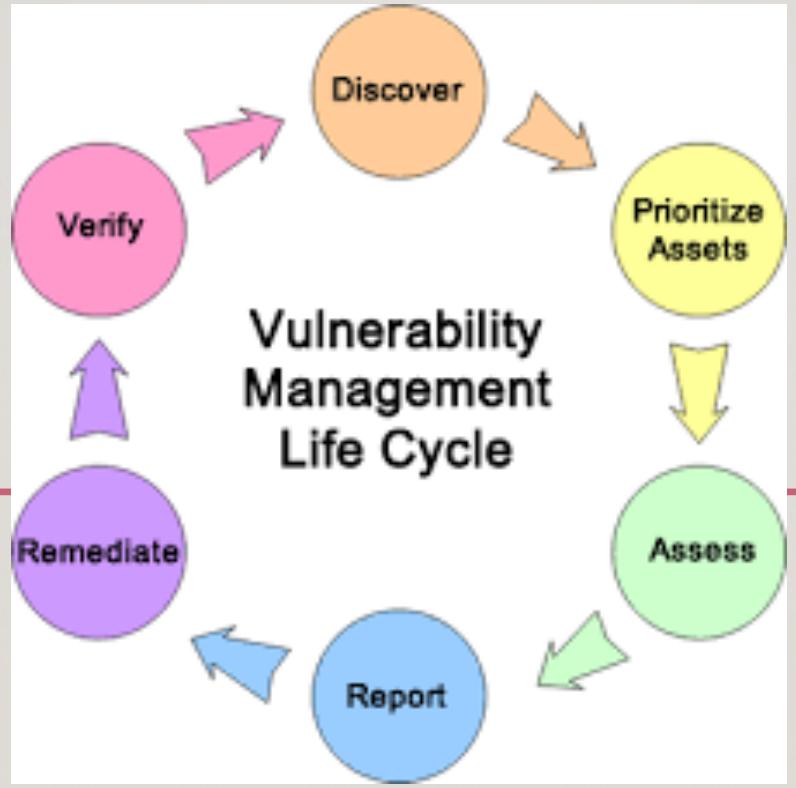
The events, characters and firms depicted in this photoplay are fictitious. Any similarity to actual persons, living or dead, or to actual firms, is purely coincidental.

VULN MNGT PROCESS

OVERVIEW



DISCOVER

- We are scanning the infra by Rapid 7.
- Internal
- External ….

- Internal Scan … npton

DISCOVER VS INVENTORY

- Do we have an inventory to compare whether the scanned assets are accurate?

Which needs to be scanned and which needs to be excluded!

SITES

Name	Assets
[redacted]	2,512
[redacted]	2,176
[redacted]	1,973
[redacted]	409
[redacted]	408
[redacted]	202
[redacted]	188
[redacted]	49
[redacted]	10
[redacted]	134

Row Labels	Count of Address
[redacted]	409
[redacted]	134
[redacted]	202
[redacted]	2512
[redacted]	3257

Unnamed Assets

Row Labels	Count of Address
(blank)	1562
[redacted]	252
[redacted]	53
[redacted]	36
[redacted]	1221
Grand Total	1562

Routers, Switches, GW

(Ne Excluded)

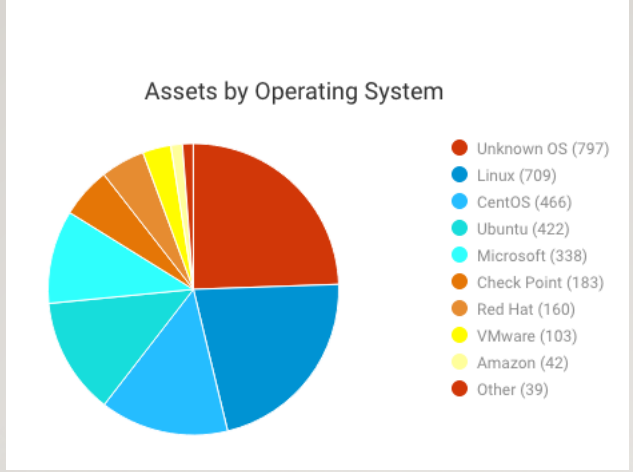
(Ser

Can we fine tune/Decom/Ownership?

Tagging

ASSET TAGS

Name	Type
[redacted]	Location
[redacted]	Location
[redacted]	Location
[redacted]	Location
[redacted]	Location
[redacted]	Location
[redacted]	Location
[redacted]	Location
[redacted]	Location
[redacted]	Location
[redacted]	Location
[redacted]	Location
[redacted]	Location
[redacted]	Location



Tagging can be done for

- Project
- Owners
- Criticality
- Exposure
- Audit List

Sample Dashboard for continuous monitorin

With all these analyzed we prioritize and create Remediation project for the Ops to fix/patch/remediate Vuln’s.

PRIORITIZE

How or What are we Prioritizing, The Vulnerability?

By Assets???
By
By
Assets that fail for SOX Audit???

We are tagging and differentiating Assets that are Exposed Public, Whitelisted, Internal, by the criticality/Impact.

We will be improvising to letting you know and patch/remediate which needs immediate attention.

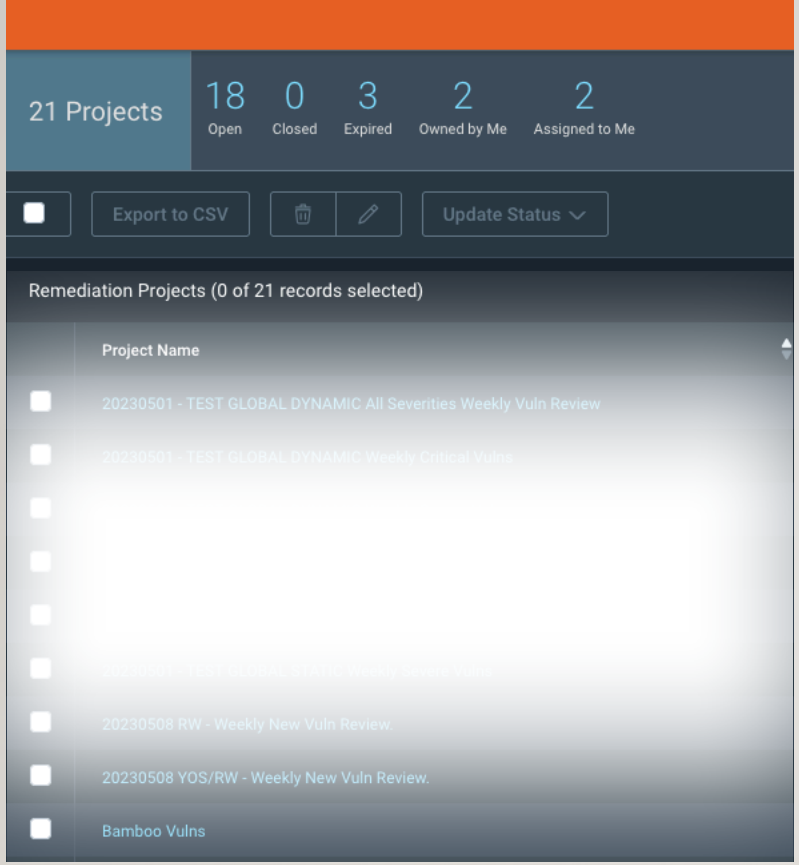
ASSESS

Vulnerability Risk Assessment Factors:

- Is this vulnerability a true or false positive?
- Could someone directly exploit this vulnerability from the Internet?
- How difficult is it to exploit this vulnerability?
- Is there known, published exploit code for this vulnerability?
- What would be the impact to the business if this vulnerability were exploited?
- Are there any other security controls in place that reduce the likelihood and/or impact of this vulnerability being exploited?
- How old is the vulnerability/how long has it been on the network?

REPORT

- We will be creating REMEDIATION PROJECTS in R7.
- As per the SLA & GOALS depending upon the vuln criticality the project will be given a time period to remediate with the report of Solutions how the same needs to be remediated/patched.
- Eg. If an External Facing Asset is found h vuln that has an Exploit code that is ex h no auth.



Depending on the Priority and Criticality the Remediation Project will be created with the SLA Time Period.

7 Days
30 Days
90 Days

REMEDIATE

- The business can take any of the approach as per the criticality so that the vuln is not exploited in the wild.

- The LCM & Patching cycle that are followed will be marked/added into the projects respectively on every month unless if its not critical & only be reported if any gets unattended during the patch cycle.
- The solution list will be a great resource.
- We need Operations help and support for this.

VERIFY

- We will evaluate the missed ones post the SLA’s are breached.

VULN EXCEPTION

- EOL.
- EOS.
- SUPER SEEDED.
- BUSINESS DEPENDENCY.
- RISK ACCEPTED.

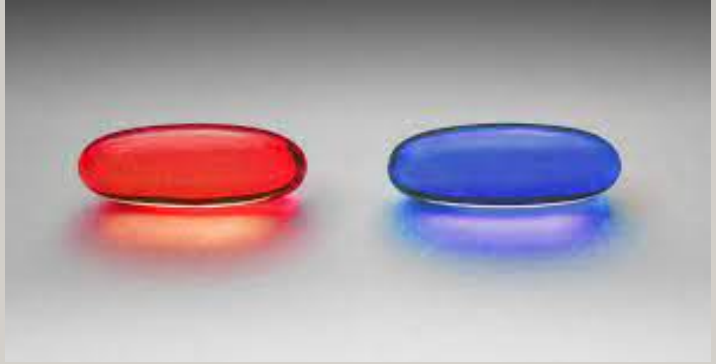
WHO OWNS THE

RISK


IT should report to Security, not the other way around


IT should report to Security, not the other way around
CHANGE MY MIND

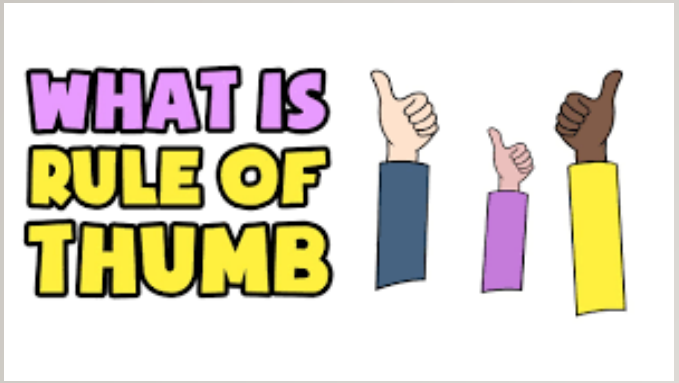

AI



When the SLA’s are getting breached???

Do we need extra resource I Management Intervenes required (=+-)???

When all Assets and Vuln are marked and assessed
A MARKETING Strategy that can be added..??



Do ~~not~~ Speak, Seek, Ask & Question!!!???