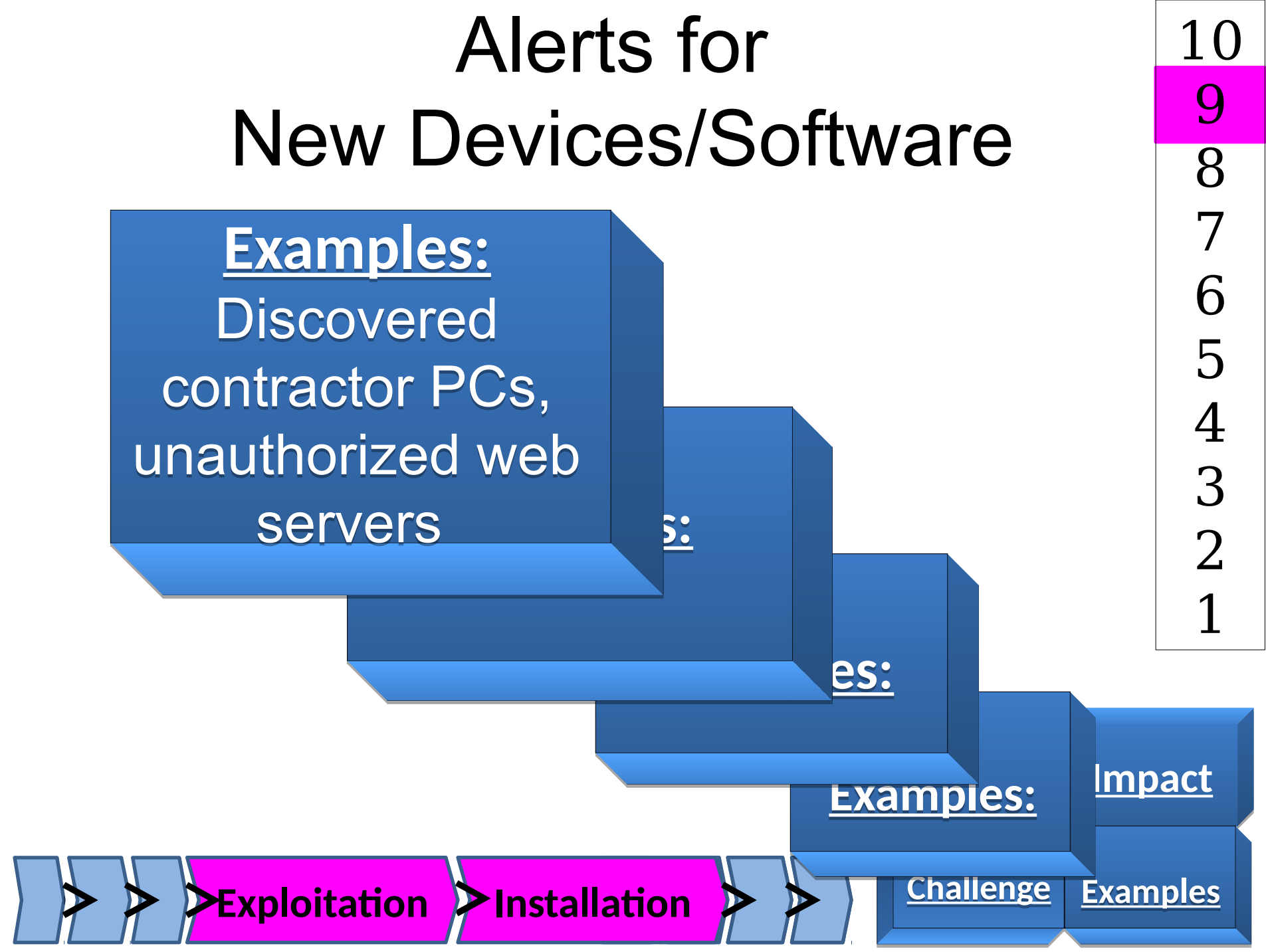
enge:

Impact

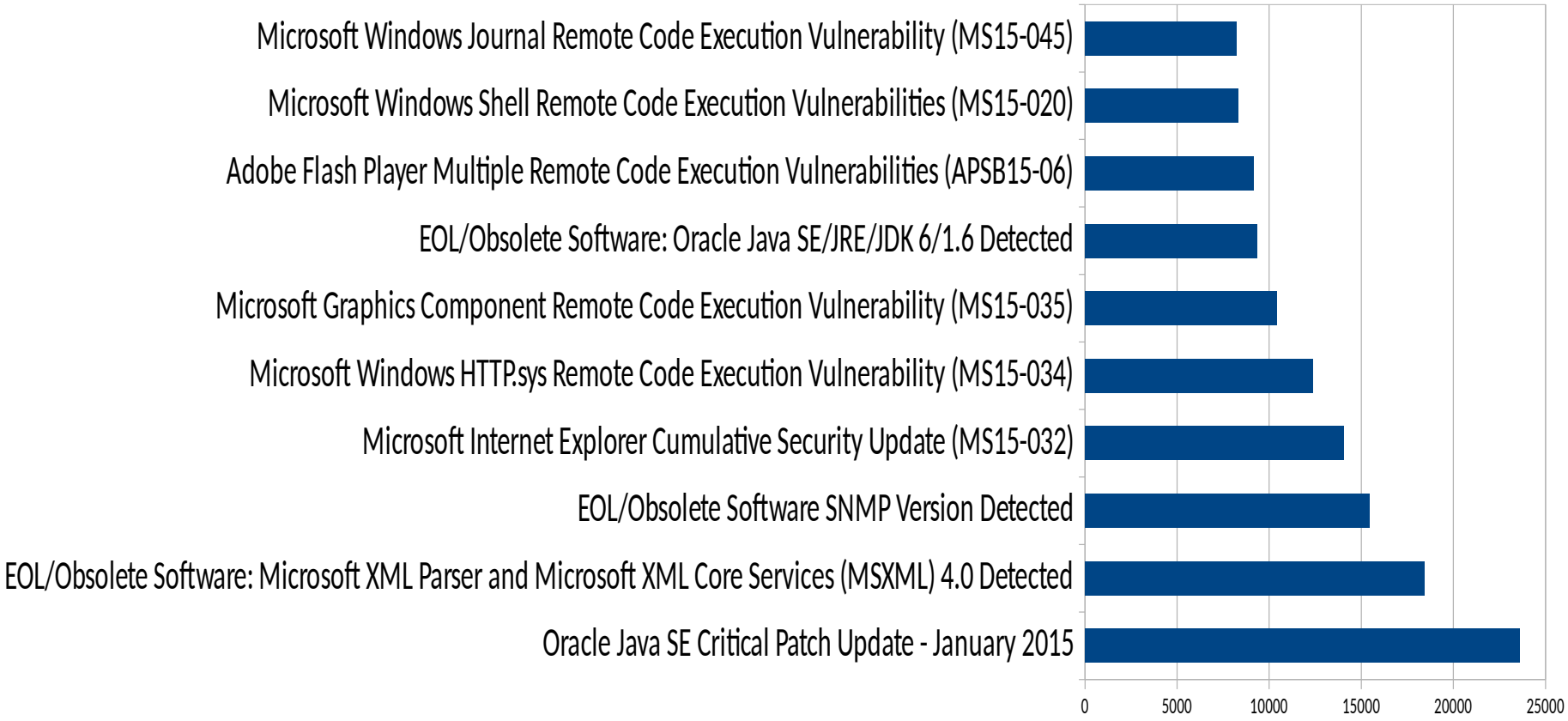
Examples

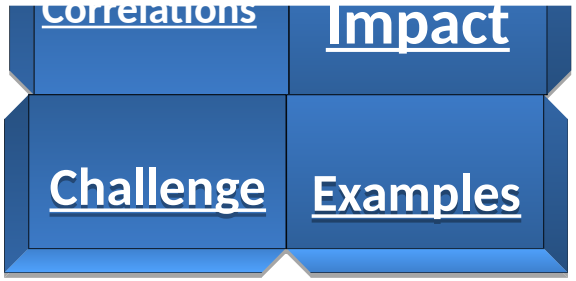
Exploitation > Installation >

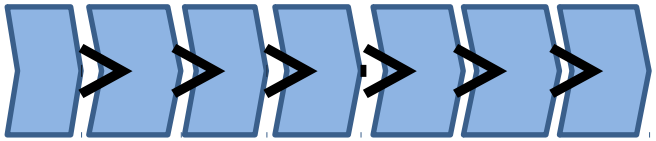
Alerts for New Devices/Software



Vulnerability Statistics







Vulnerability Statistics

Impact:
See the areas of most risk by class of vulnerability

Impact:

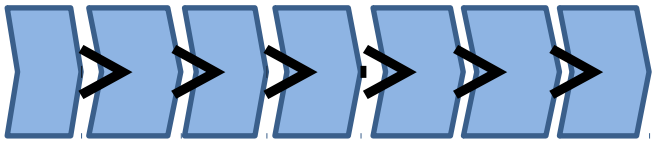
Impact:

Impact:

Impact

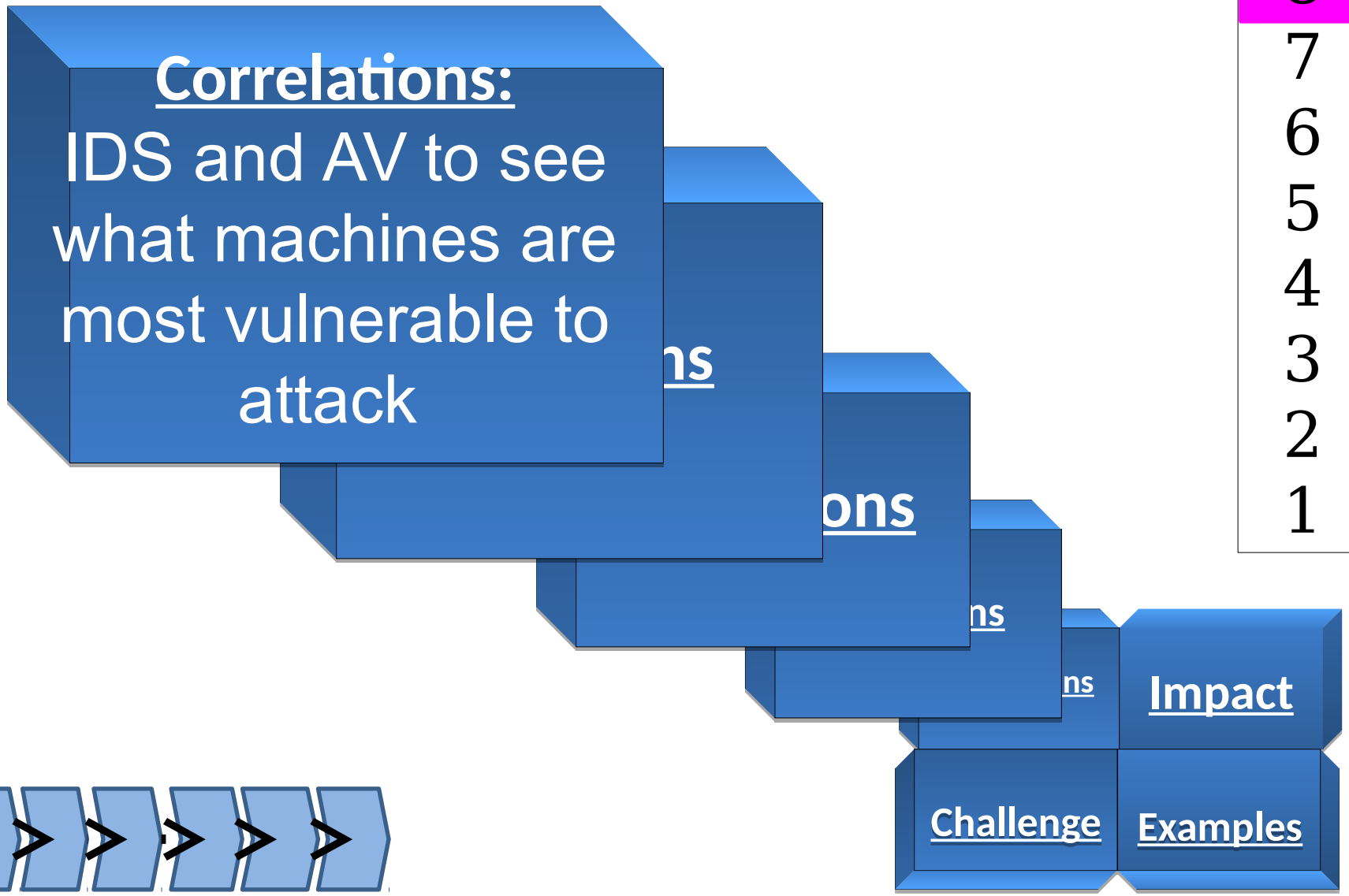
Challenge

Examples



Vulnerability Statistics

Correlations:
IDS and AV to see what machines are most vulnerable to attack



Vulnerability Statistics

Challenge:
Eliminating false positives, determining vulnerability mitigations

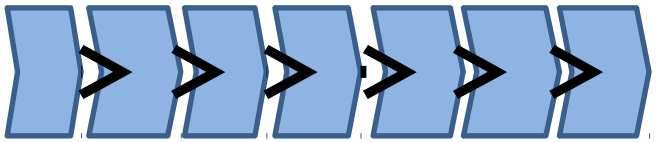
ge:

nge:

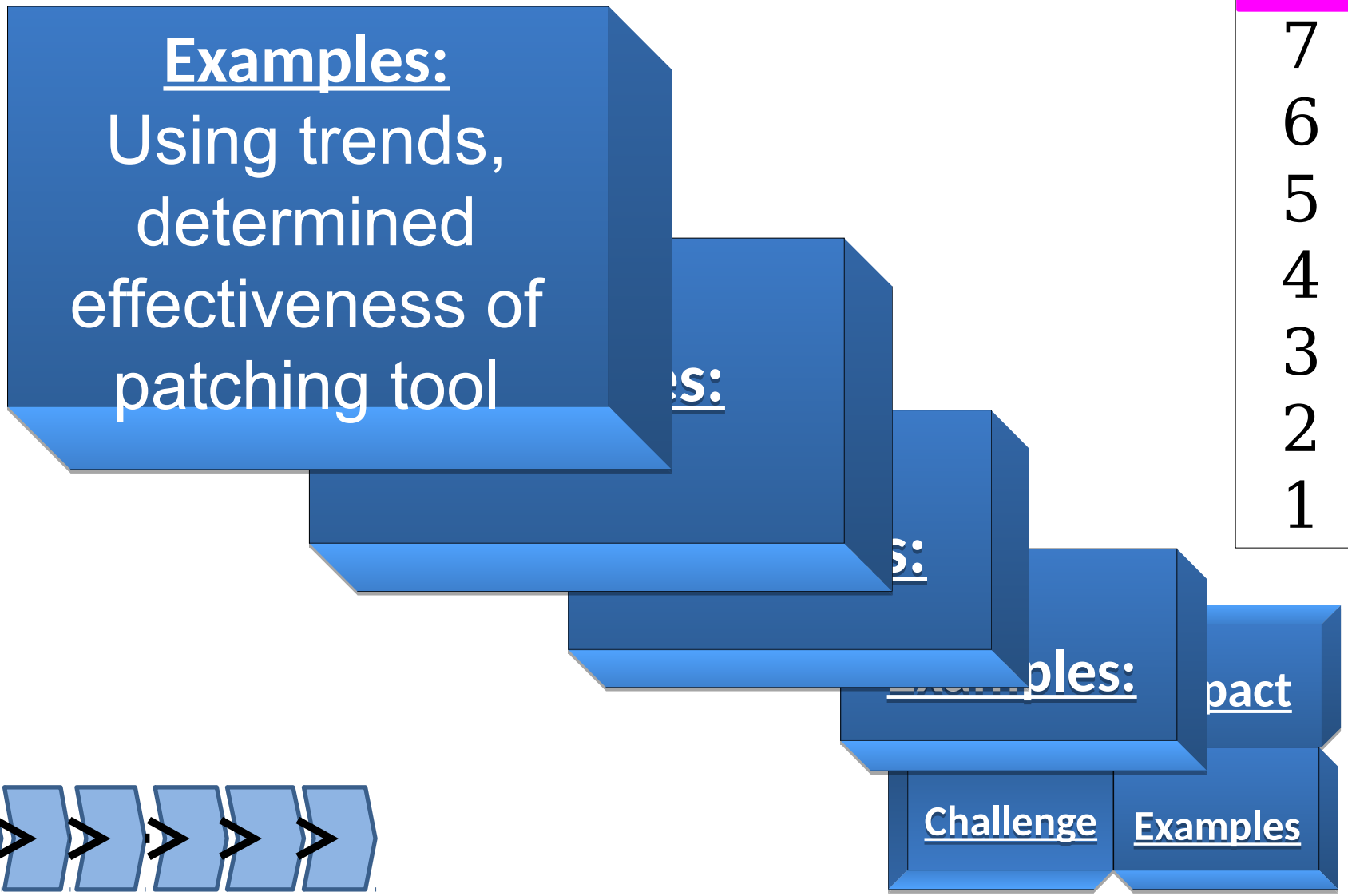
nge:

Impact

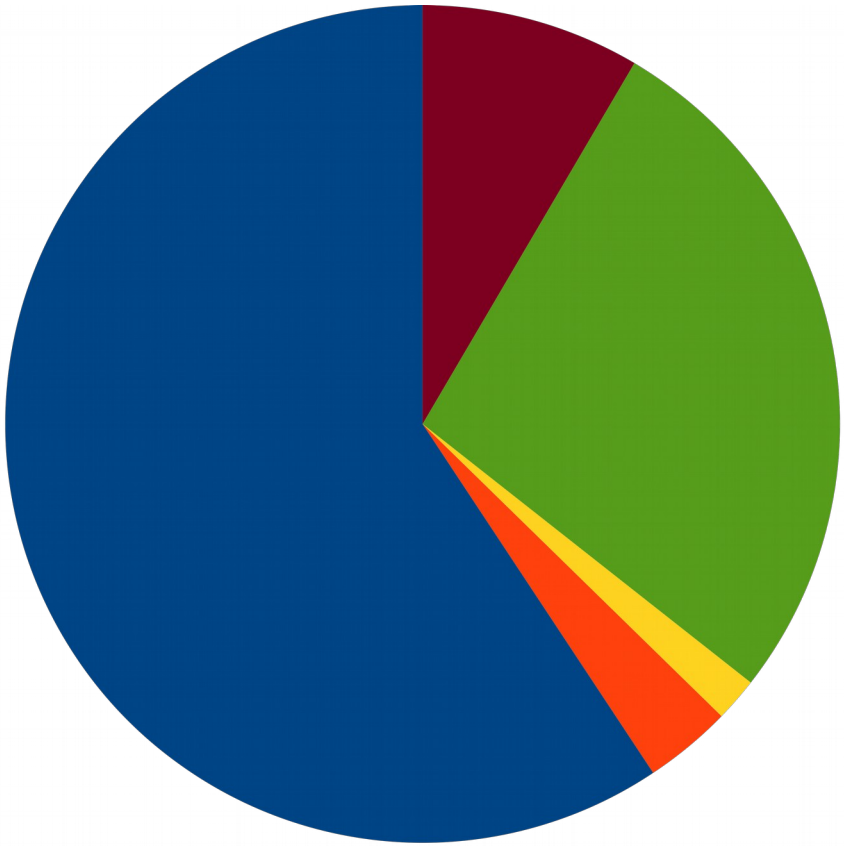
Examples



Vulnerability Statistics



Top AV/HIPS Alerts



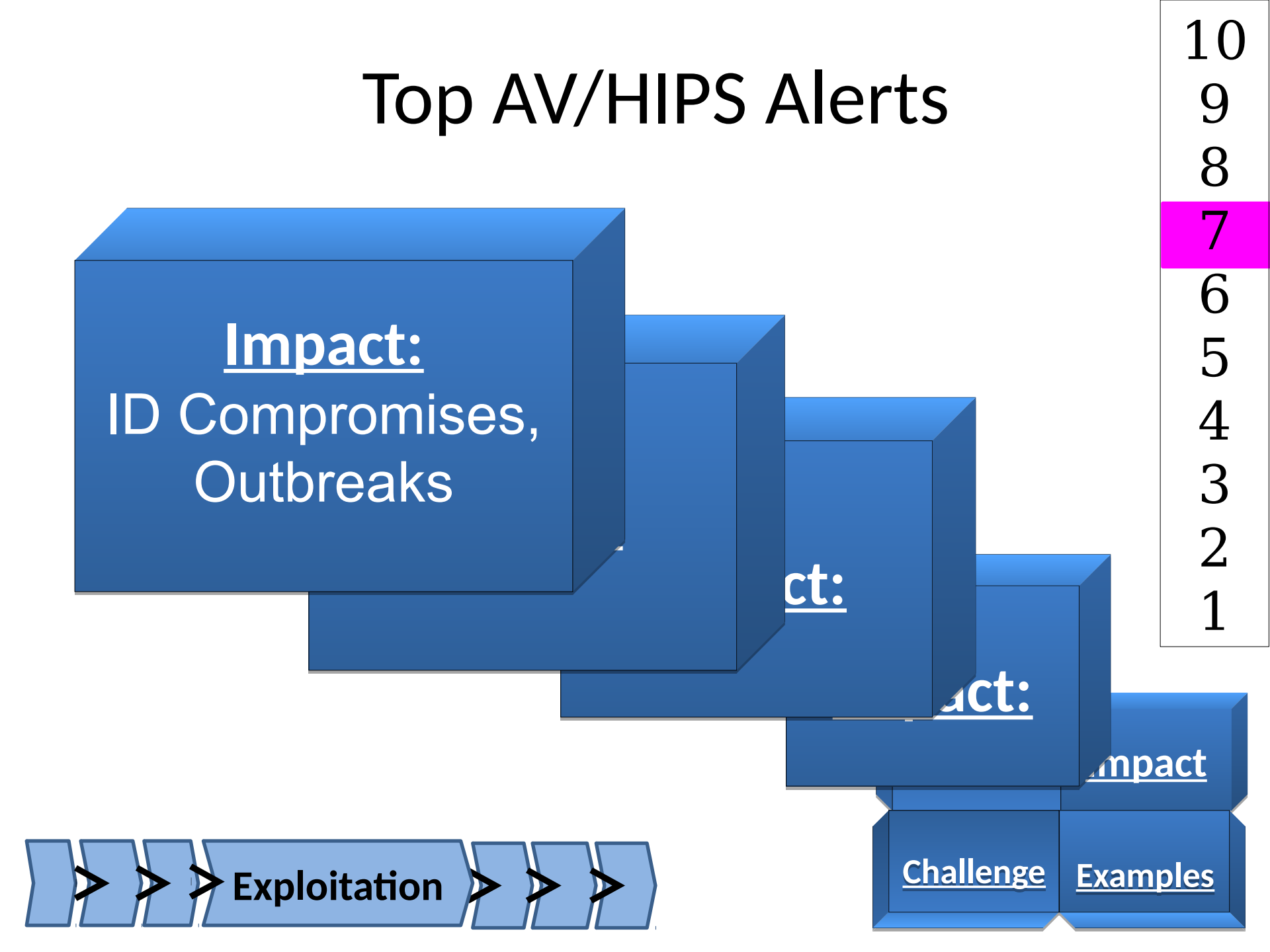
Today – 1 week

- Port Scan Detected
- Conficker
- MyDoom
- PoisonIvy
- I Love You

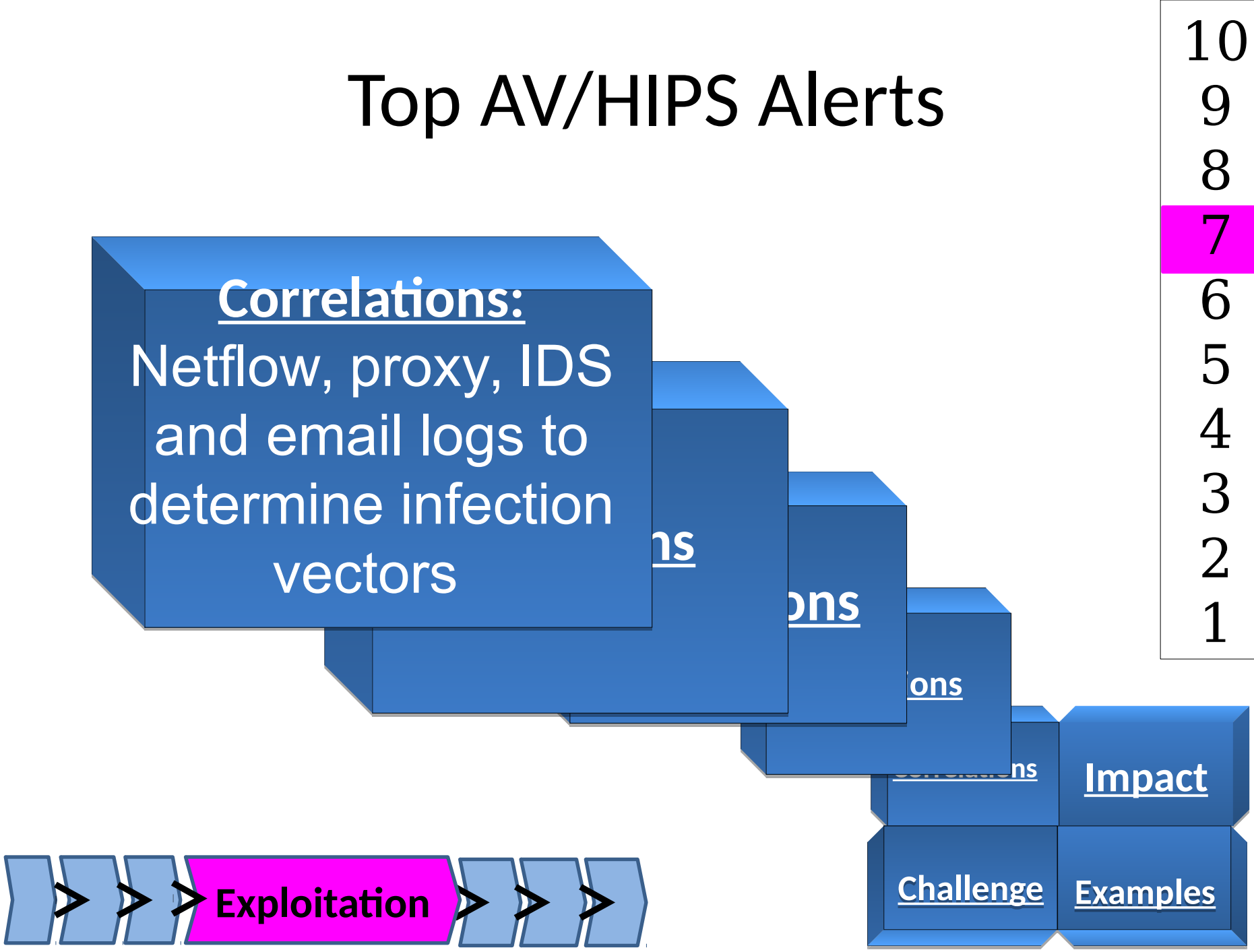
10
9
8
7
6
5
4
3
2
1

Challenge Examples

Top AV/HIPS Alerts



Top AV/HIPS Alerts



Top AV/HIPS Alerts

10
9
8
7
6
5
4
3
2
1

Challenge:
False positives, updating signatures, ineffectiveness of AV

Challenge:

Challenge:

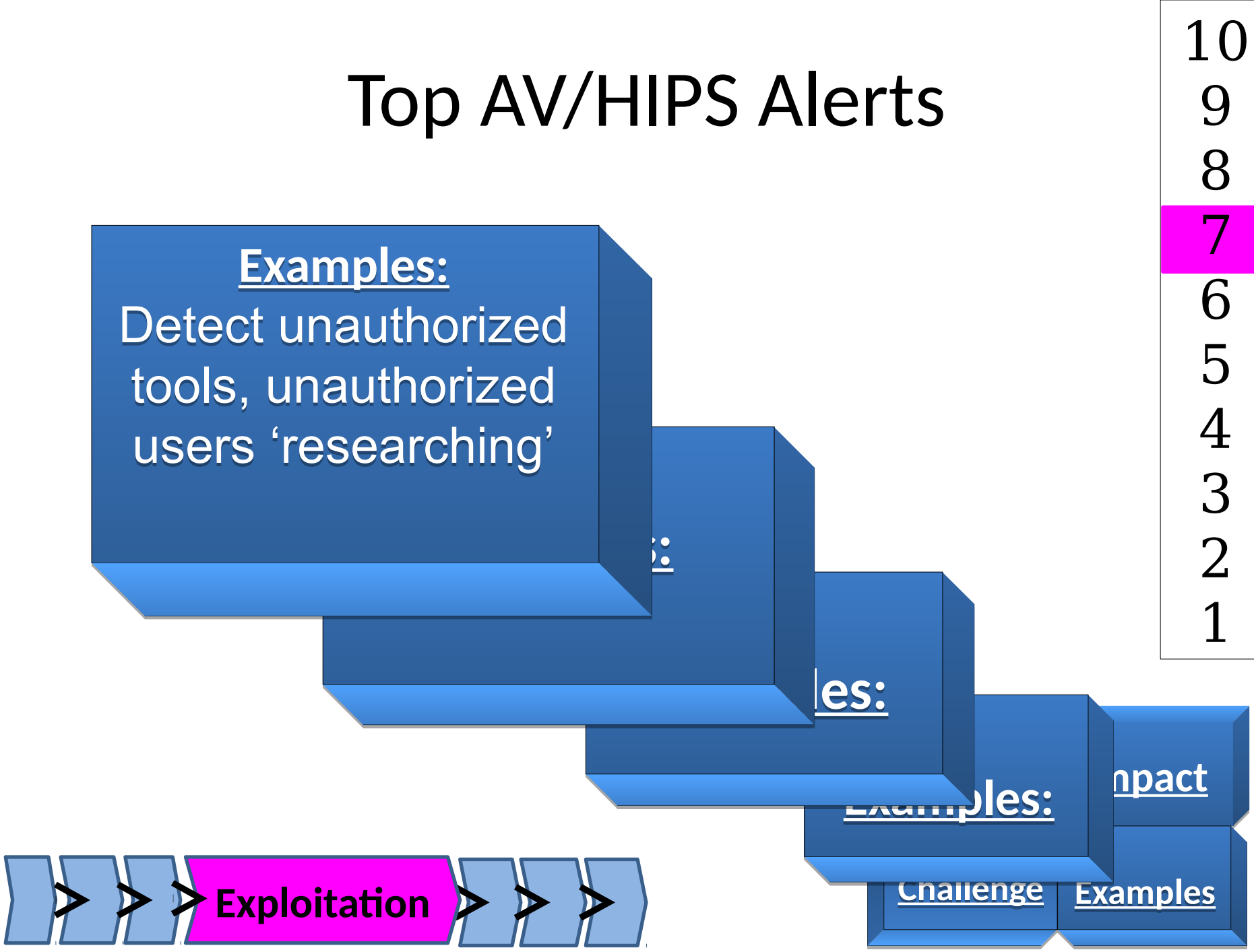
Challenge:

Impact

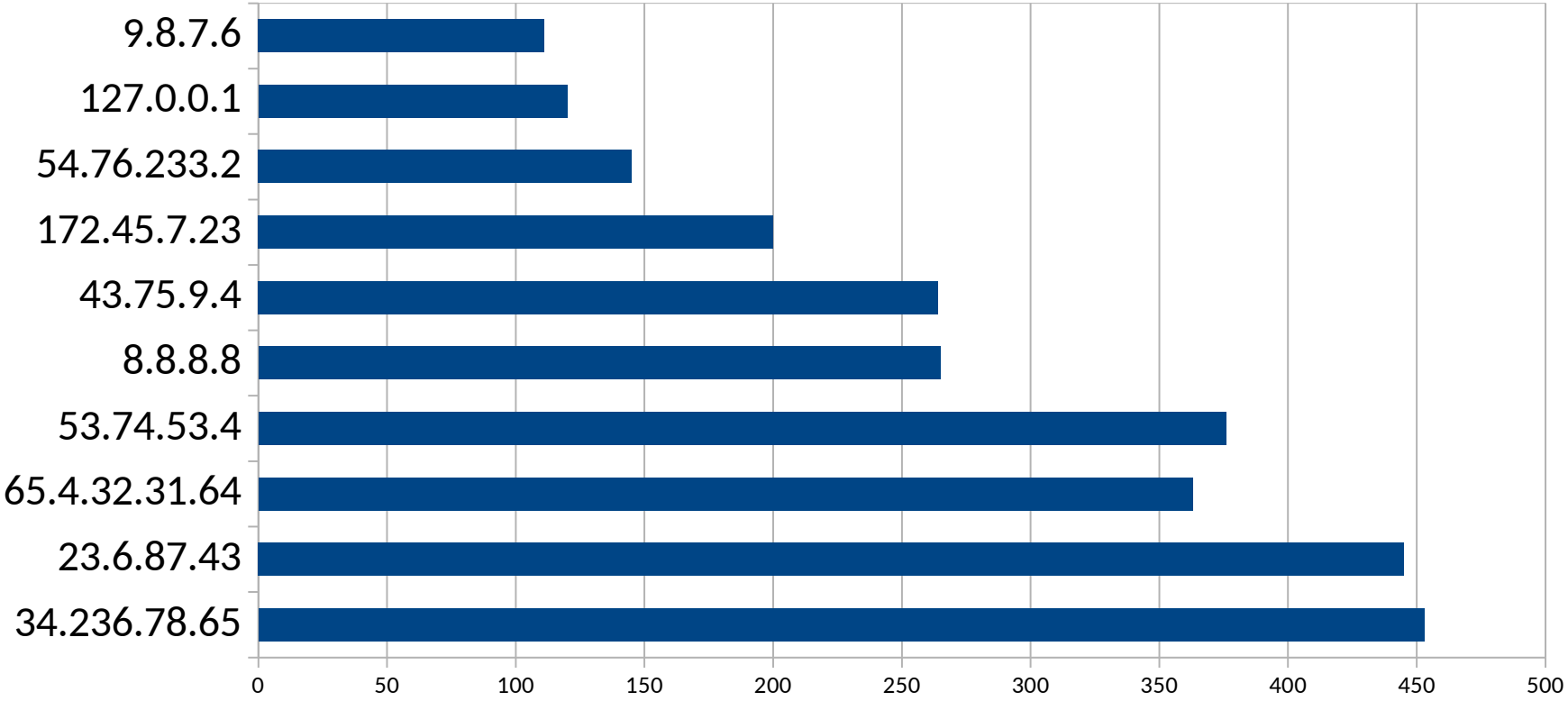
Examples

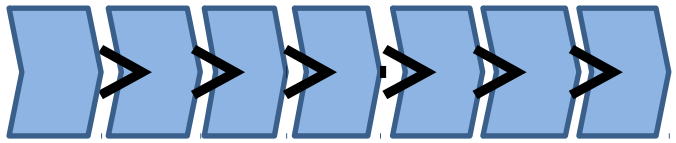
Exploitation

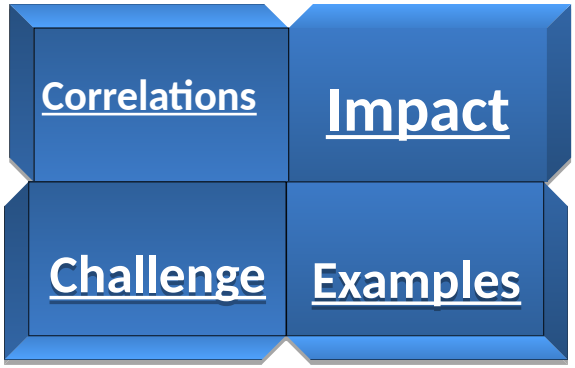
Top AV/HIPS Alerts



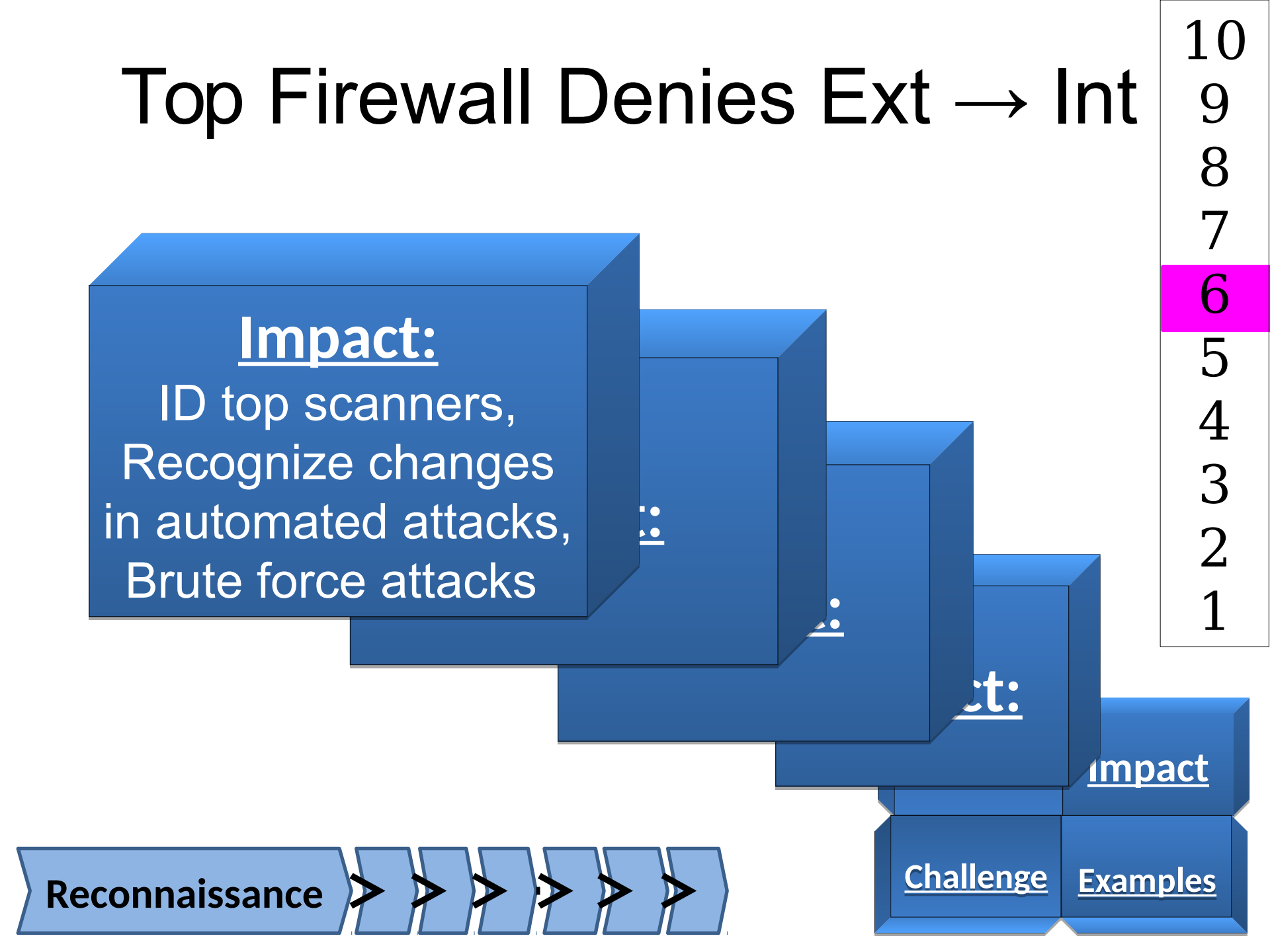
Top Firewall Denies Ext → Int



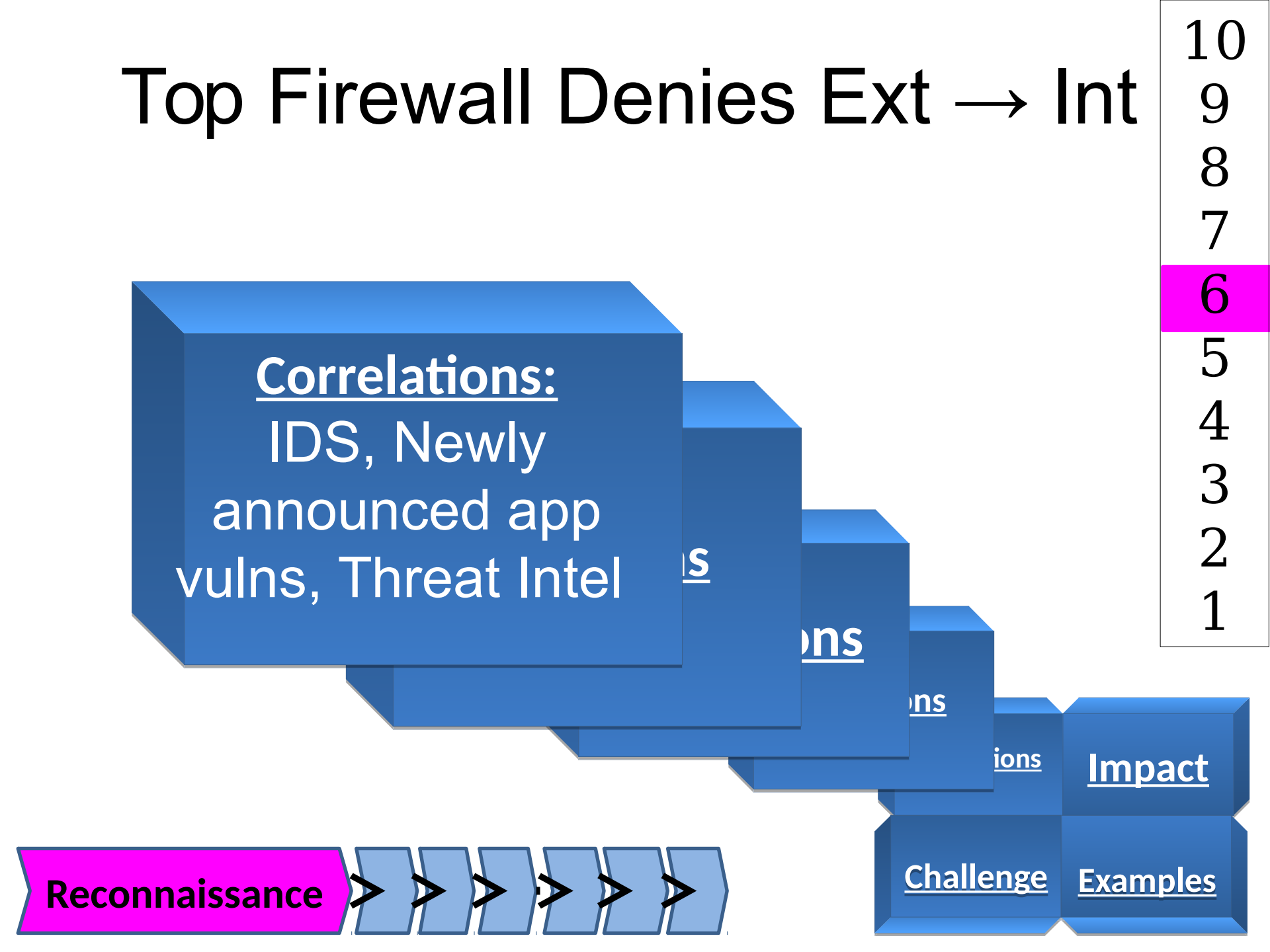




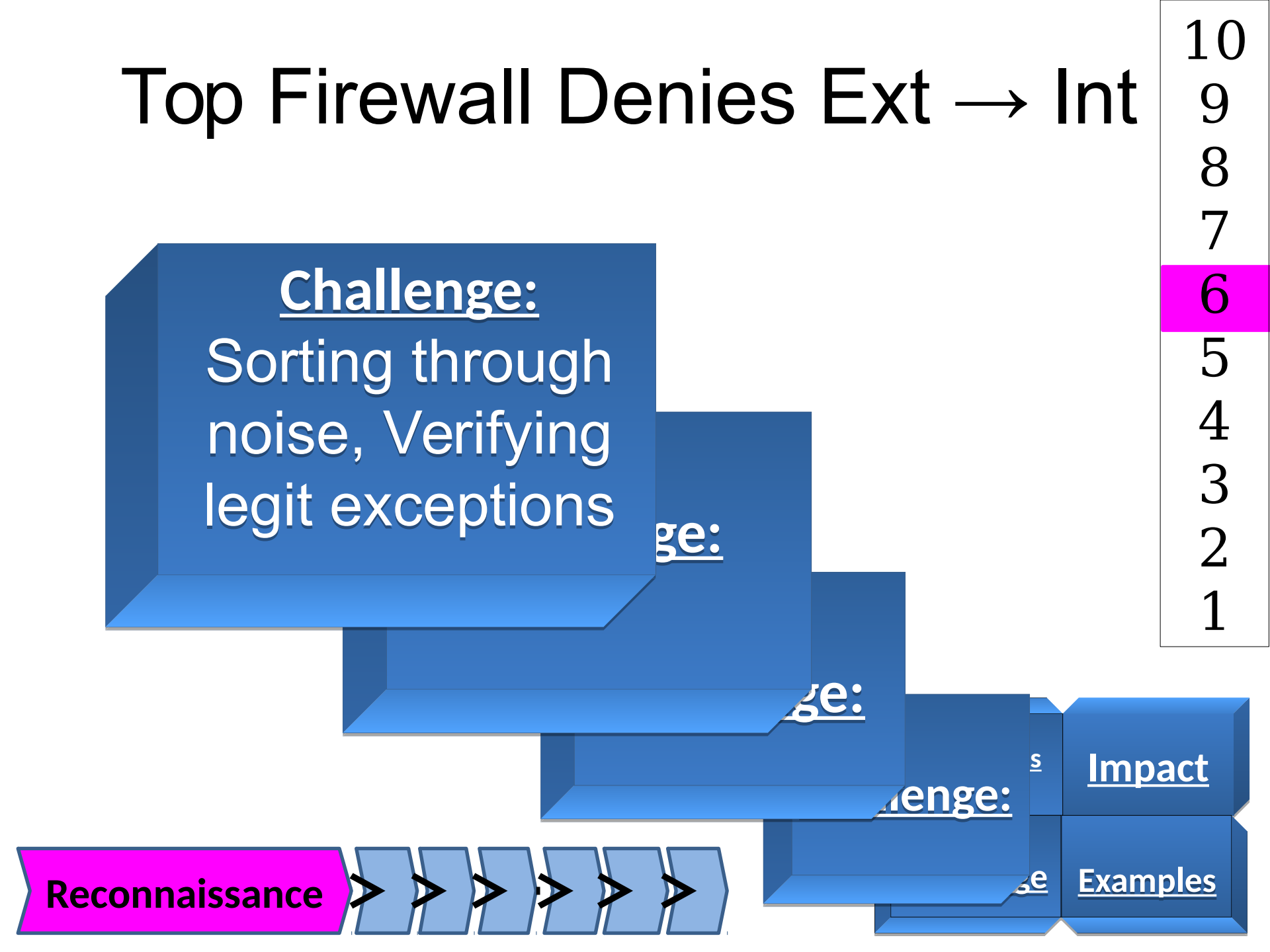
Top Firewall Denies Ext → Int



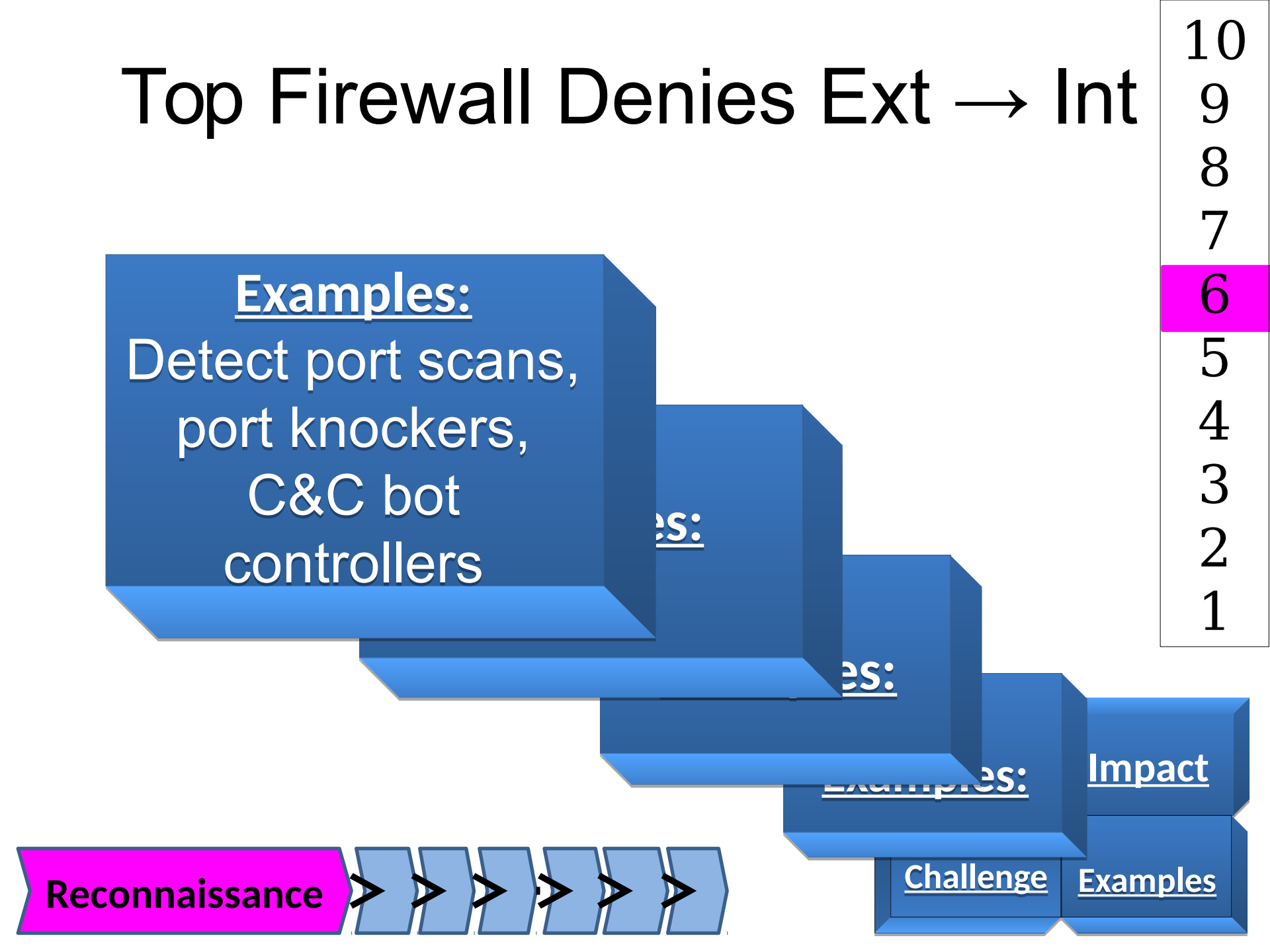
Top Firewall Denies Ext → Int



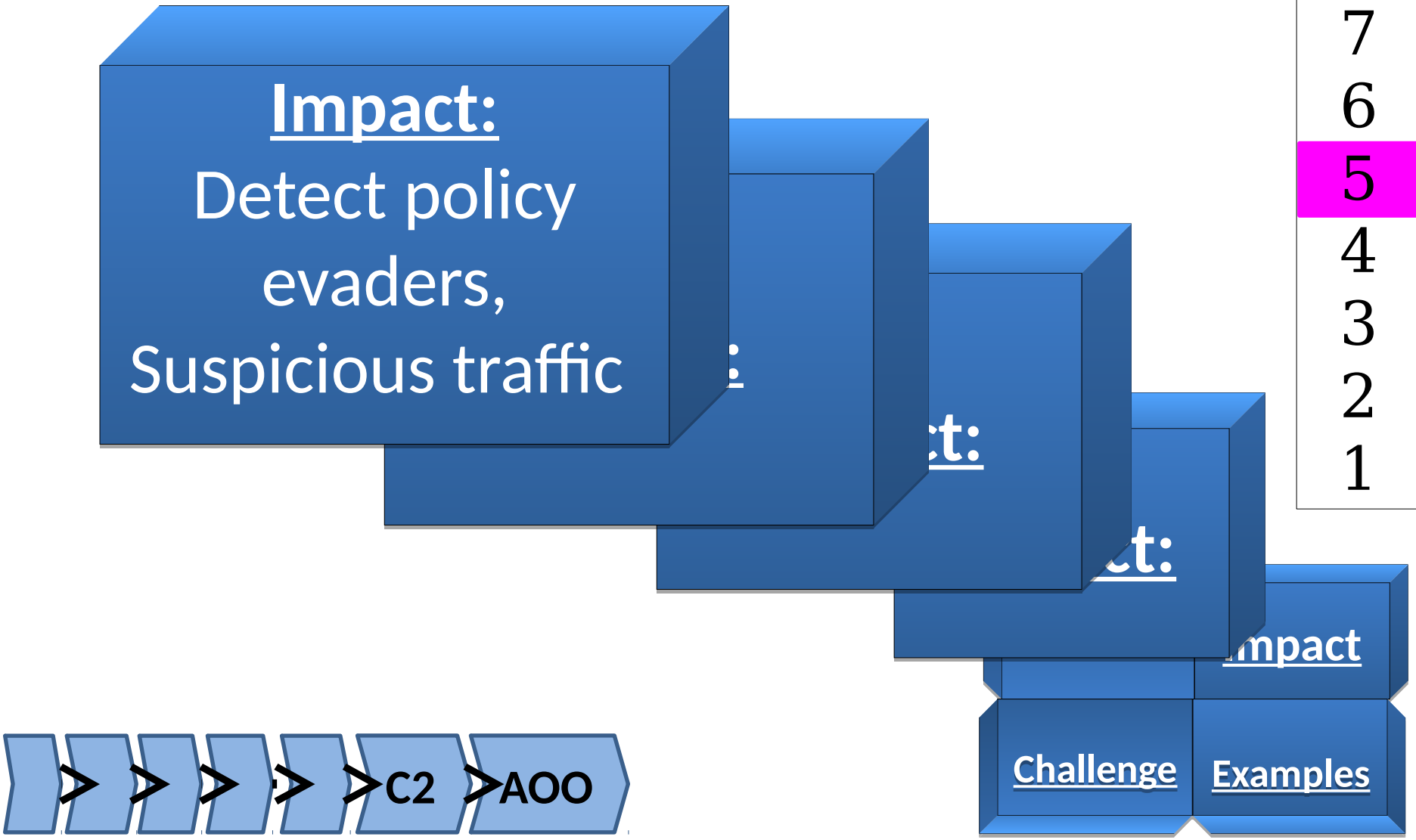
Top Firewall Denies Ext → Int



Top Firewall Denies Ext → Int

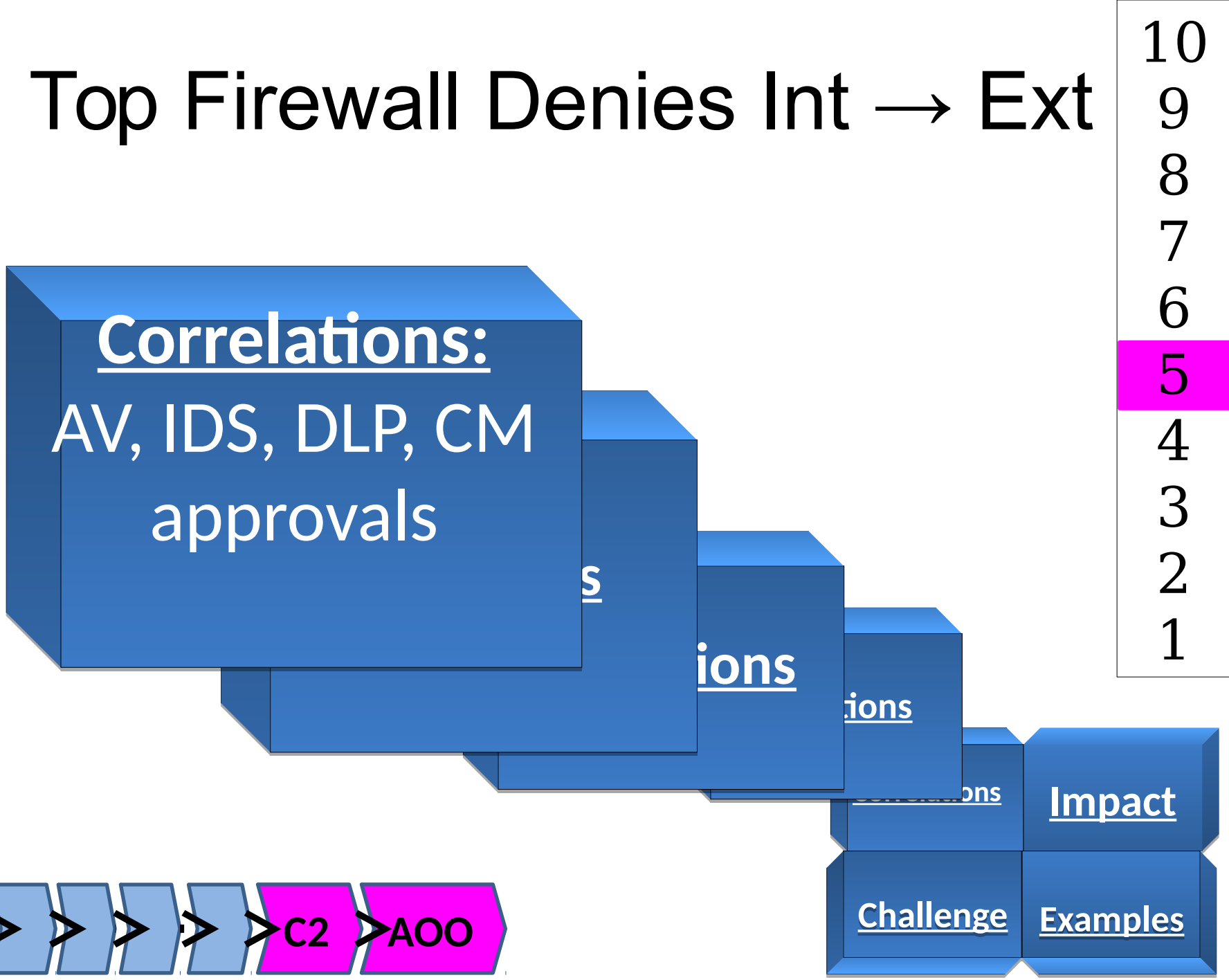


Top Firewall Denies Int → Ext

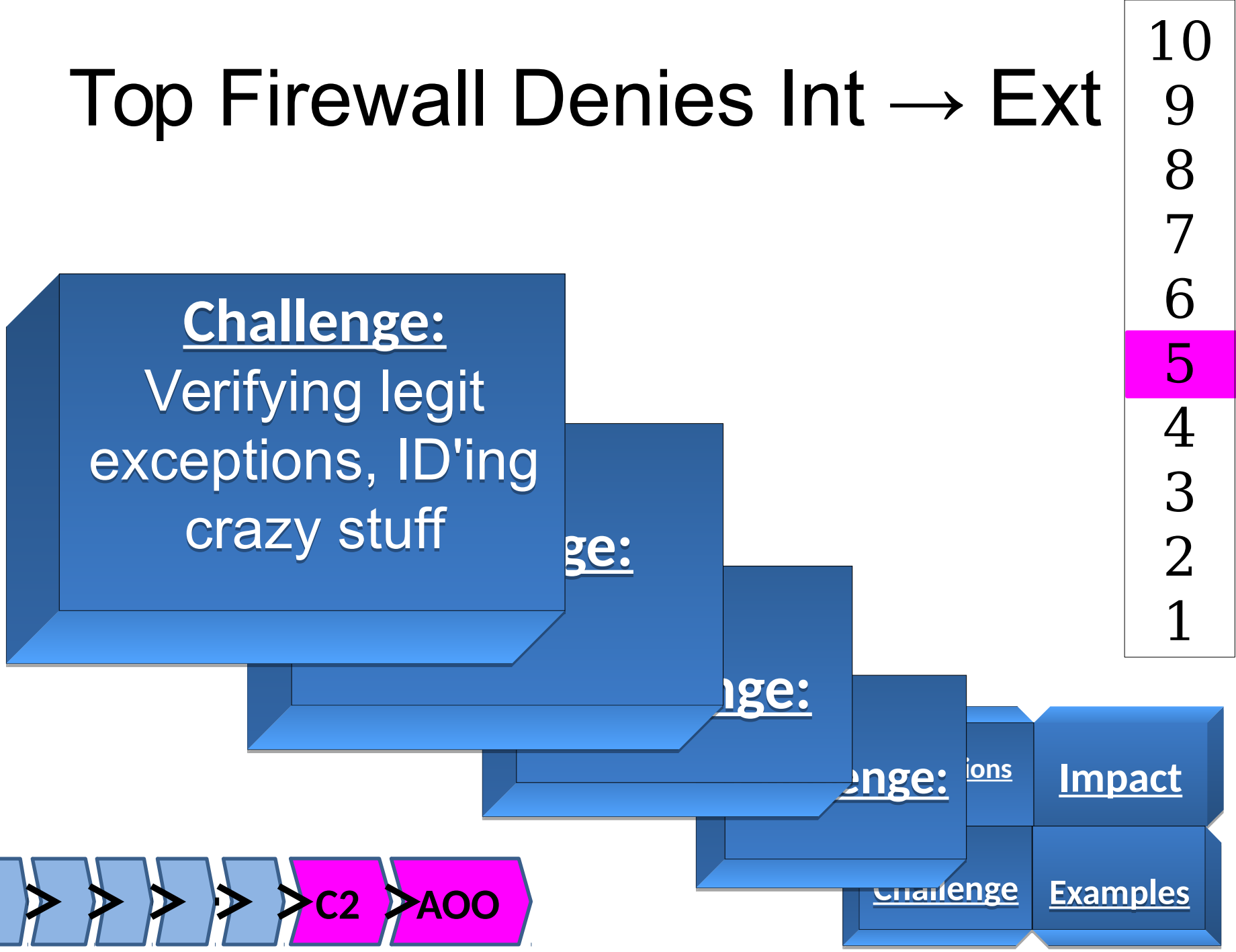


10
9
8
7
6
5
4
3
2
1

Top Firewall Denies Int → Ext



Top Firewall Denies Int → Ext



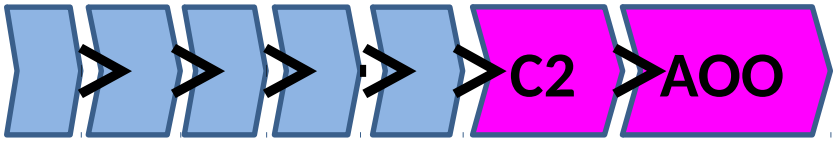
Top Firewall Denies Int → Ext

10
9
8
7
6
5
4
3
2
1

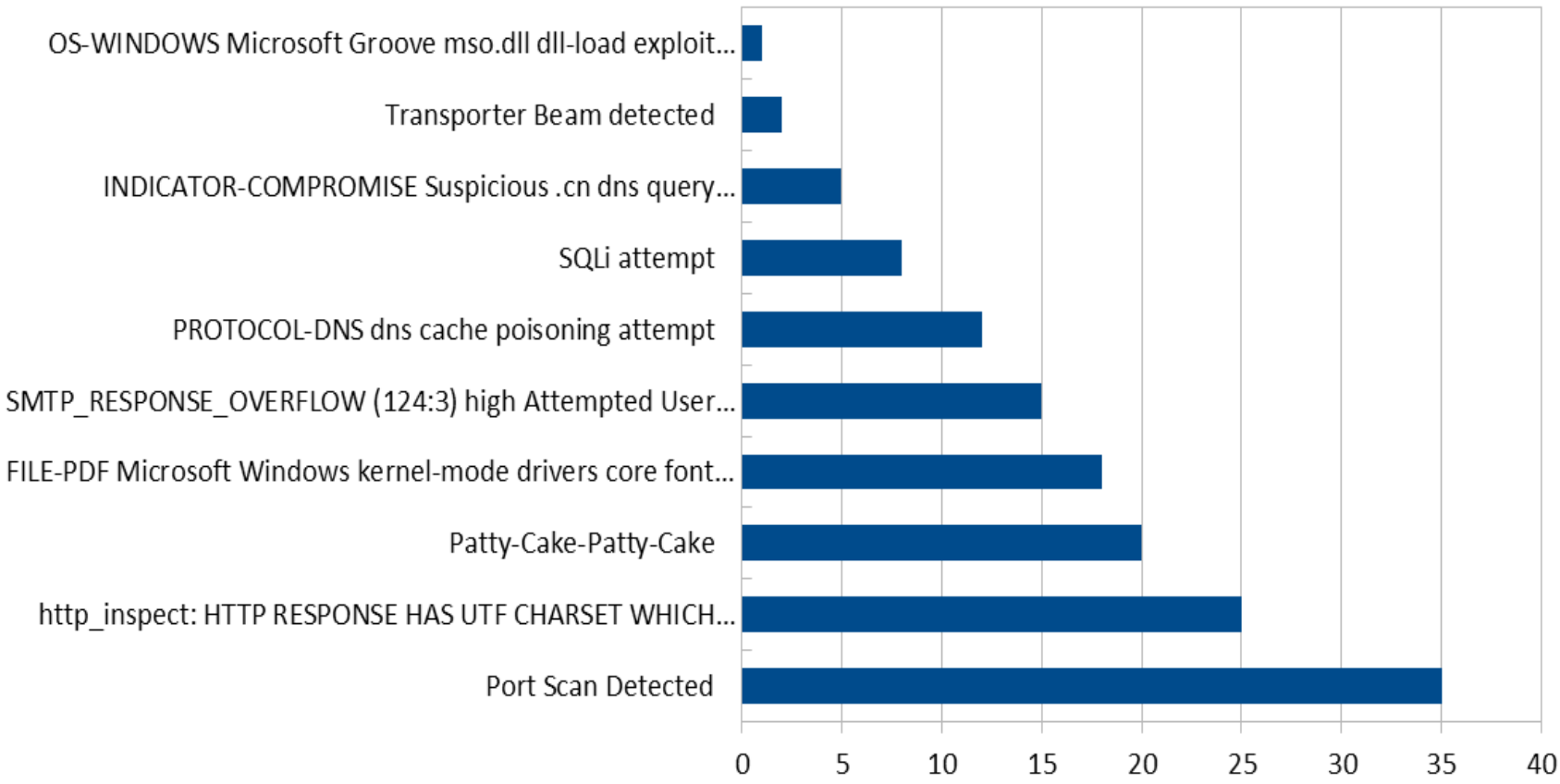
Examples:
Vendors who don't allow their "call home" to be disabled

Impact

Challenge **Examples**



Top IDS Alerts Ext → Int



10
9
8
7
6
5
4
3
2
1

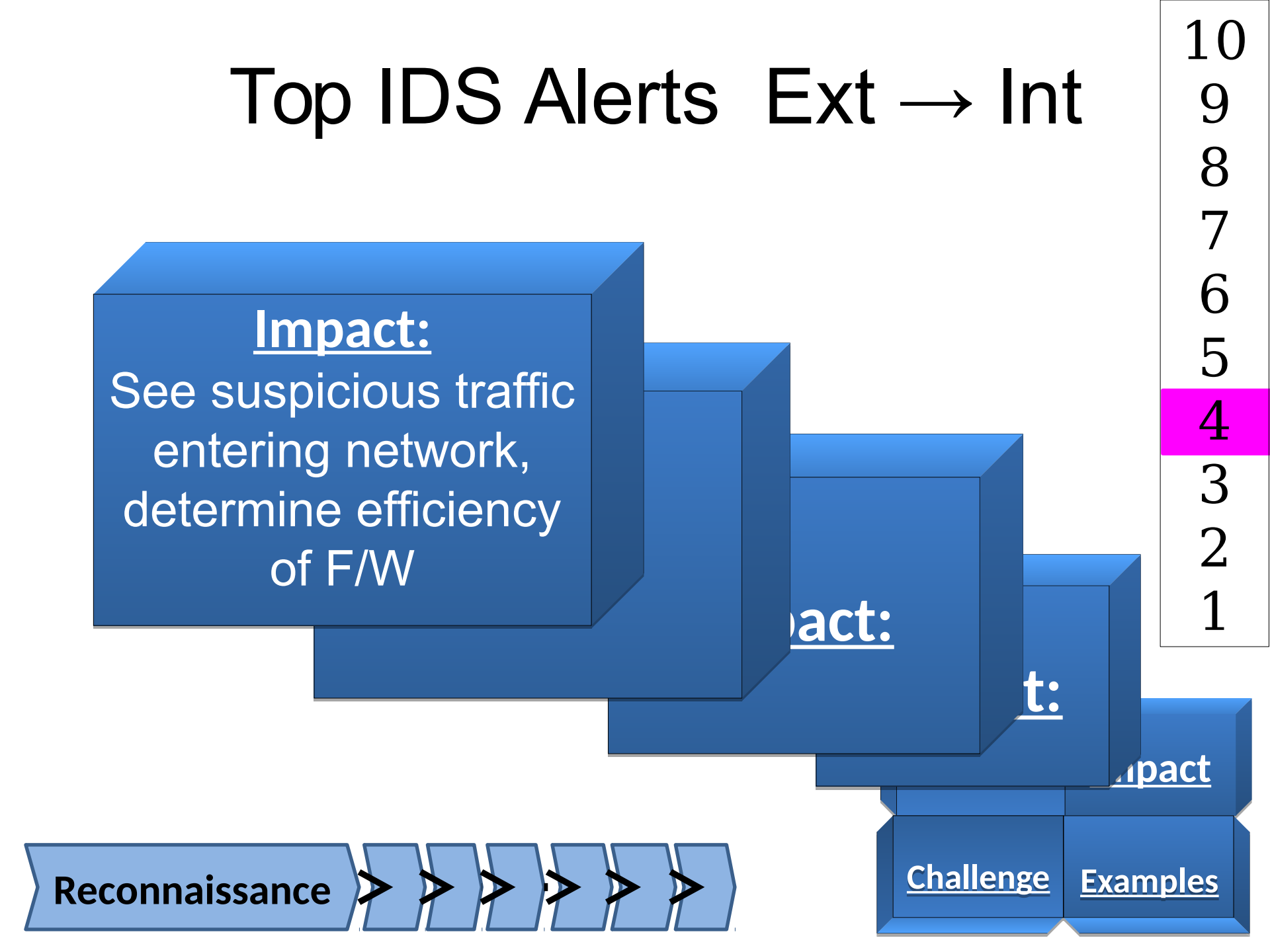
Correlations

Impact

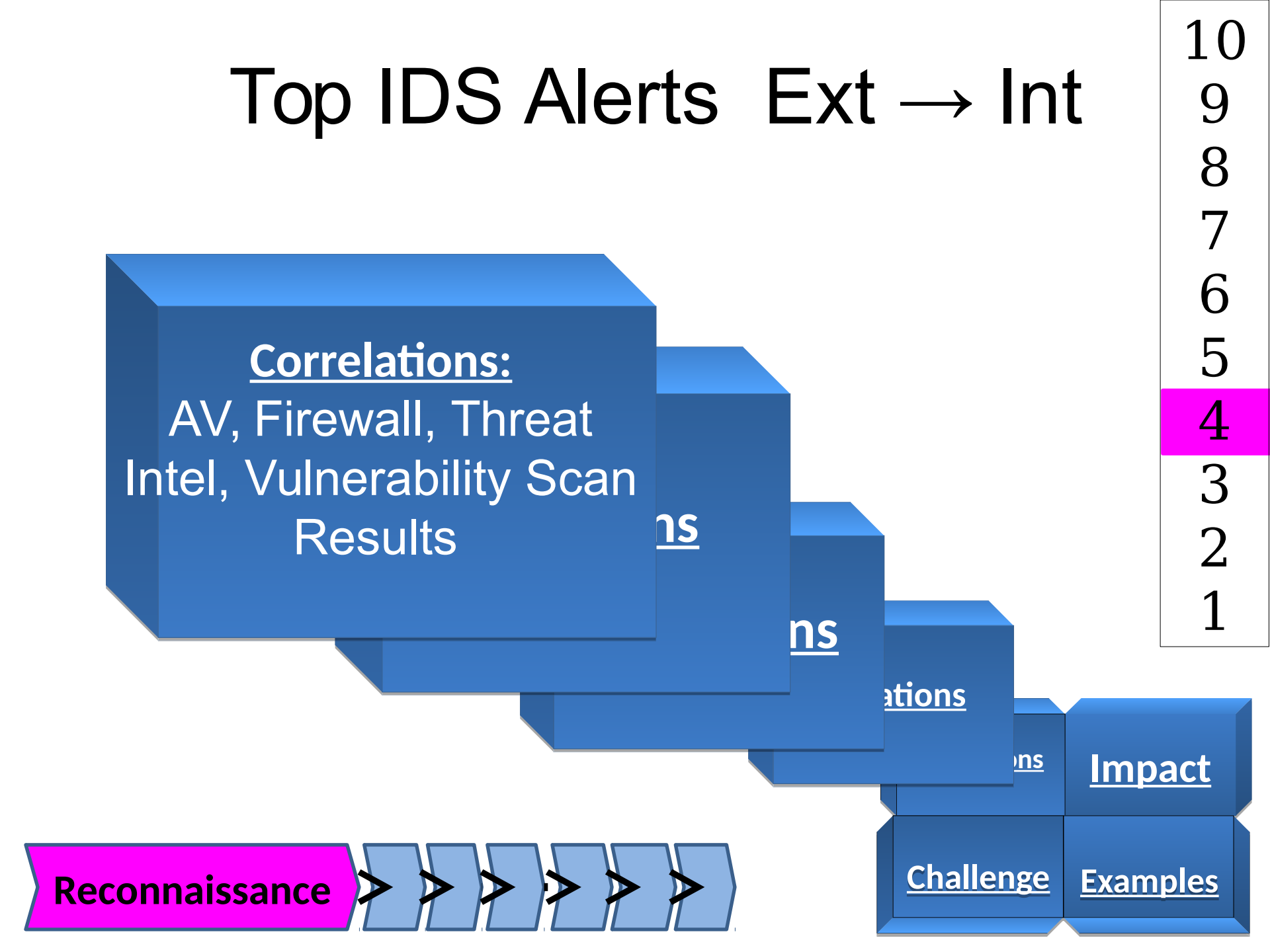
Challenge

Examples

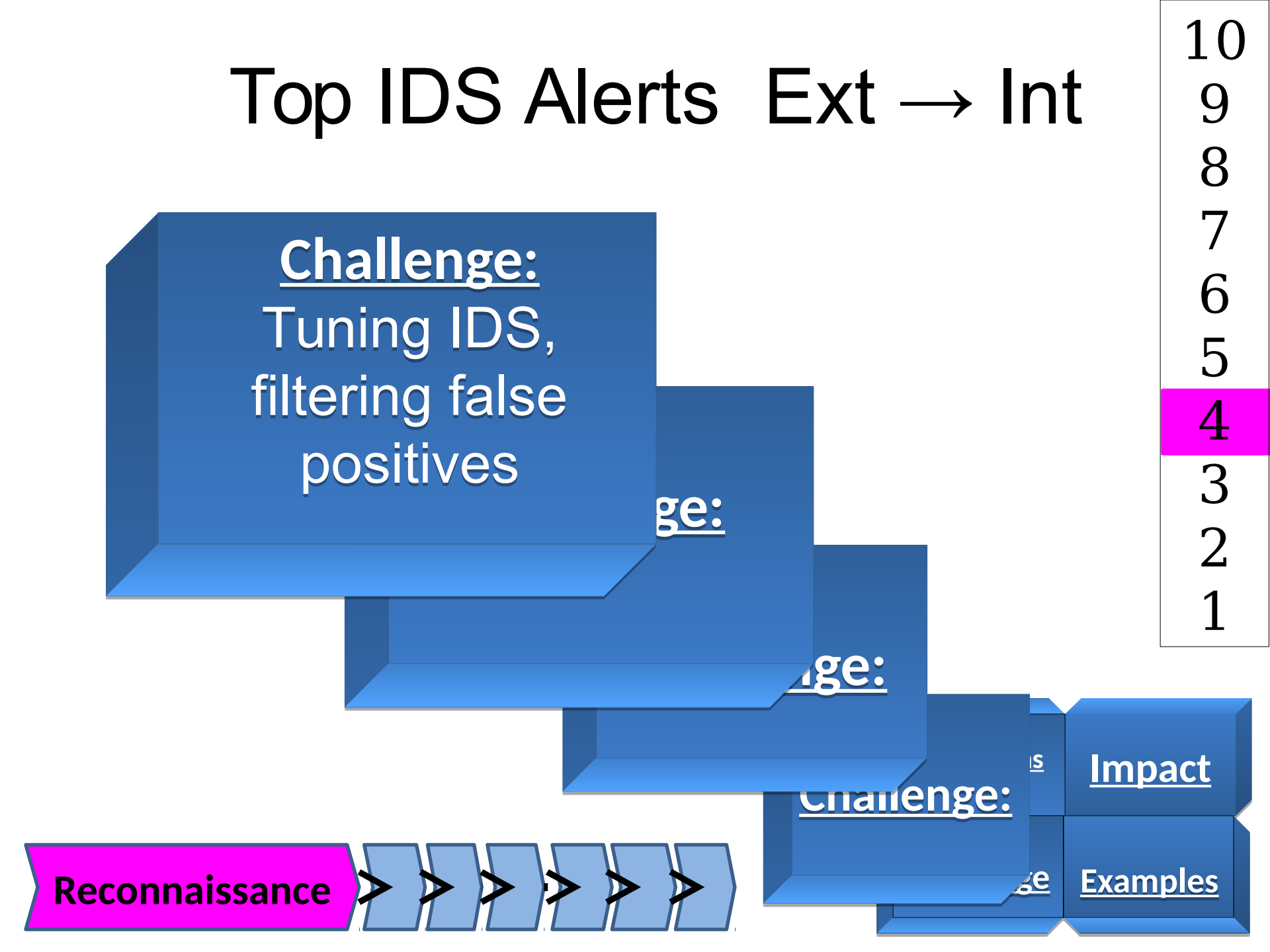
Top IDS Alerts Ext → Int



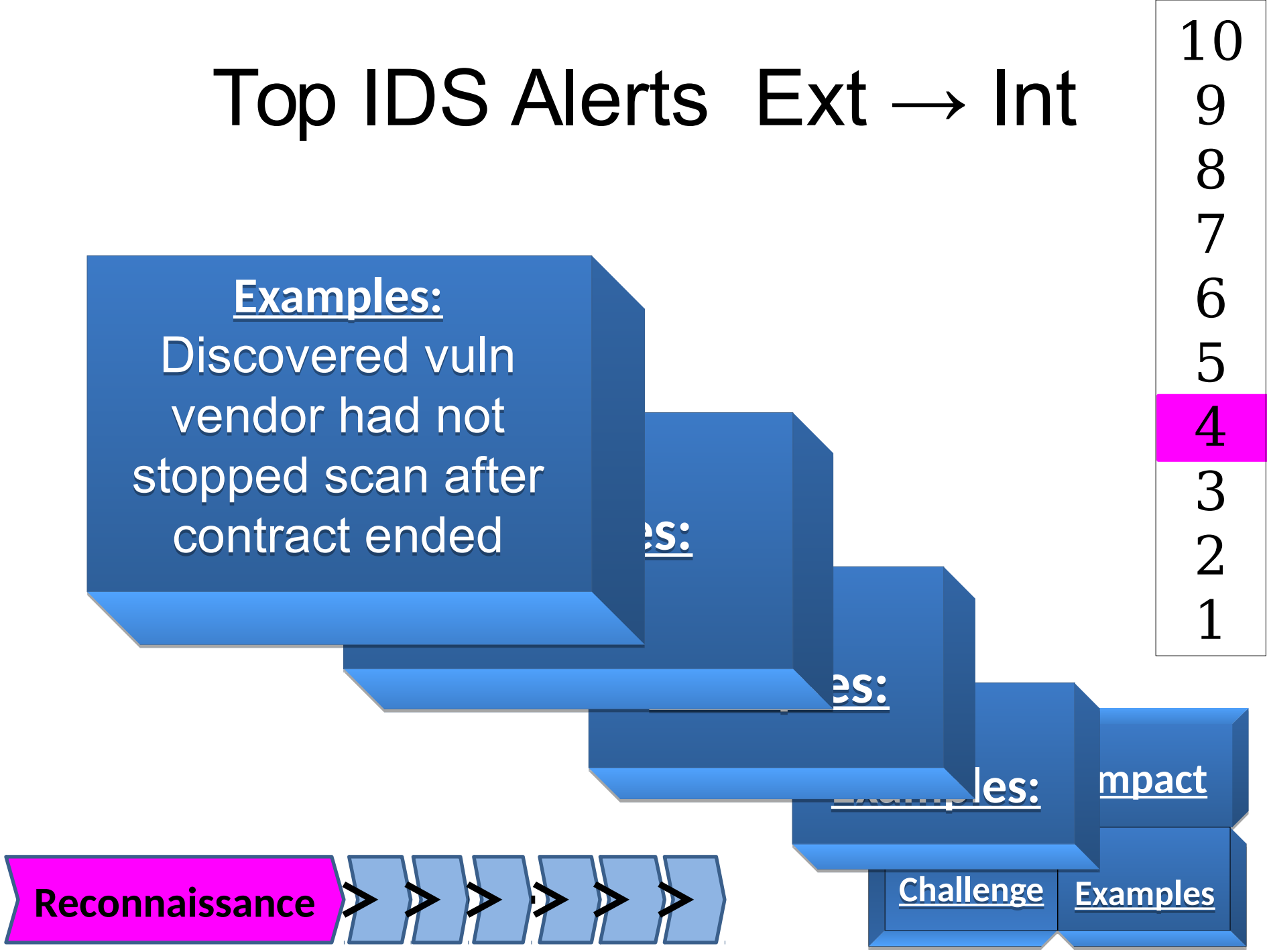
Top IDS Alerts Ext → Int



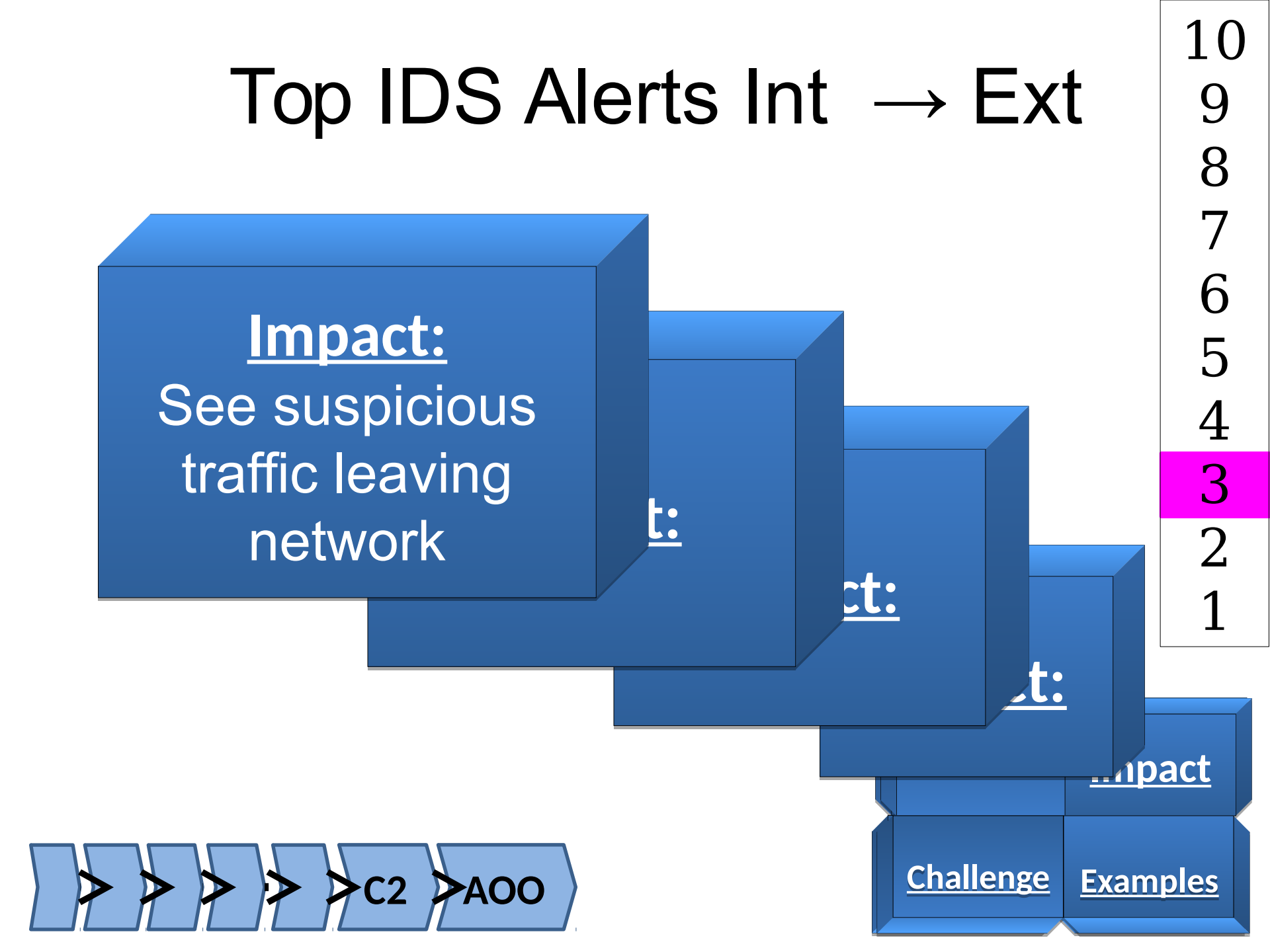
Top IDS Alerts Ext → Int



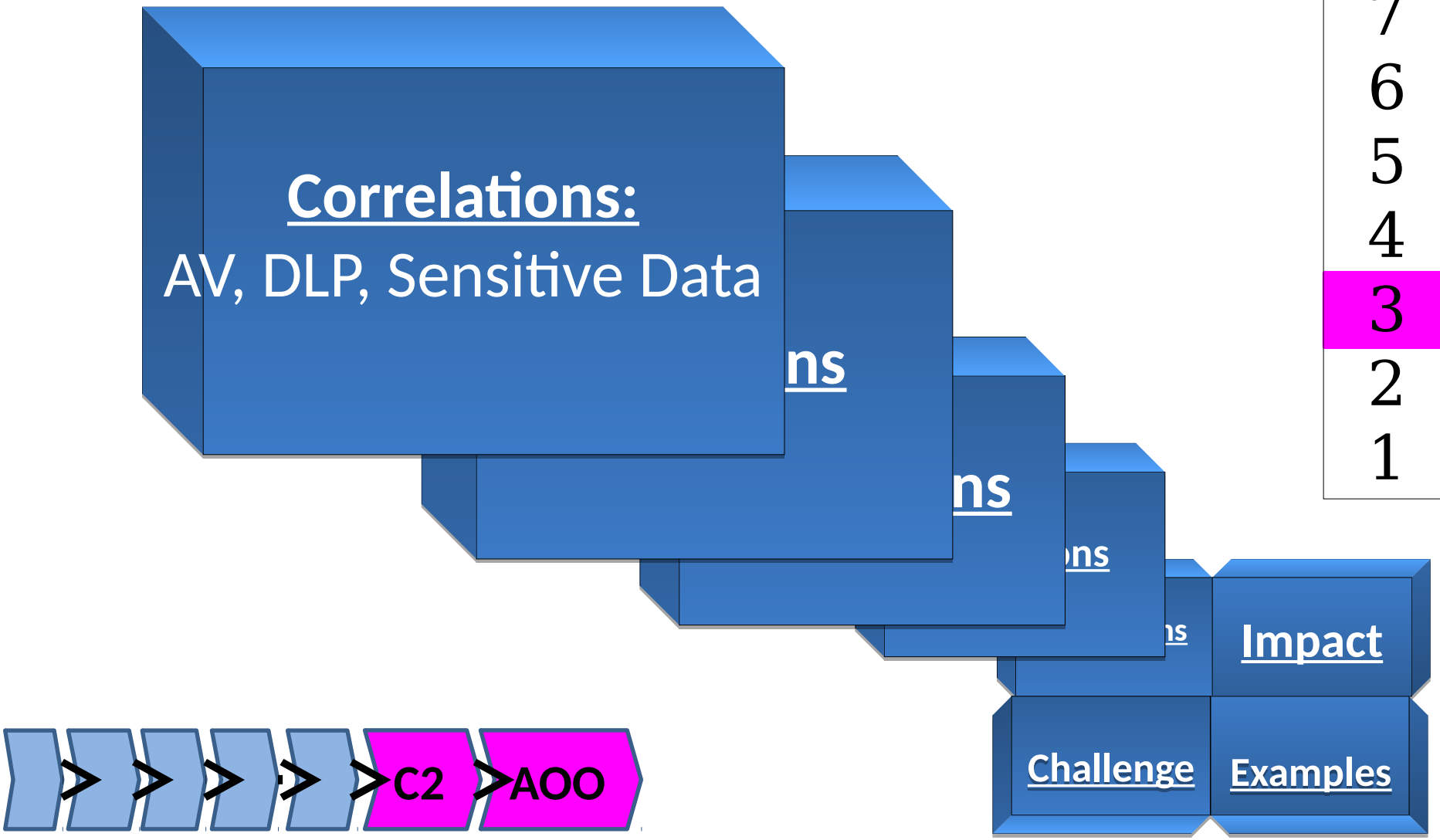
Top IDS Alerts Ext → Int



Top IDS Alerts Int → Ext



Top IDS Alerts Int → Ext



10
9
8
7
6
5
4
3
2
1

Top IDS Alerts Int → Ext

Challenge:
Tuning IDS, filtering false positives

ge:

nge:

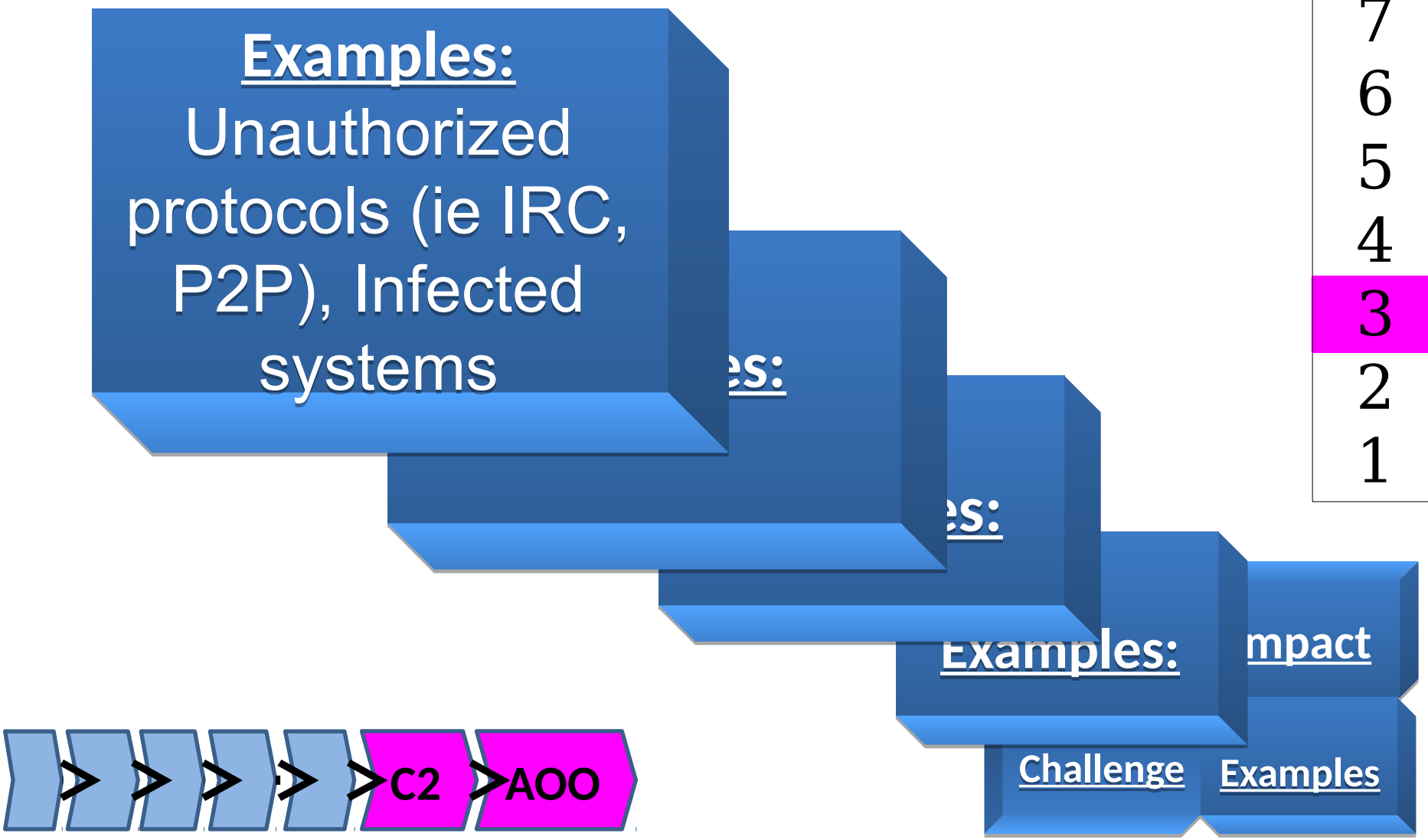
Challenge:

Impact

Examples

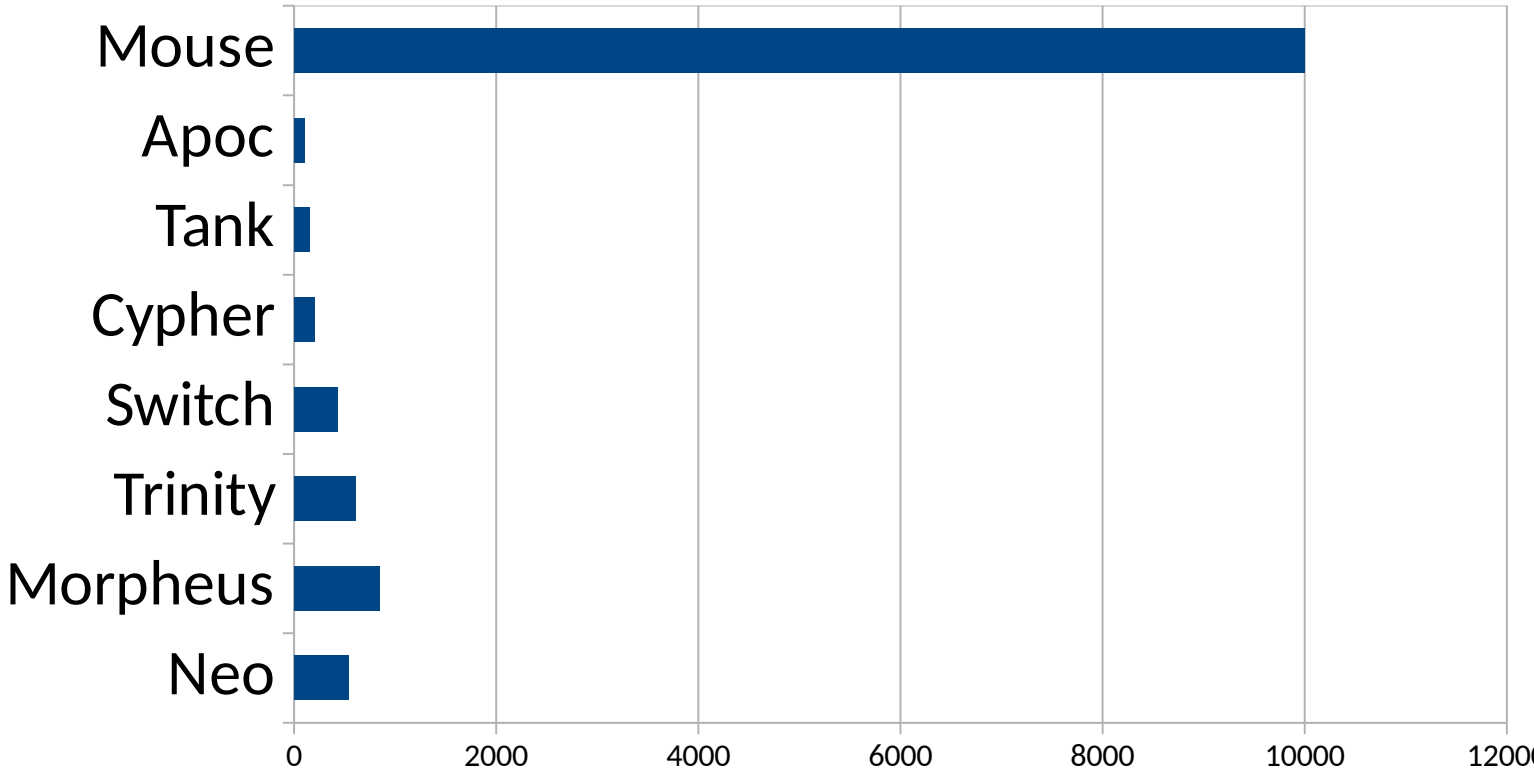
C2 AOO

Top IDS Alerts Int → Ext

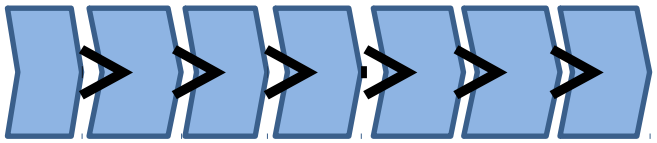


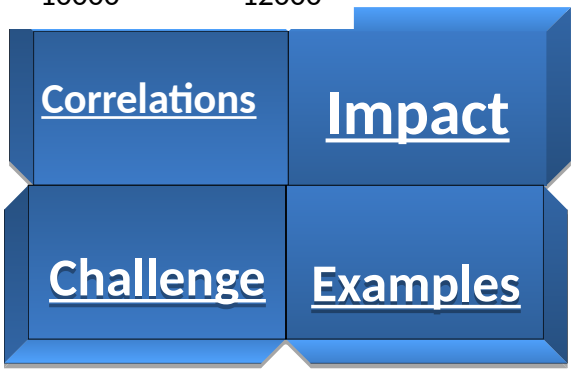
10
9
8
7
6
5
4
3
2
1

Logon Successes

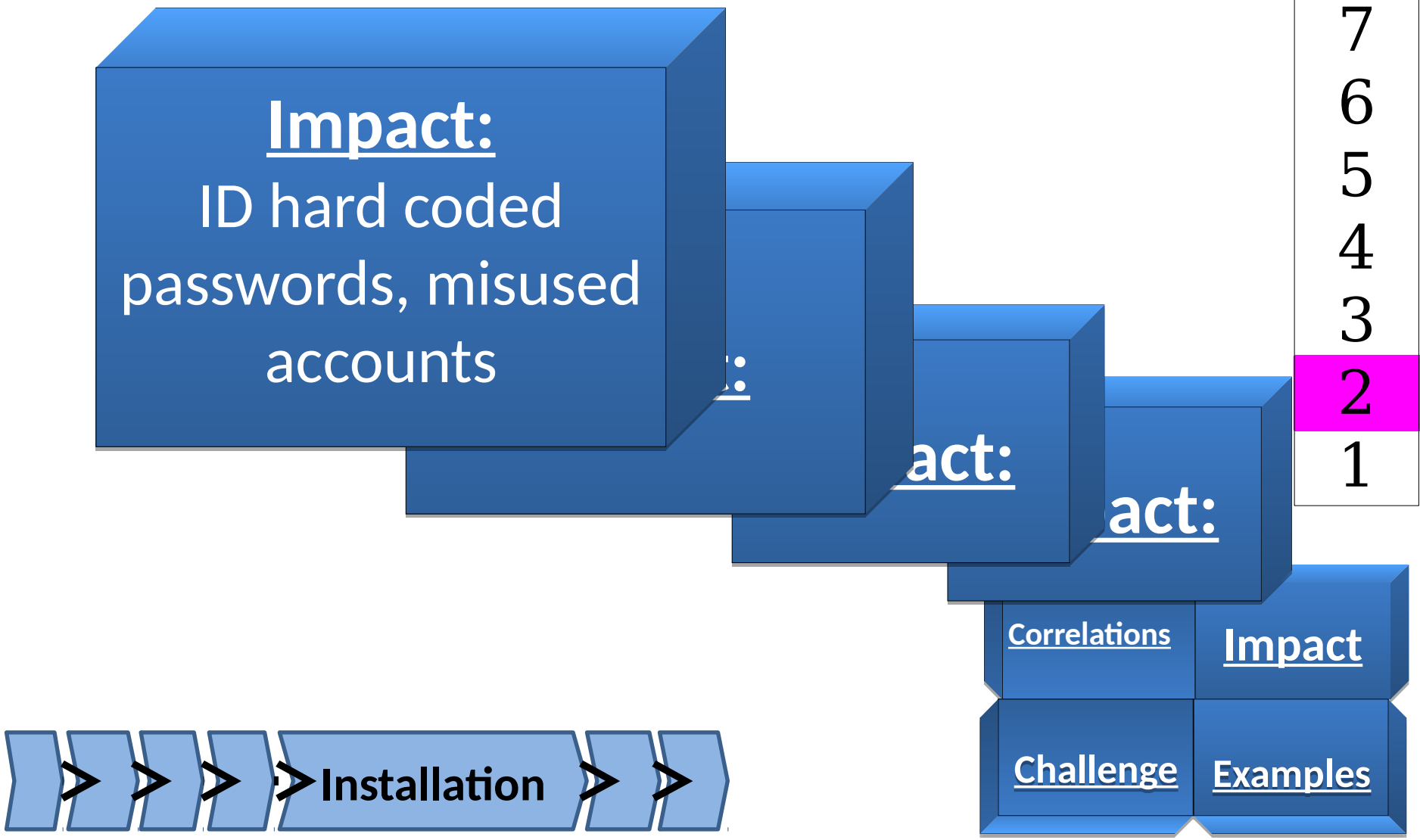


10
9
8
7
6
5
4
3
2
1

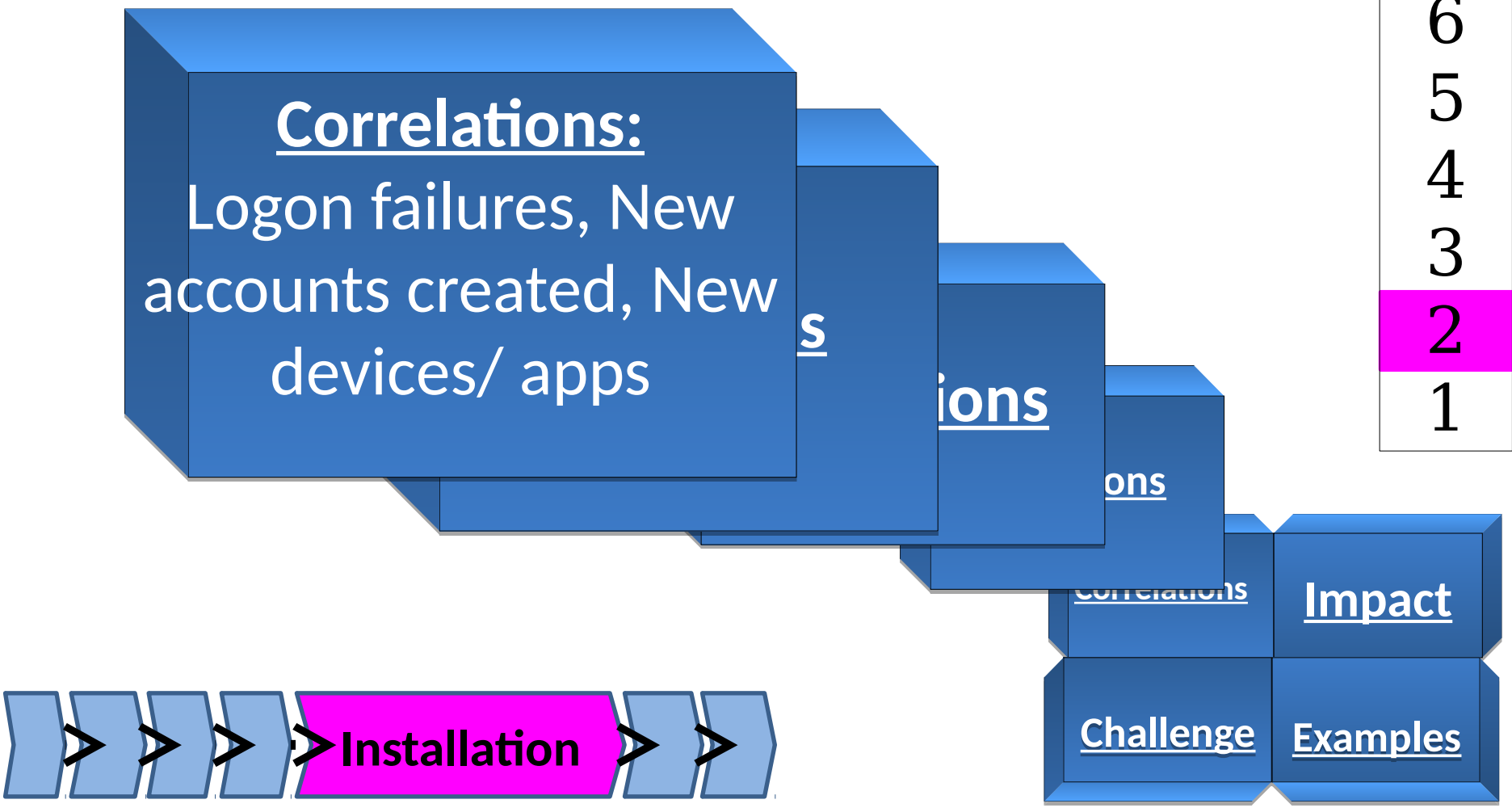




Logon Successes

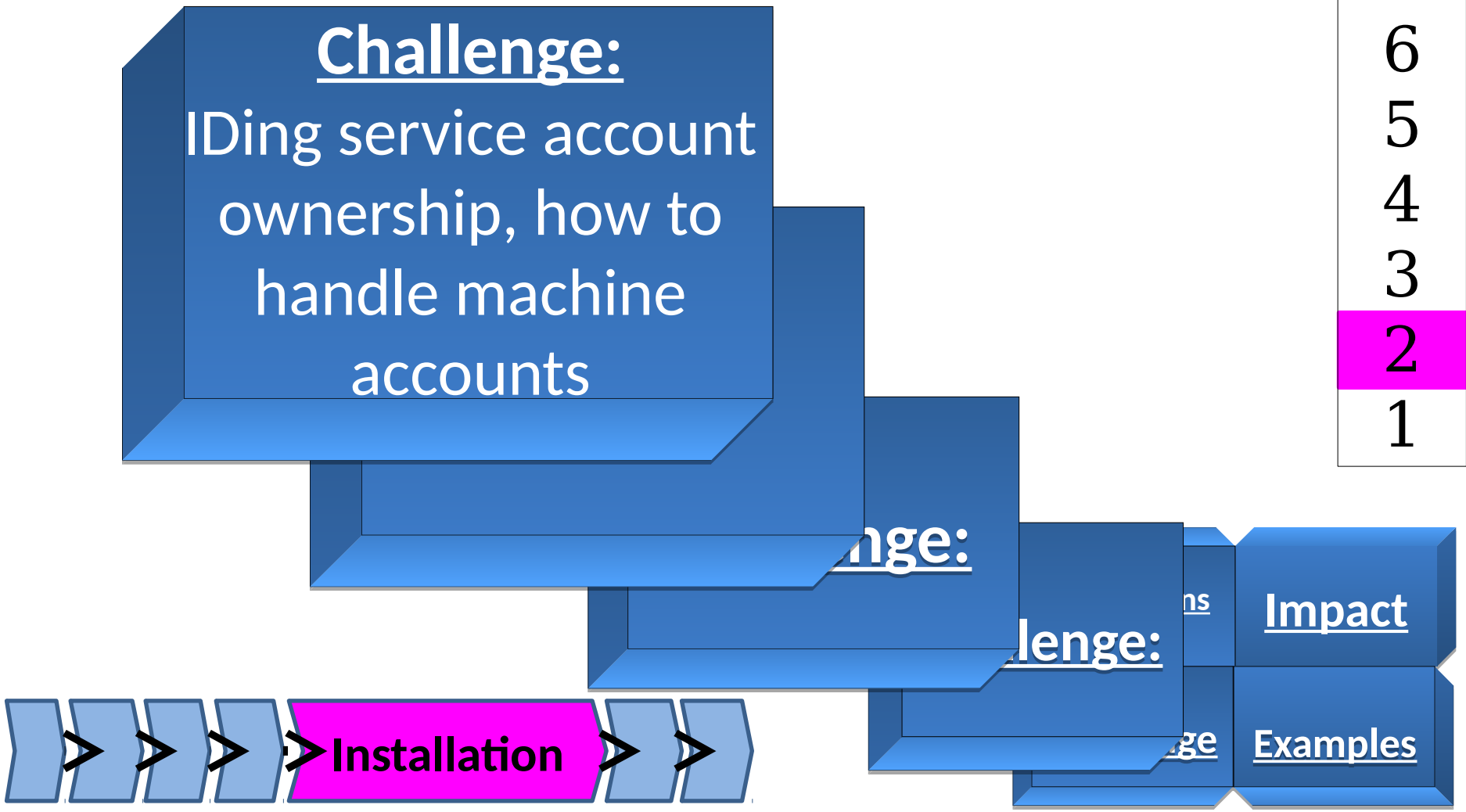


Logon Successes



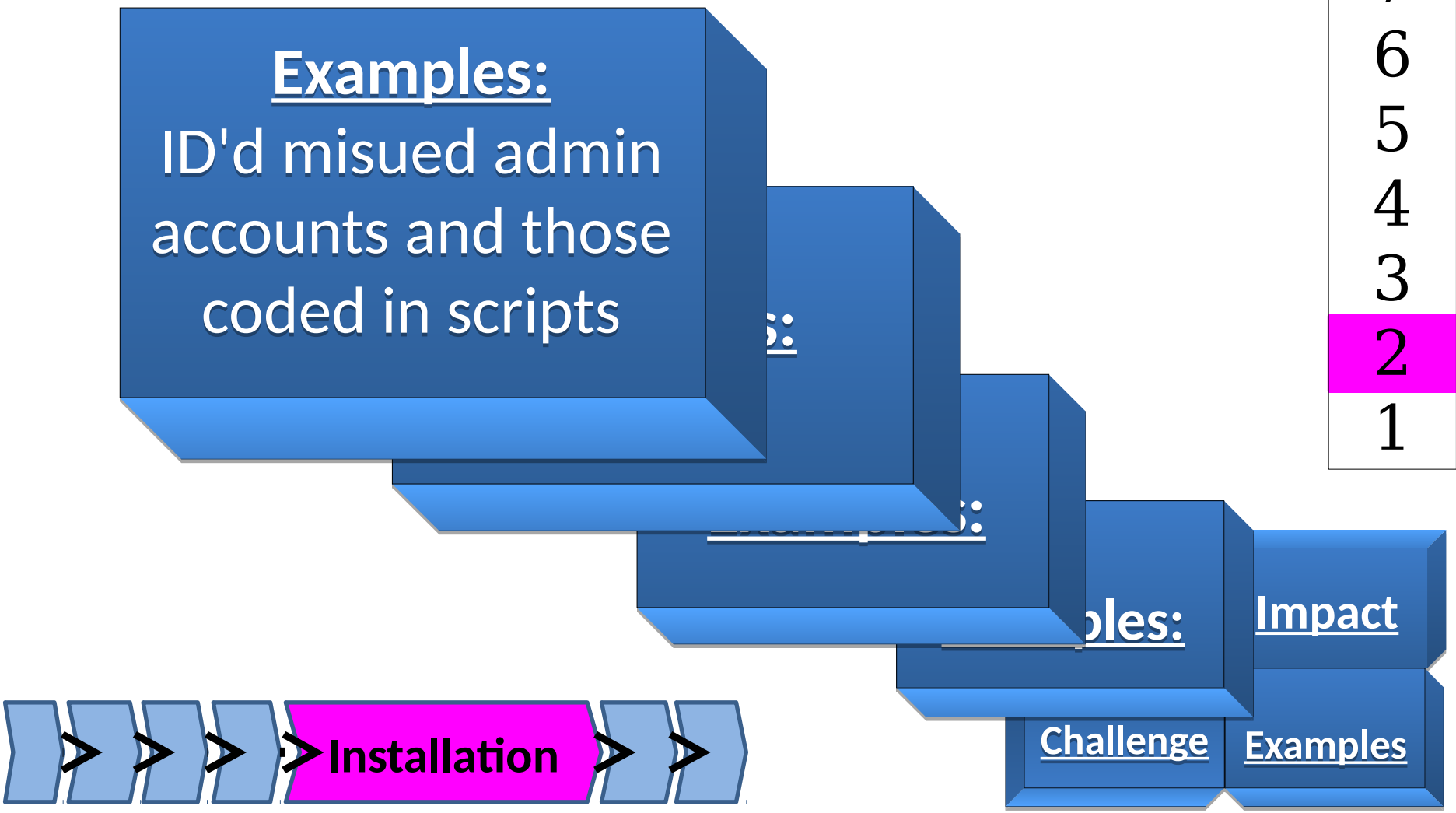
10
9
8
7
6
5
4
3
2
1

Logon Successes



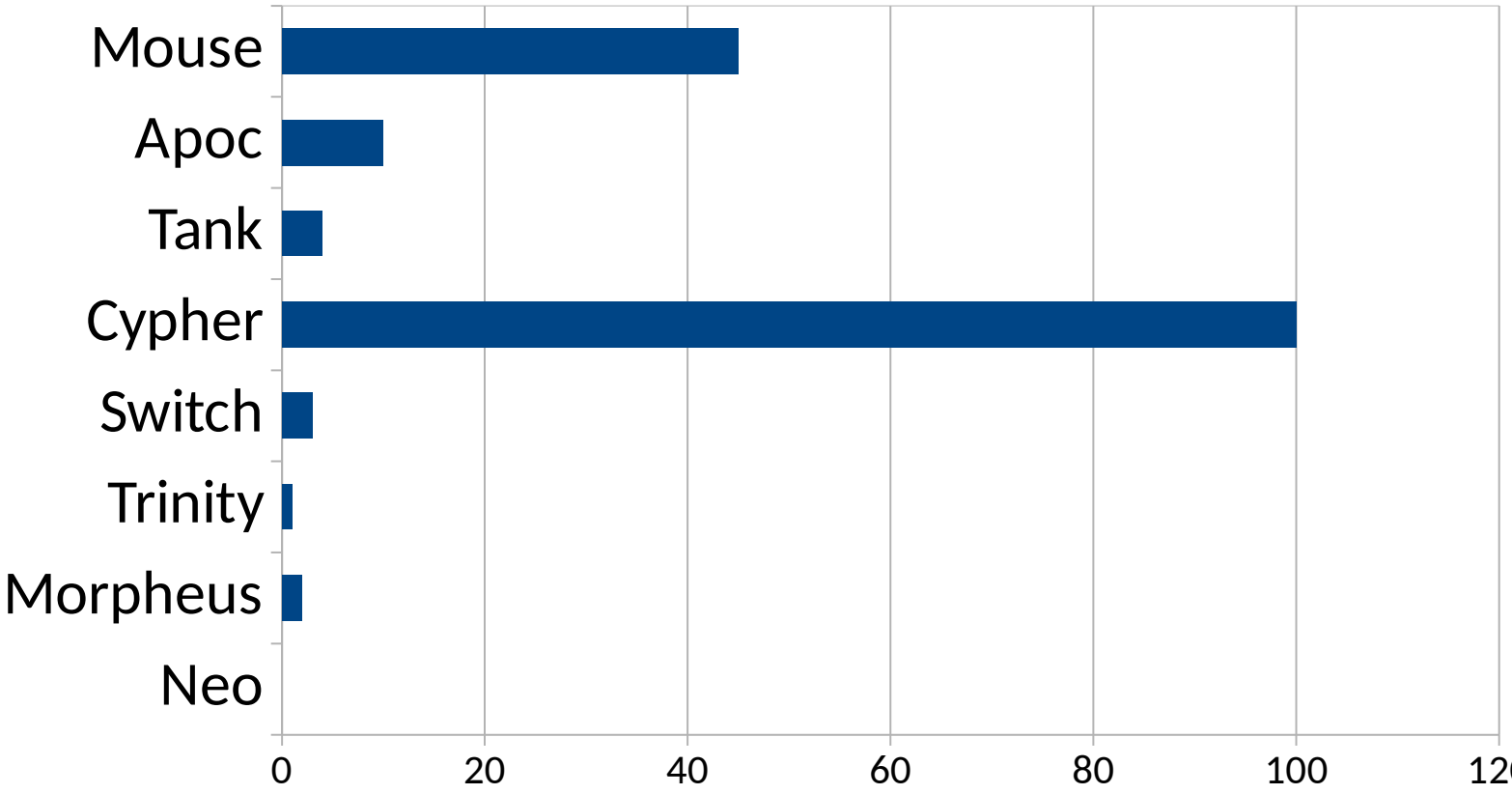
10
9
8
7
6
5
4
3
2
1

Logon Successes



10
9
8
7
6
5
4
3
2
1

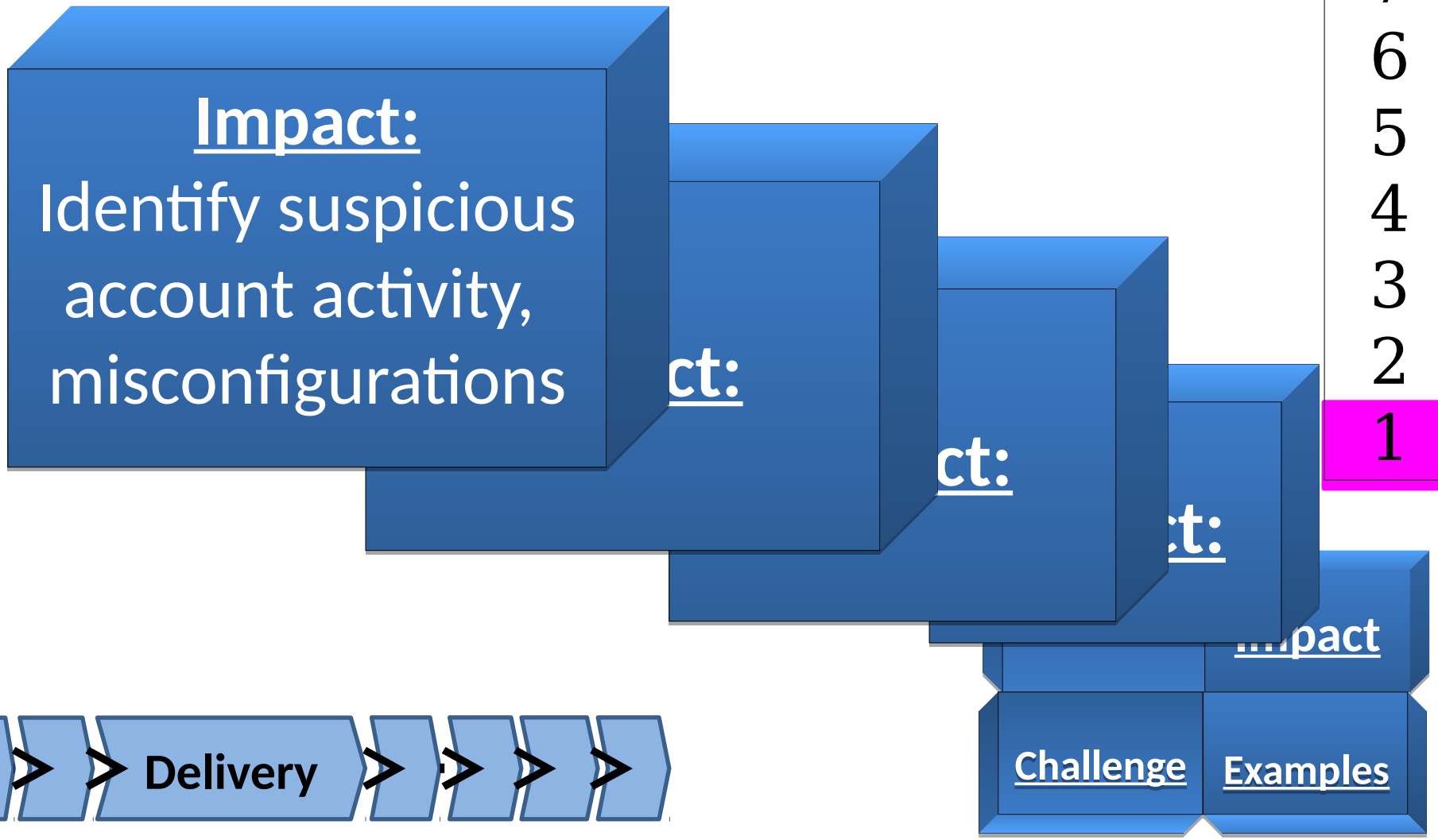
Logon Failures



10
9
8
7
6
5
4
3
2
1

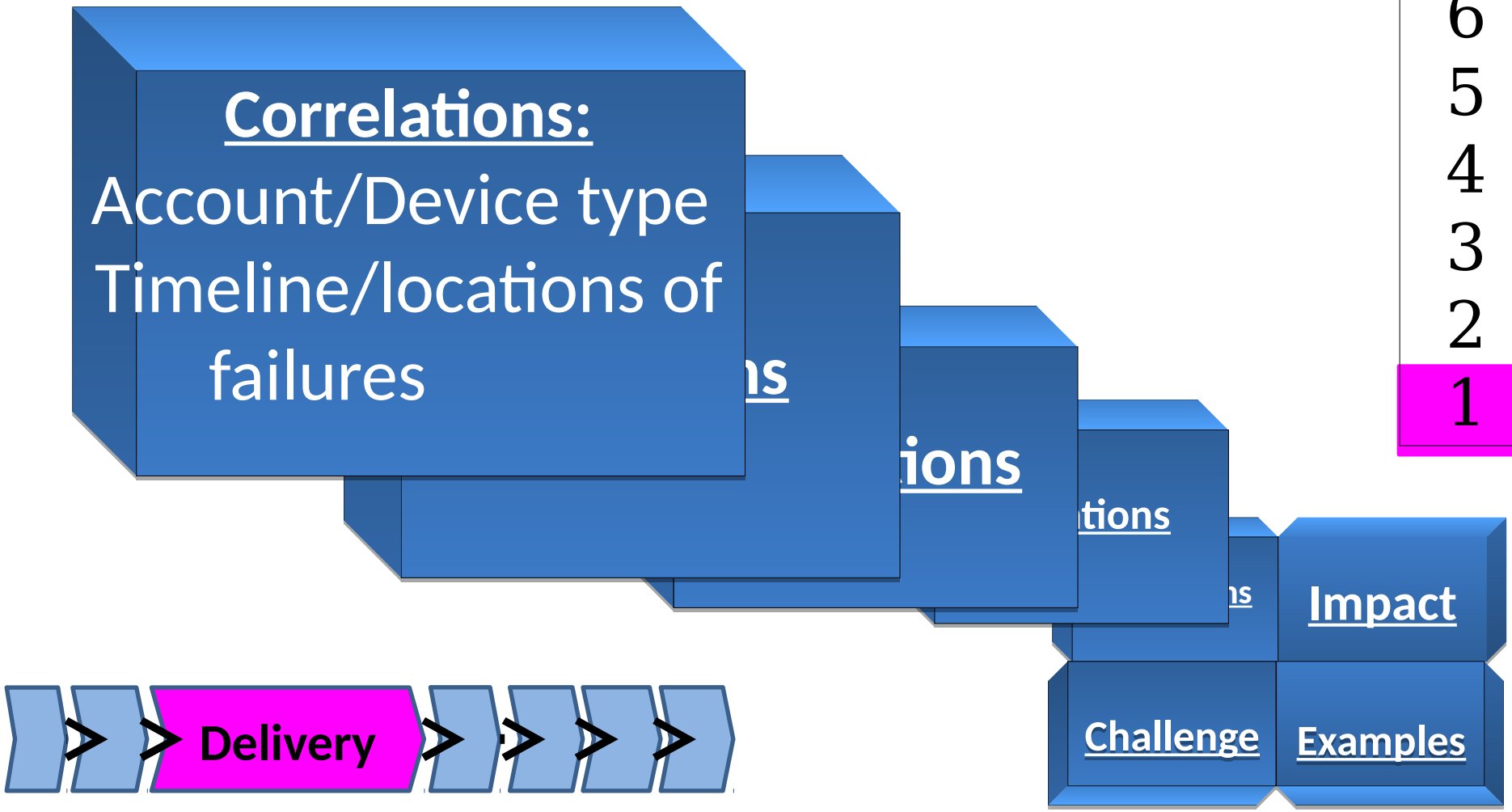
Correlations
Impact
Challenge
Examples

Logon Failures



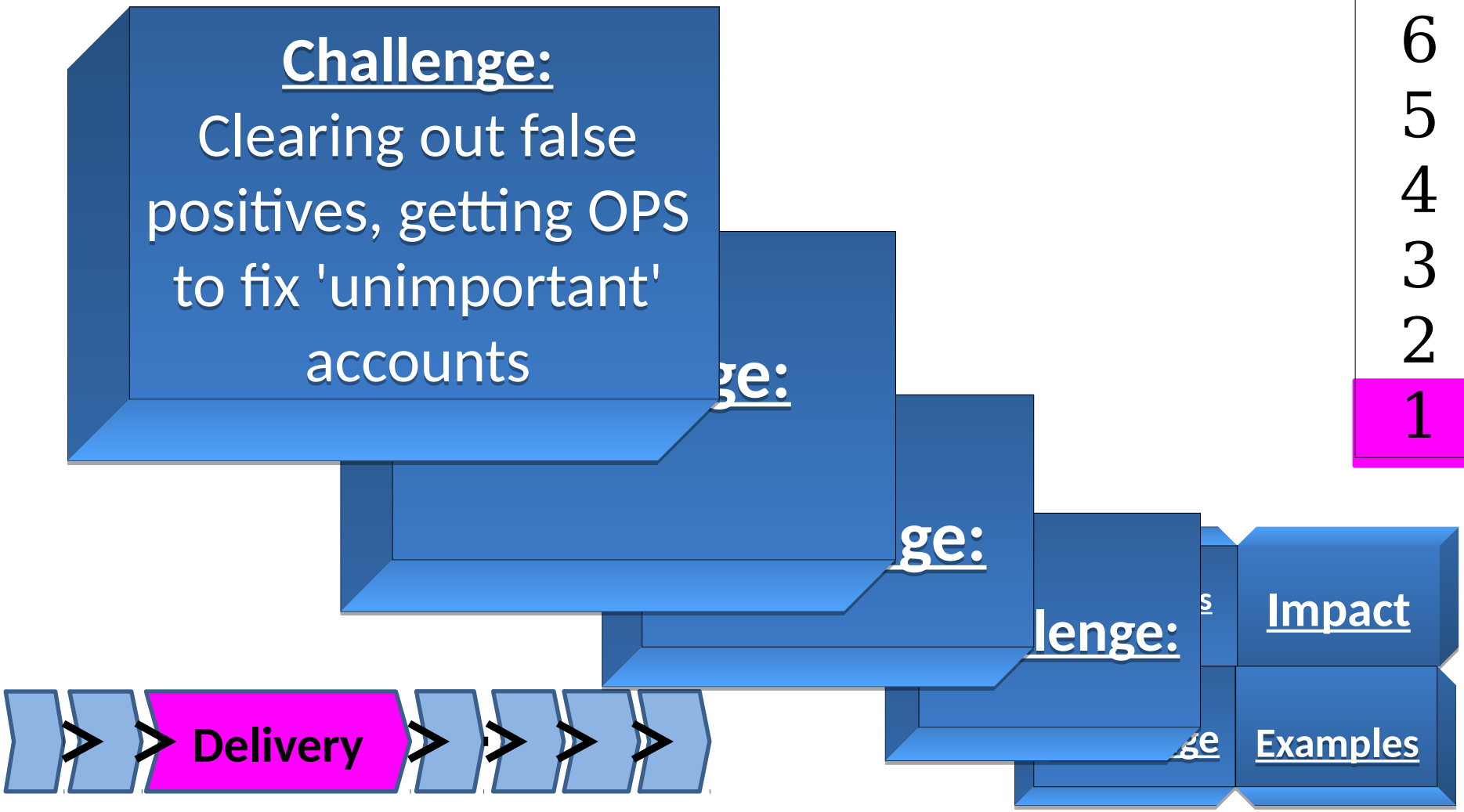
10
9
8
7
6
5
4
3
2
1

Logon Failures



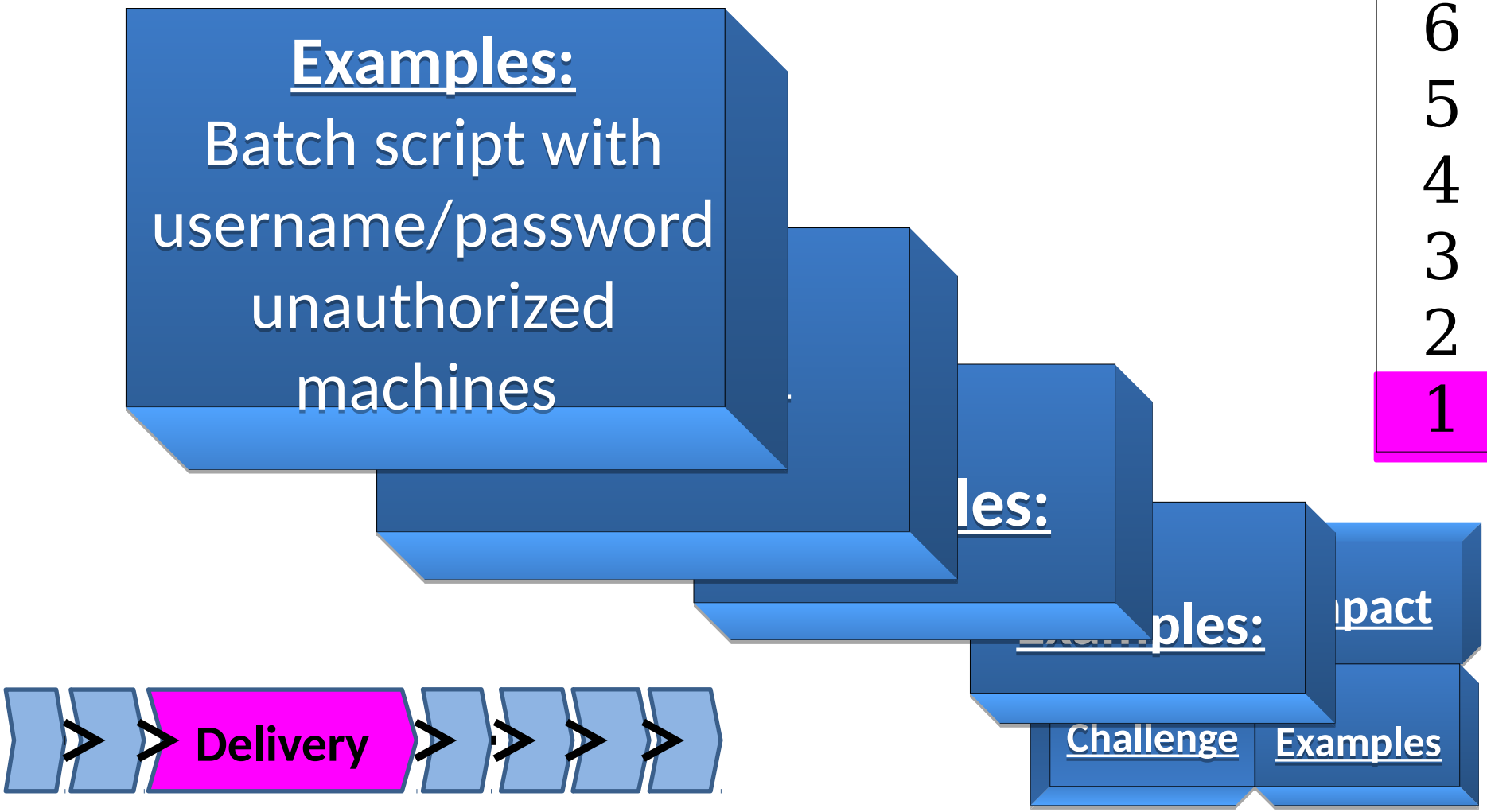
10
9
8
7
6
5
4
3
2
1

Logon Failures



10
9
8
7
6
5
4
3
2
1

Logon Failures



10
9
8
7
6
5
4
3
2
1

Dashboards left off list

IDS Alerts Int → Int

Netflow by Total MB

Unique or Rare Ports used

Unique or Rare IDS hits

Firewall accepts Ext → Int

- Perform passive asset detection

Summary

Dashboards designed for quick setup, ease of use, but may be replaced long term.

Must use these dashboards in correlation with other information to obtain actionable data

Will discover many configuration and operational issues at first

- need to clear out or ignore this noise to see important events

Able to provide simple initial overview of security posture of Enterprise

Next Steps

Tie FISMA into each dashboard?

20 Critical Controls

Solicit more input, discussions

FEEDBACK Welcome

reswob10@gmail.com is best

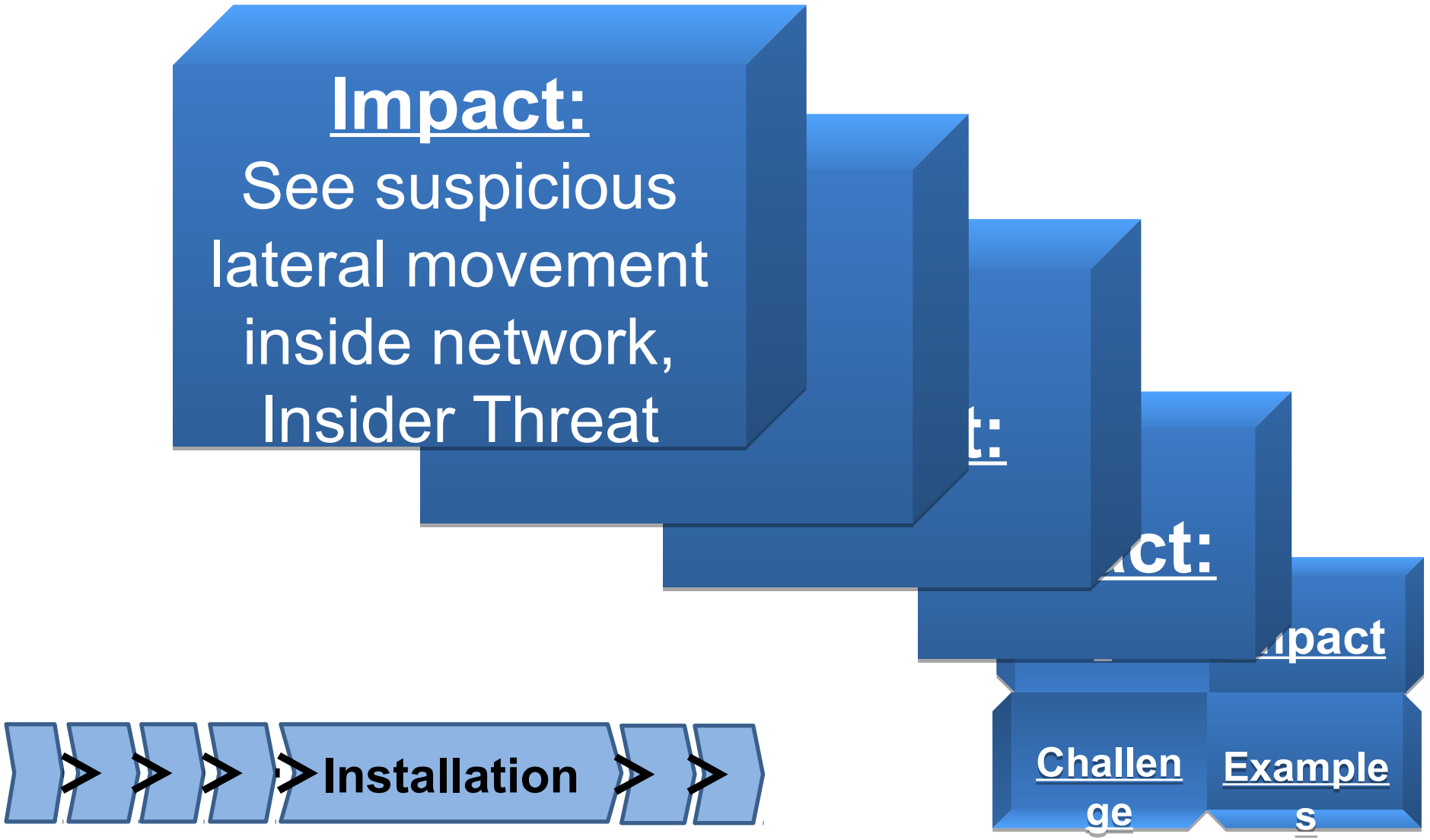
@reswob10 for twitter

When somebody writes, "call if you have any questions," Do they really mean ANY questions? Because I'm really wondering about platypuses.

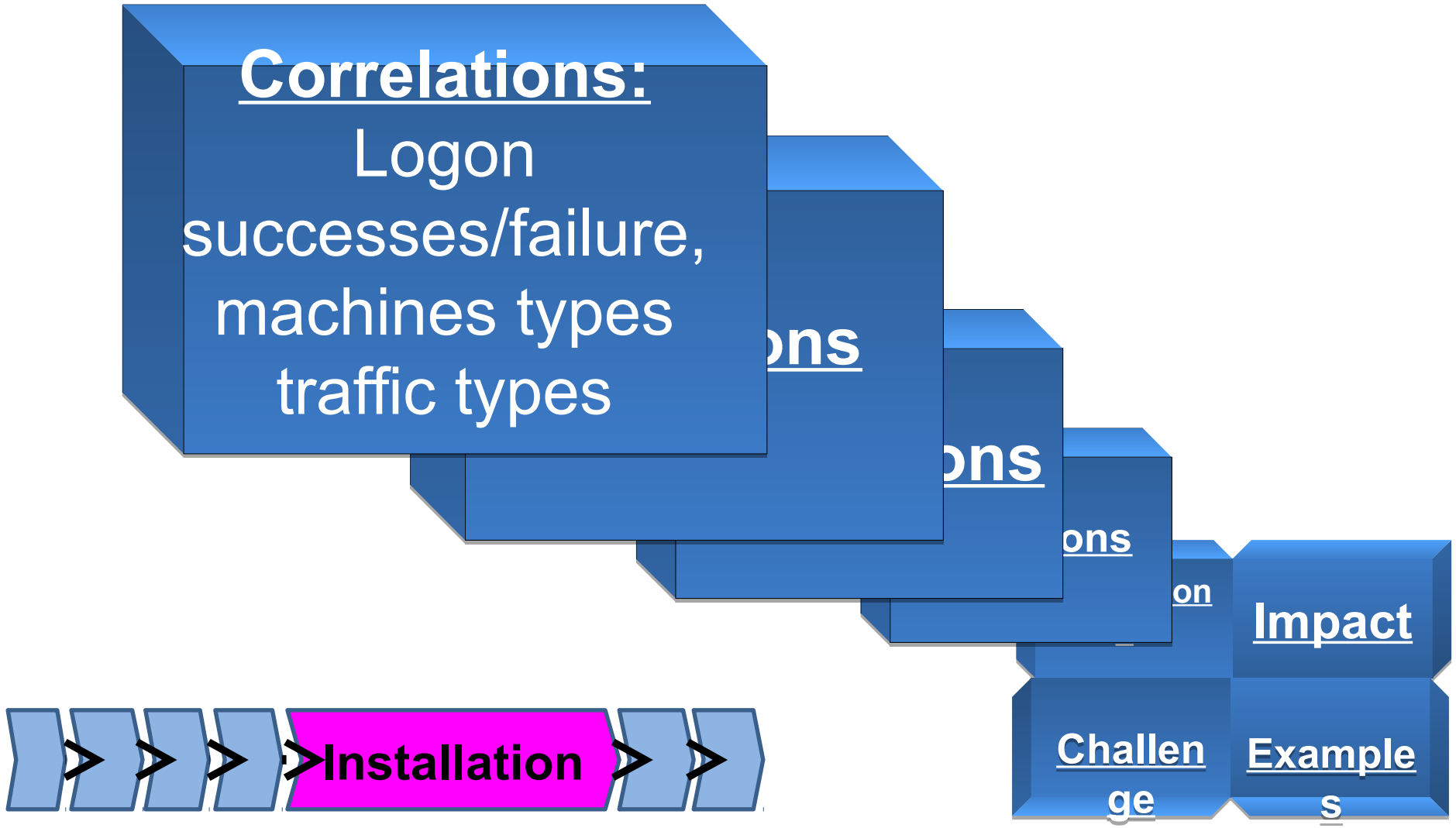
someecards
user card

BACKUP SLIDES

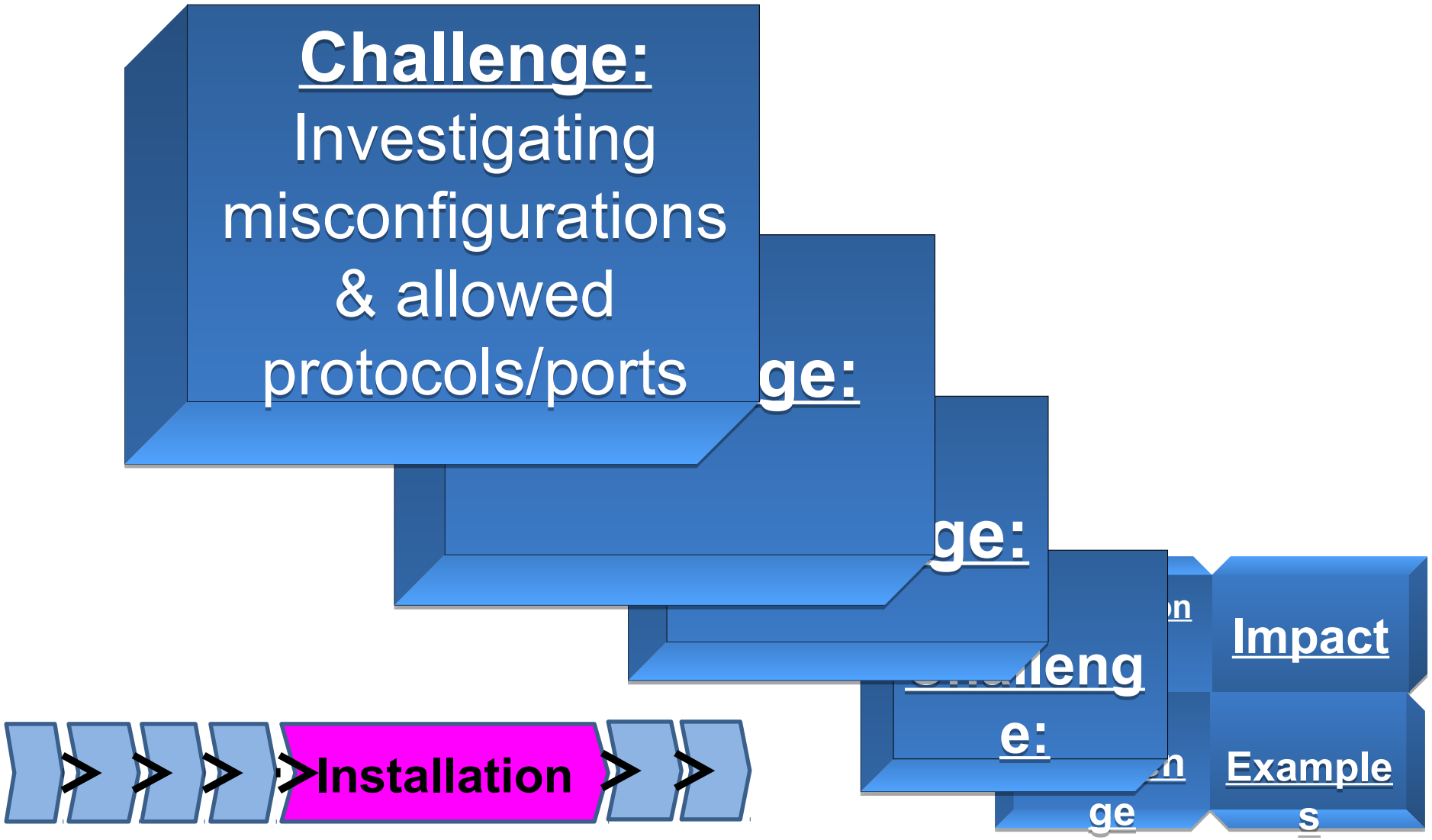
Top IDS Alerts Int → Int



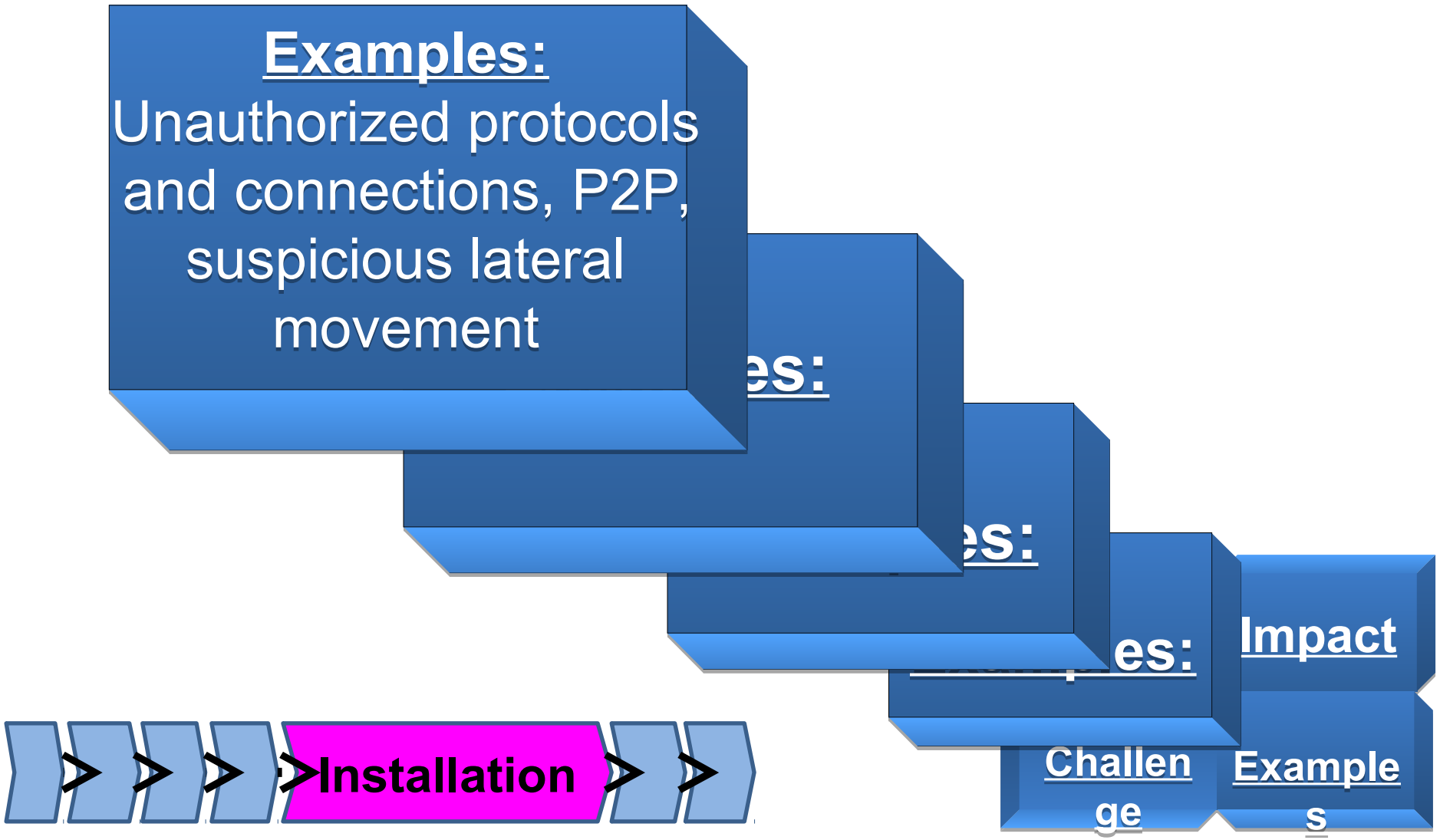
Top IDS Alerts Int → Int



Top IDS Alerts Int → Int



Top IDS Alerts Int → Int



URL hits against blacklist
BONUS # 1

Impact: See suspicious connections
Correlate with: firewall, IDS, netflow activity to determine full extent of activity
Challenge: Keeping blacklist current (remove outdated entries, update new ones)
Examples: Discovering hijacked web sites with redirects
CKC – C2

Activity against inactive accounts BONUS # 2

Impact: See suspicious user activity
Correlate with: authentication failures, access to sensitive network locations, suspicious traffic
Challenge: Keeping list current, coordinating with HD when accounts are reactivated
Example: Found several accounts that were used to configure a service that runs rarely.
CKC – Exploitation