COMP6443 – TOPIC 5 (WEEK 9) Extended

Enterprise Security – Detecting our Attackers

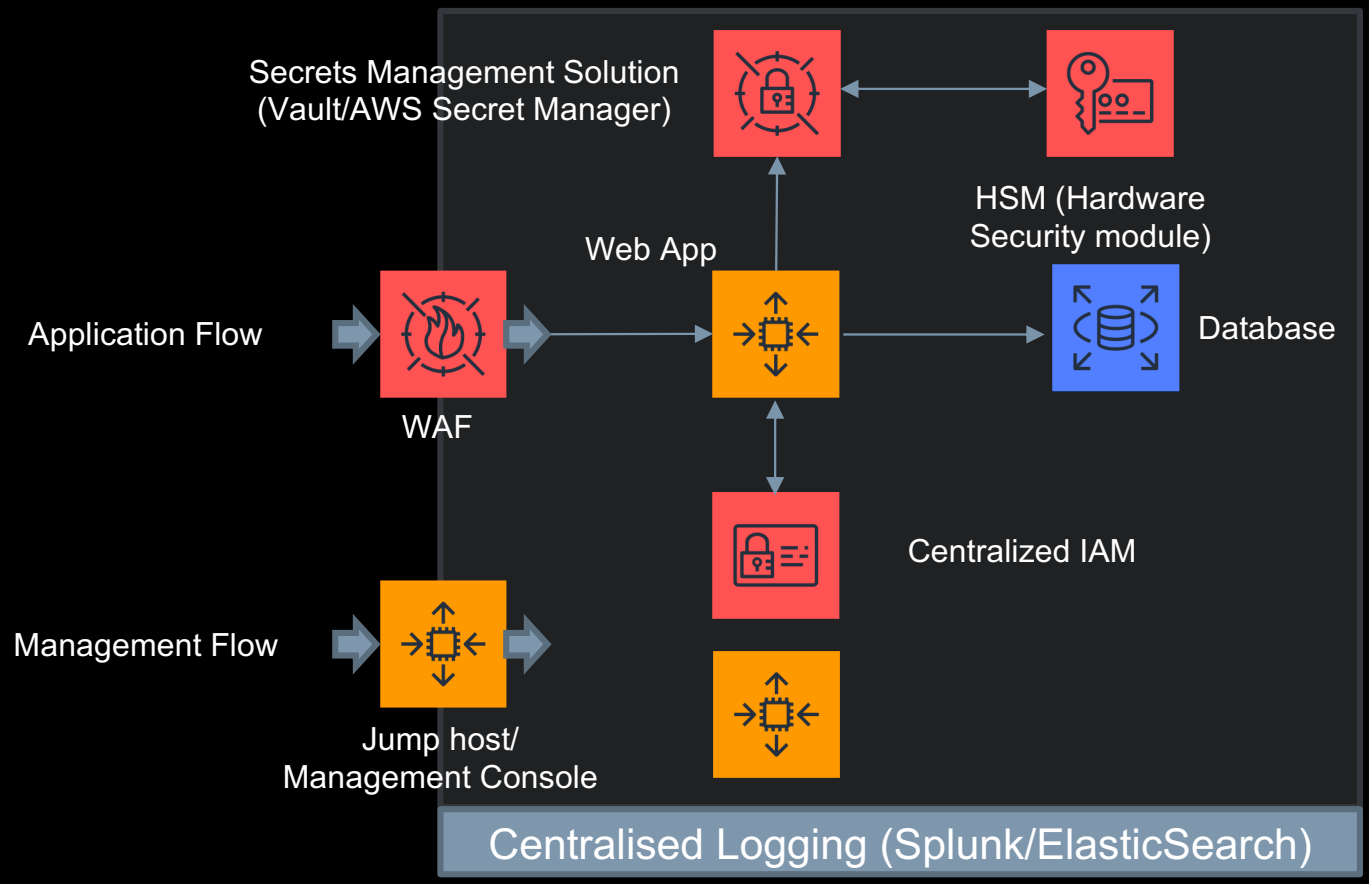
Today’s approach

- Today we’re going to have a look at what a defensive team sees and doesn’t see when you’re attacking a web application
- The main focus is on providing you with a reasonable understanding of how a defensive team

A NOTE ON ETHICS...

- This course will teach both attacker and defender mindsets
- UNSW hosting this course is an extremely important step forward.
- We expect a high standard of professionalism from you, meaning:
  - Respect the property of others and the university
  - Always abide by the law and university regulations
  - Be considerate of others to ensure everyone has an equal learning experience
  - Always check that you have written permission before performing a security test on a system

Architecture of a modern WebApp



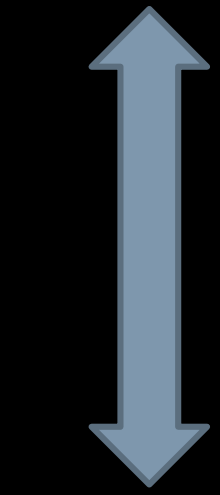
Splunk Demo

Splunk Demo

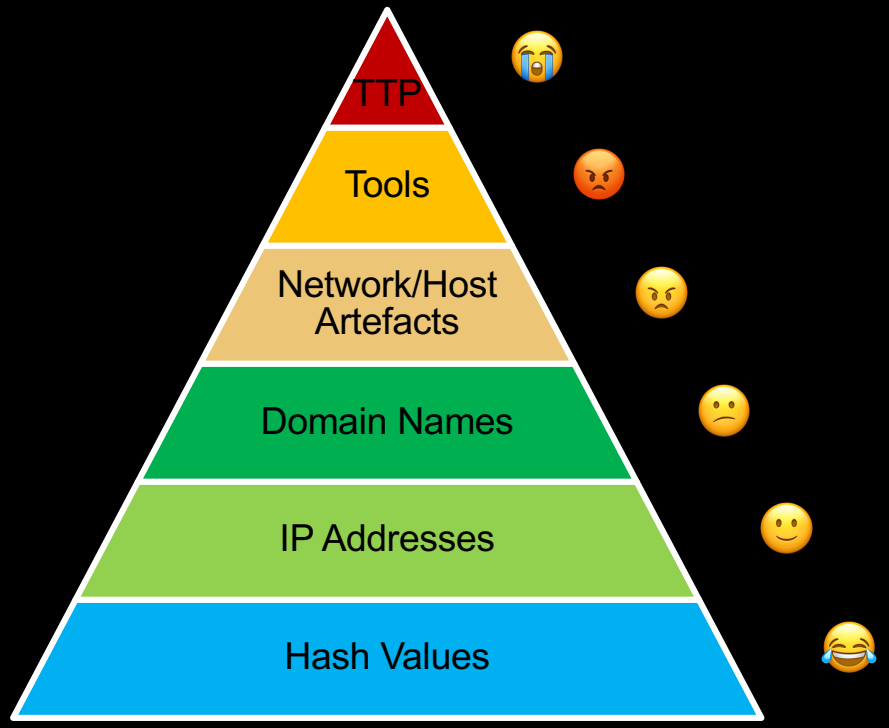
Different types of detection

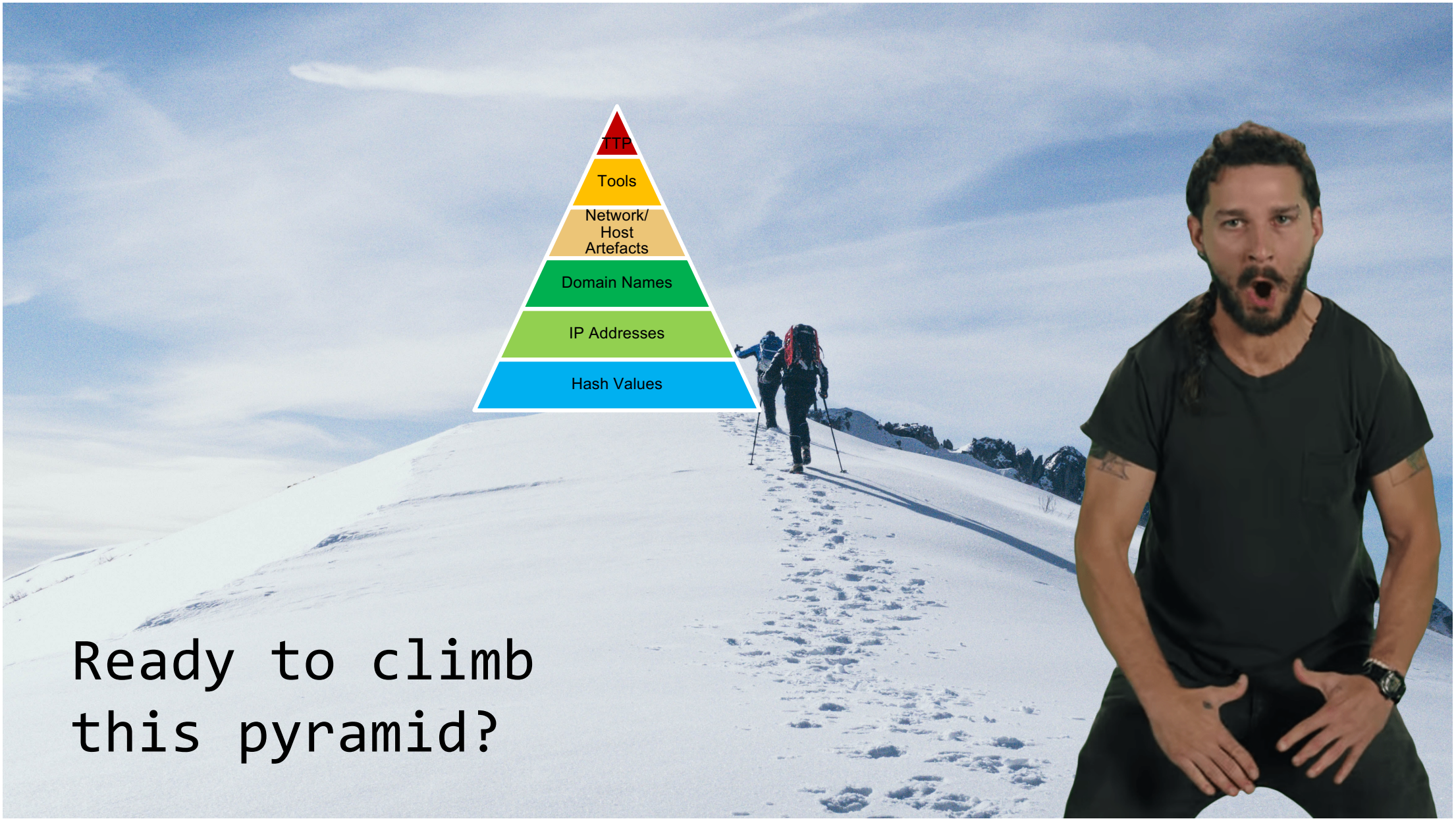
Meet: The Pyramid of Pain

Security Event of Interest



High confidence of known Bad/Indicators of Compromise




TTP
Tools
Network/
Host
Artefacts
Domain Names
IP Addresses
Hash Values
Ready to climb
this pyramid?

The bottom of the pyramid

Known bads || Indicators of Compromise

- As a defensive team you'll have a large number of detection tools.
- Security controls like we discussed on Monday are good examples (WAF, IAM, Secrets Vault)
- Often the goal is to get them to report into the same tool allowing you to manage correlation and alerting from a single platform.

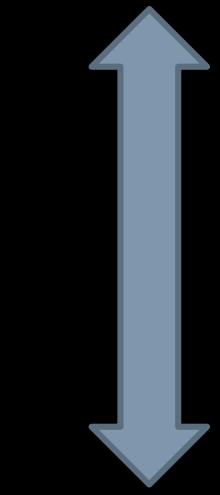
Splunk Query:

```
index=botsv3 sourcetype=xmlwineventlog
Hash="*SHA256=7A1367EFBA05B09E317909B040C3CDA972544212B4F9DB639237492351A3A405"

index=botsv3 sourcetype=stream:ip dest_ip=54.148.121.12

index=sysmon QueryName="sec.edu.au"
```

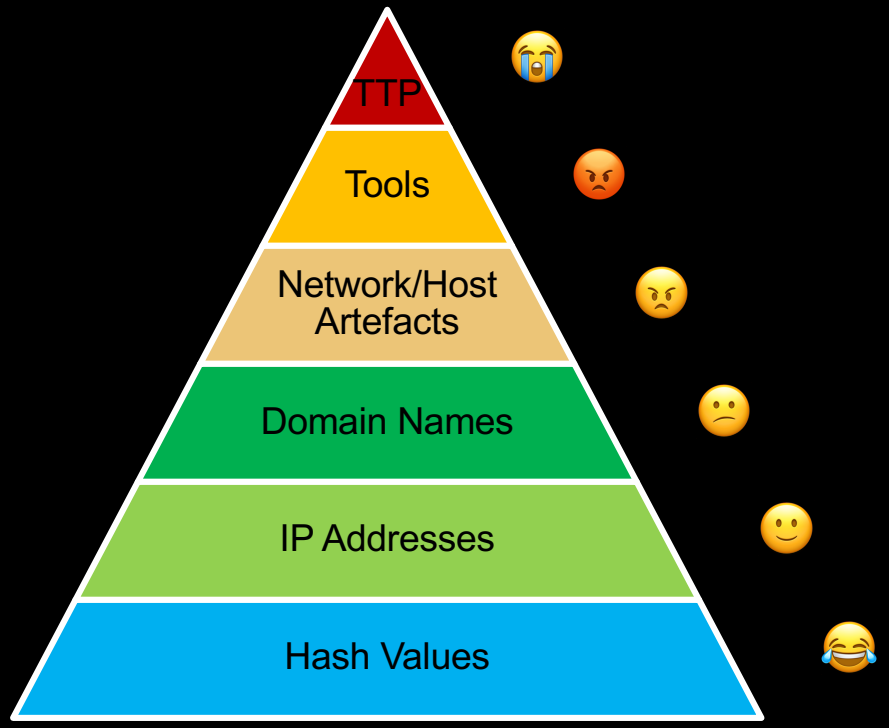
Different types of detection

Meet: The Pyramid of Pain

Security Event of Interest



High confidence of known Bad/Indicators of Compromise

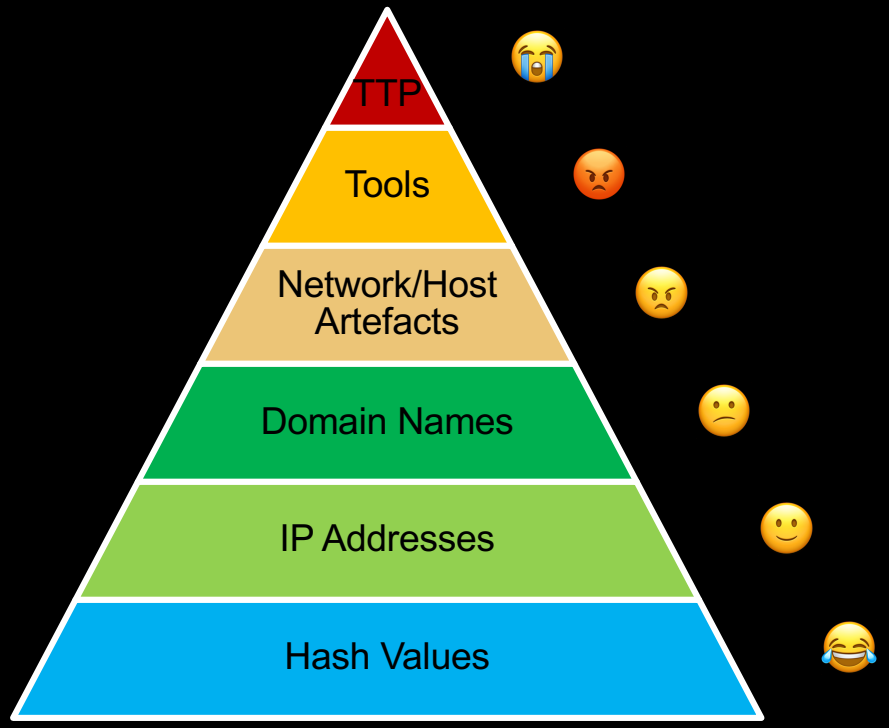


Different types of detection

Meet: The Pyramid of Pain

Security Event of Interest

High confidence of known Bad/Indicators of Compromise



Time consuming, and expense to change

Easy and cheap to change

MITRE ATT&CK

- The MITRE ATT&CK framework[1] is a dictionary for attack tactics and techniques.
- Tactics (why), techniques (how), and procedures (implementation)
- Used to make sure that when I say ‘Steal Web Session Cookie’ (T1539) we all know what I’m talking about; https://attack.mitre.org/techniques/T1539/
- A common mistake for security people is to aim for mitre attack matrix coverage.
- Each TTP has a 1:* mapping, which means that stealing a web session cookie can occur via many different implementation (procedures)

[1] https://attack.mitre.org/

Example: XSS to logon

- You were able to leverage an XSS vulnerability to steal a users o365 cookie. You placed this cookie into your own browser and are able to log into the email app as that user.
- **MITRE ATT&CK mapping:**
  - ‘Drive by Compromise’ to get code execution in the user’s browser
  - ‘Steal Web Session Cookie’ to get access to their session
  - ‘Email Forwarding Rule’ to automatically start collecting your target’s email

The (almost) top of the pyramid

Security Event of Interest

- T1053 Scheduled Task/Job (https://attack.mitre.org/techniques/T1053/)
- Creation of a schedule task/job on a windows machine using the schtask.exe binary

Splunk Query:

index=wineventlog Process_Command_Line="SCHTASKS*/Create*”

SCHTASKS /CREATE /SC DAILY /TN "MyTasks\backdoor" /TR "C:\Windows\System32\cmd.exe" /ST 11:00

Want to know more?

- **Part 1 The Funnel of Fidelity:**
  ttps://posts.specterops.io/introducing-the-funnel-of-fidelity-b1bb59b04036
- **Part 2 Capability Abstraction:**
  https://posts.specterops.io/capability-abstraction-fbeaeeb26384
- **Part 3 Detection Spectrum:**
  https://posts.specterops.io/detection-spectrum-198a0bfb9302

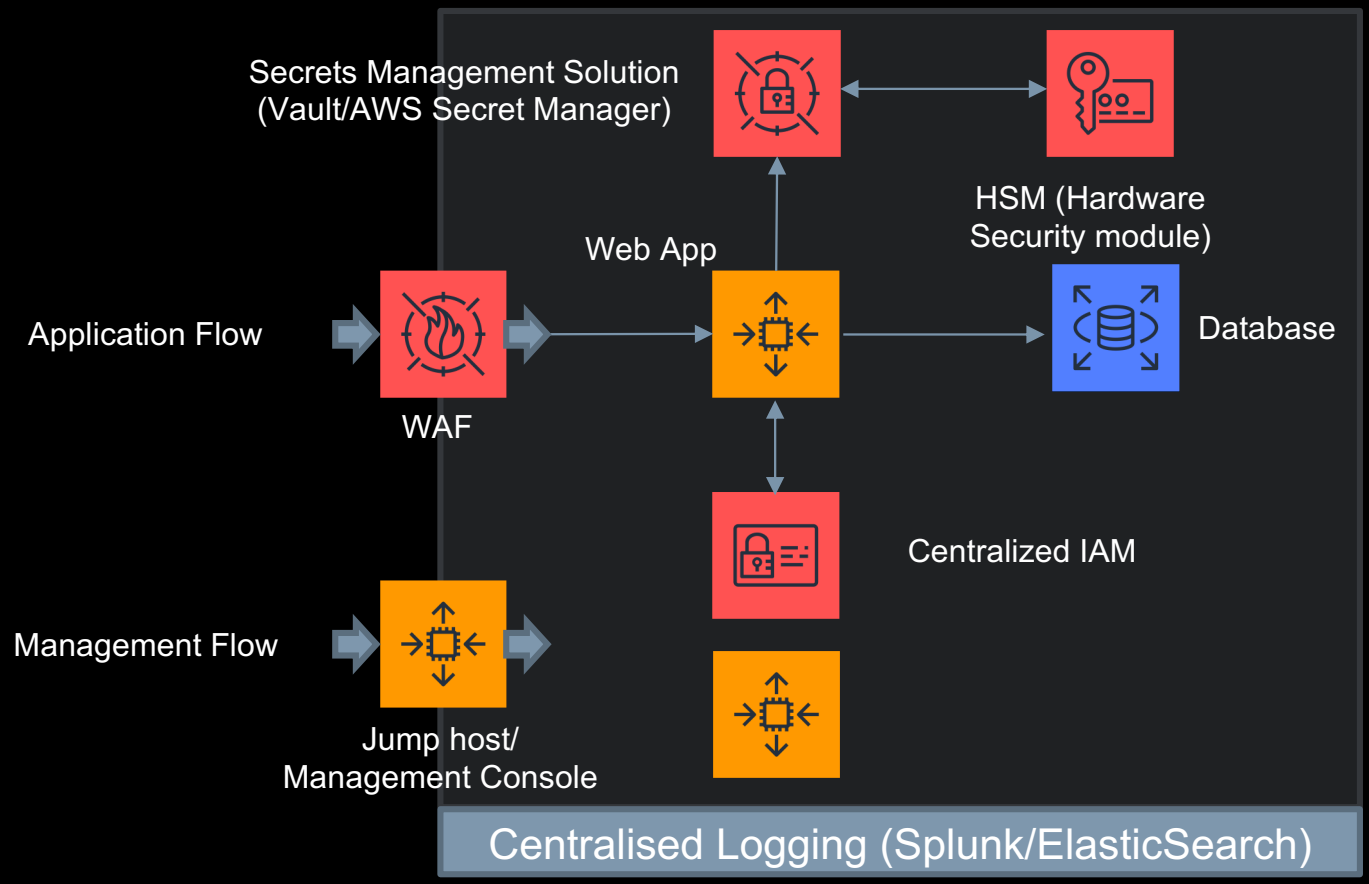
Public RW S3 Buckets

- Logs can help you do more than just detect attackers
- They can help you detect high risk security situations
- Example below used: https://www.gorillastack.com/news/cloudtrail-event-names/

Splunk Query:

```
index=botsv3 sourcetype=aws:cloudtrail eventName=PutBucketAcl
| search requestParameters.AccessControlPolicy.AccessControlList.Grant{}.Grantee.URI="http://acs.amazonaws.com/groups/global/AllUsers"
| spath output=aclControlList path="requestParameters.AccessControlPolicy.AccessControlList"
| spath input=aclControlList output=grantee path=Grant{}
| mvexpand grantee
| spath input=grantee
| search "Grantee.URI"="http://acs.amazonaws.com/groups/global/AllUsers"
| eval iso8601time=strftime(_time,"%Y-%m-%dT%H:%M:%S%z")
| stats values(iso8601time) as time, values(Permission) as permissions_granted, values(userIdentity.arn) as arn by requestParameters.bucketName
```

Architecture of a modern WebApp



DetectionLab

- https://github.com/clong/DetectionLab
- A detection environment with all the tools installed
- Allows you to write detection logic for techniques from top to bottom of the pyramid.

Assignment

Splunk

THANKZZZZ!!!11

questions? slack/email/talk to me

Thank you