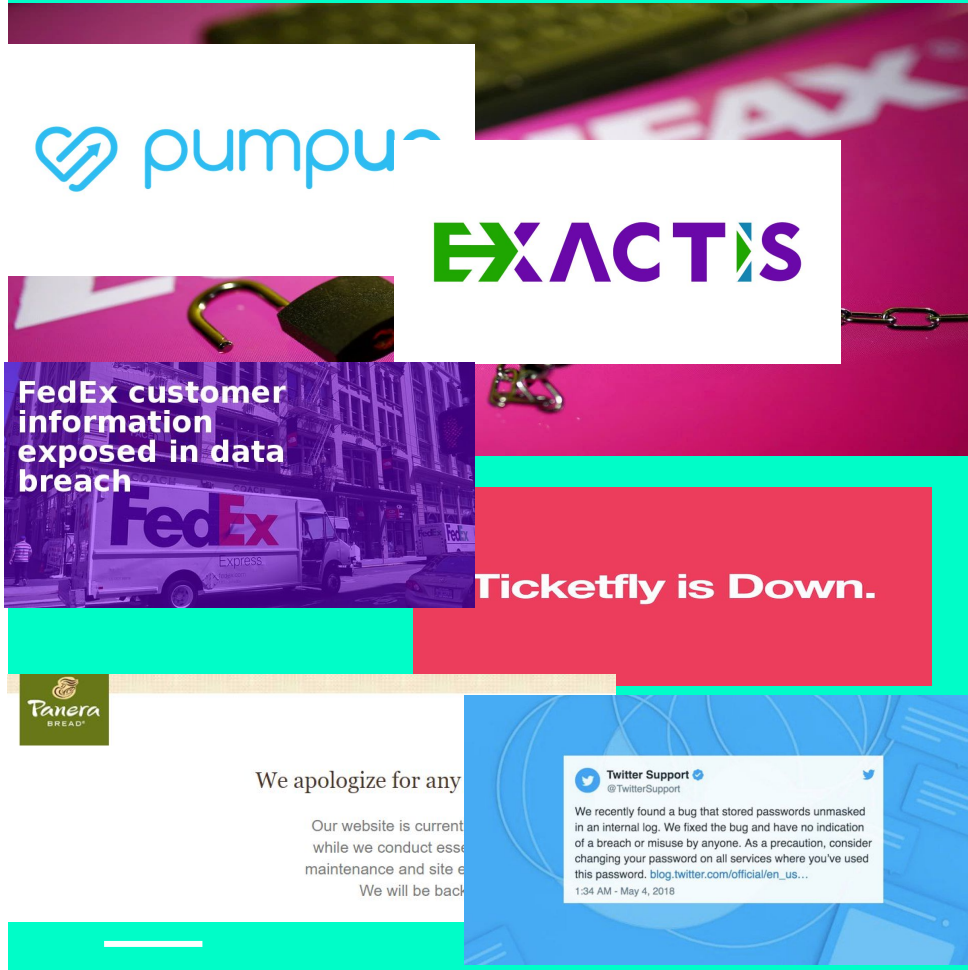
How NOT to suck at Vulnerability Management

Shellcon.io
Plug (@plugxor) and Chris (@ChrisHalbersma)

Current Landscape

- Apache Struts
- backend server exposed to the Internet
- database exposed
- unsecured server
- data leak
- Software Bug



SOURCE: https://blog.barkly.com/biggest-data-breaches-2018-so-far

DUO Labs - Beyond S3: Exposed Resources on AWS
https://duo.com/blog/beyond-s3-exposed-resources-on-aws

Summary of Findings

To help understand the magnitude of this problem, the following summarizes how many of each resource were found exposed to the internet.

- 116,386 public Elastic Block Store (EBS) snapshots from 3,213 accounts
- 373 public Relational Database Service (RDS) snapshots from 227 accounts
- 711,598 public Amazon Machine Images (AMIs) from 20,952 accounts
- 16,000 public IPs of exposed AWS managed ElasticSearch clusters that could have their contents stolen or data possibly deleted - this means 17% of AWS-managed ElasticSearch servers with public IPs were misconfigured

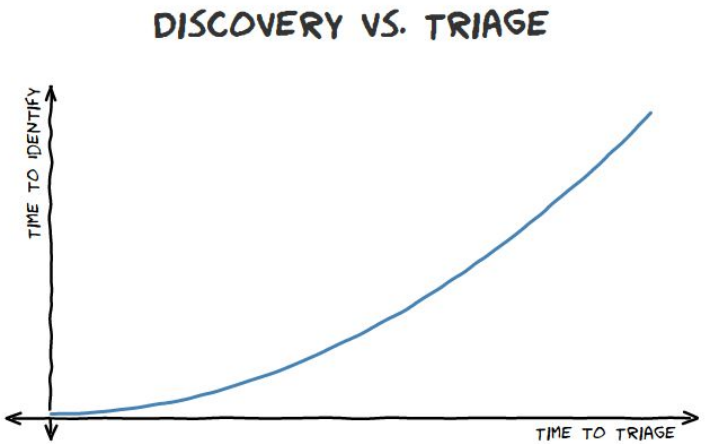
Vulnerability Management is

NOT a **Compliance**

Vulnerability Management is NOT Easy

Goals

Goals: Quick Identifications



Real Time Identification

The sooner you know of a vulnerability the better your chances to mitigate accordingly.

Reduce time of discovery

Goals: Quick Triaging of Issues

Fast Triage

You have to make critical decisions fast.
Blue teams do it, Vulns teams should too!

Goals: Starting Remediation

Mitigation and Remediation

You want to be able to mitigate, as soon as possible, taking in consideration business needs

Challenges

Multiple sources of Vulnerability Intelligence

Too many sources of data and “noise”.
Consume what you need, discard the rest

A Patch is not available or Patching is not always possible

What mitigation measures are at your disposal?
How about extra visibility and monitoring?

Common Vulnerability Scoring System (CVSS)

Standardized Rubric that can be useful for determining the impact of various vulnerabilities.

Don’t rely on it to make decisions, it’s a numerical score, useful, but you need **context!**

Don’t Accept Blindly for Triage.

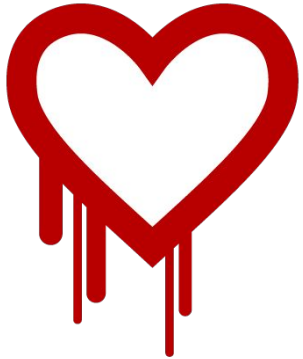
CVSS Context: Vuln Comparison

CVE-2014-0160 (Heartbleed)
SCORE v2: **5.0**

vs.

CVE-2017-0143,44,45,46 (Eternal Blue)
SCOREv3: **8.1**
SCOREv2: **9.3**

Which one affected your production environment more?

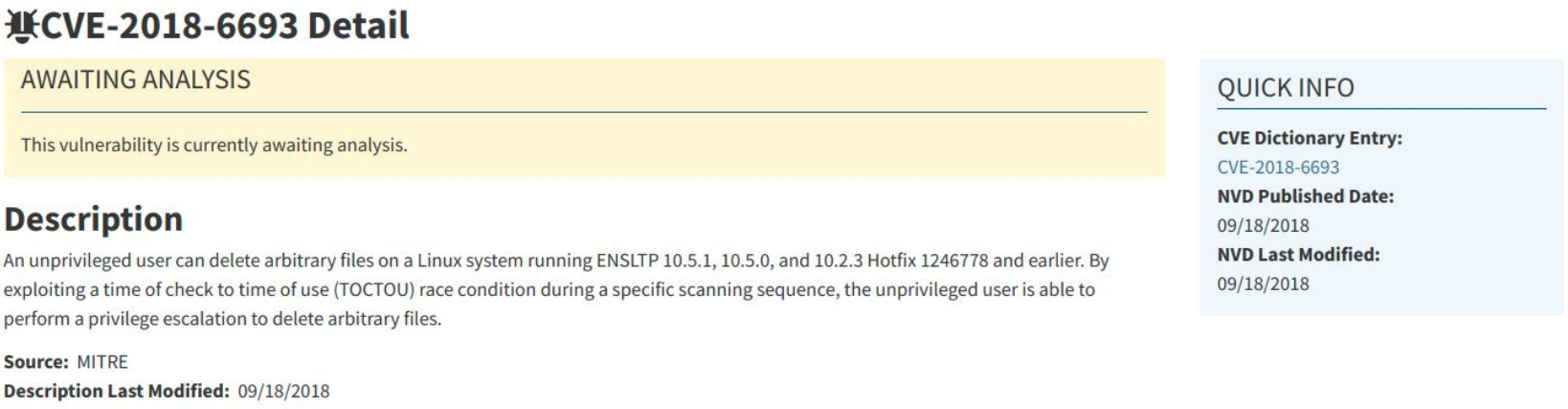


Context: Undisclosed Vulns

CVE-2018-6693 Example (ENSLTP on Linux Vuln)

Vulns can be partially disclosed. Where the fix may be out but things like details might not be disclosed yet or still under a Security Embargo.

How you handle this issue can be varied.



CVE-2018-6693 Detail

AWAITING ANALYSIS

This vulnerability is currently awaiting analysis.

Description

An unprivileged user can delete arbitrary files on a Linux system running ENSLTP 10.5.1, 10.5.0, and 10.2.3 Hotfix 1246778 and earlier. By exploiting a time of check to time of use (TOCTOU) race condition during a specific scanning sequence, the unprivileged user is able to perform a privilege escalation to delete arbitrary files.

Source: MITRE
Description Last Modified: 09/18/2018

QUICK INFO

CVE Dictionary Entry:
CVE-2018-6693
NVD Published Date:
09/18/2018
NVD Last Modified:
09/18/2018

Prerequisites

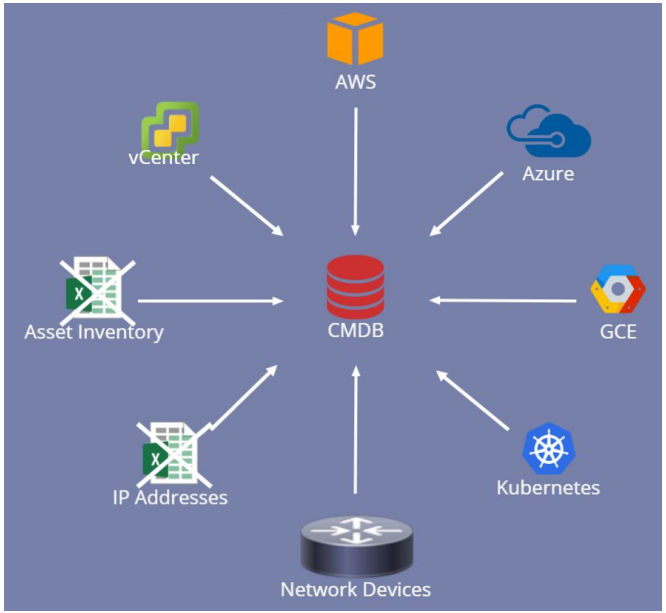
Know your assets

Comprehensive list of Assets

CMDB. Preferably not a spreadsheet.

Keeping IP ranges up-to-date

What are my organization IP blocks?
Are they current?
How about IPv6?



CMDBuild

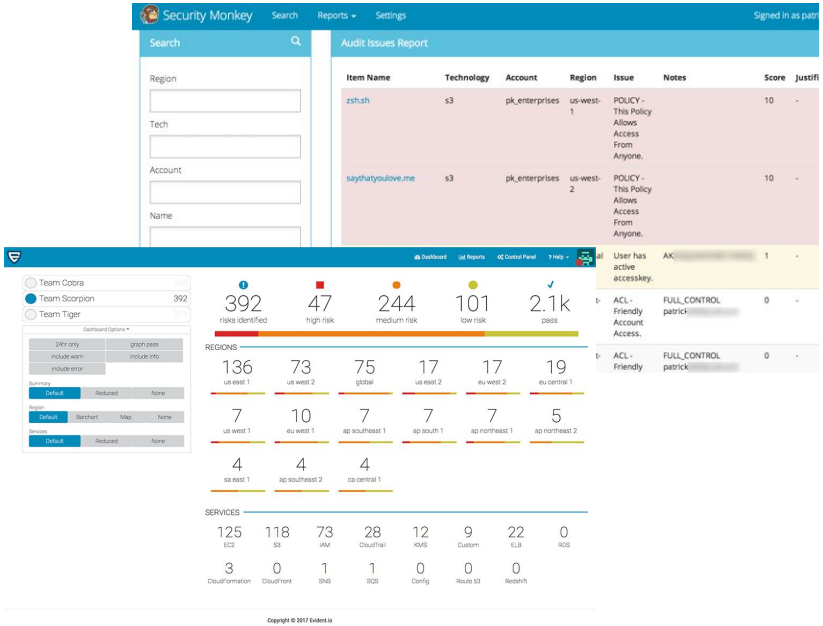
A CMDB for IT infrastructures (slides for AutomateIT² event)

ASSETS IN THE CLOUD

NETFLIX

Security Monkey

open source cloud security tracking system



The Cloud

Is the cloud at play?

Which providers?

Which environments?

What are the accounts?

Attribution

Very important for triage and remediation

Who owns asset $x?

Who do I contact?

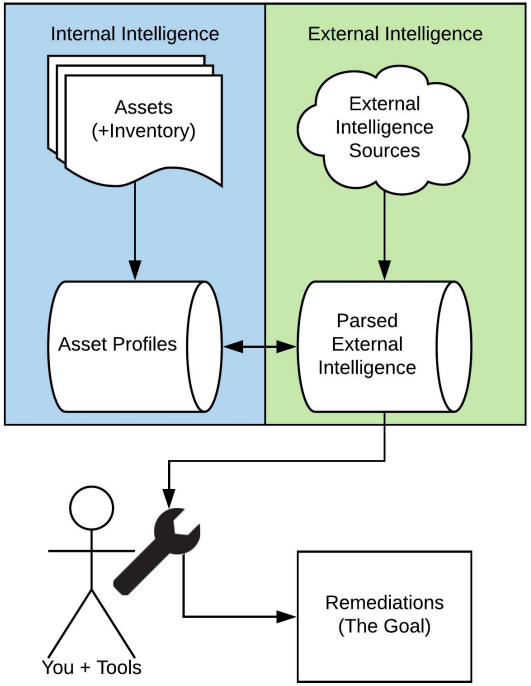
What about other records or accounts?

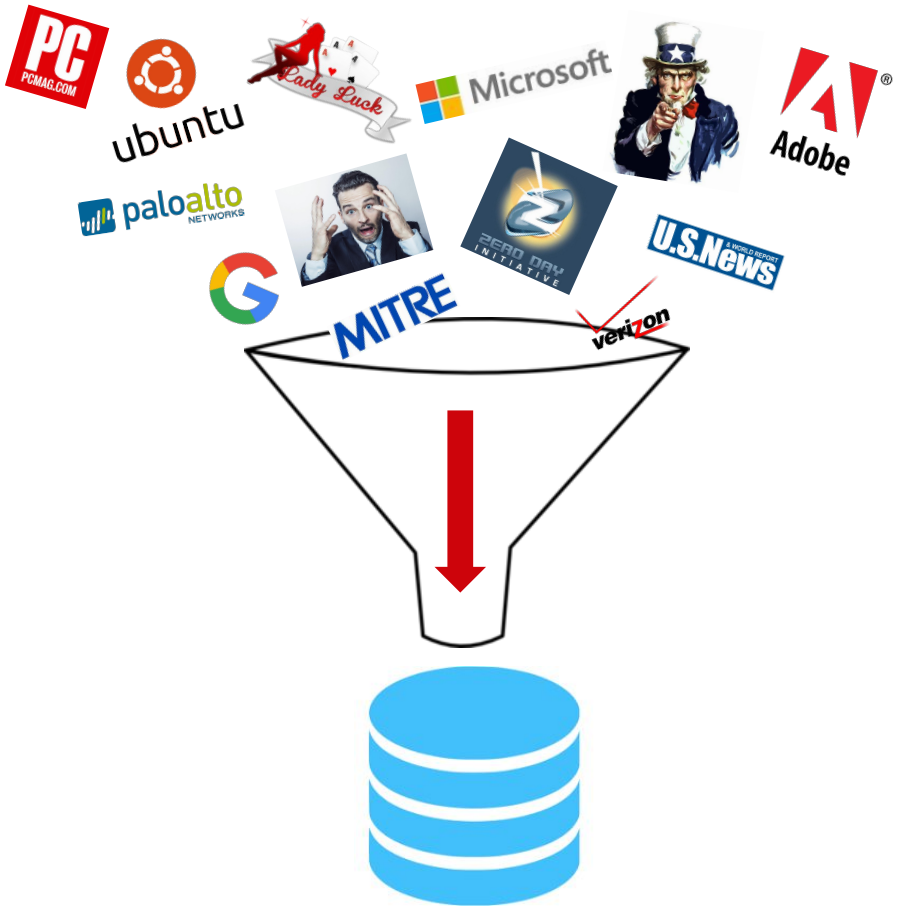
You'll never be the expert on everything. Lean on your teams.

Vuln Mgmt Theory

The General Theory of Vuln Management

- Use the combination of your internal and external intelligence to make decisions.
- Goal: Drive remediations of the issues you're vulnerable to.
- Largely you're going to say things like "go patch yourself".
- Sometimes you'll be asking more questions.
- Most important Rule: **Don't get Bogged Down!**





External Intelligence

It's a Dope Buzzword

Includes things like public CVEs, Blog Posts, Security Bulletins and other Security Info

Quality, be Picky

For your environment, focus on high signal to noise indicators, especially when starting.

Requires Parsing

While tools exist you'll likely need to parse this information to combine it with your Internal Intelligence

Internal Intelligence

Not a Buzzword, we Made it Up!

What do you know about your environment? When you ask questions this is what gives answers.

Accuracy + Quantity

You want to be able to see as much as you can with maximum accuracy. Decisions are made with this data.

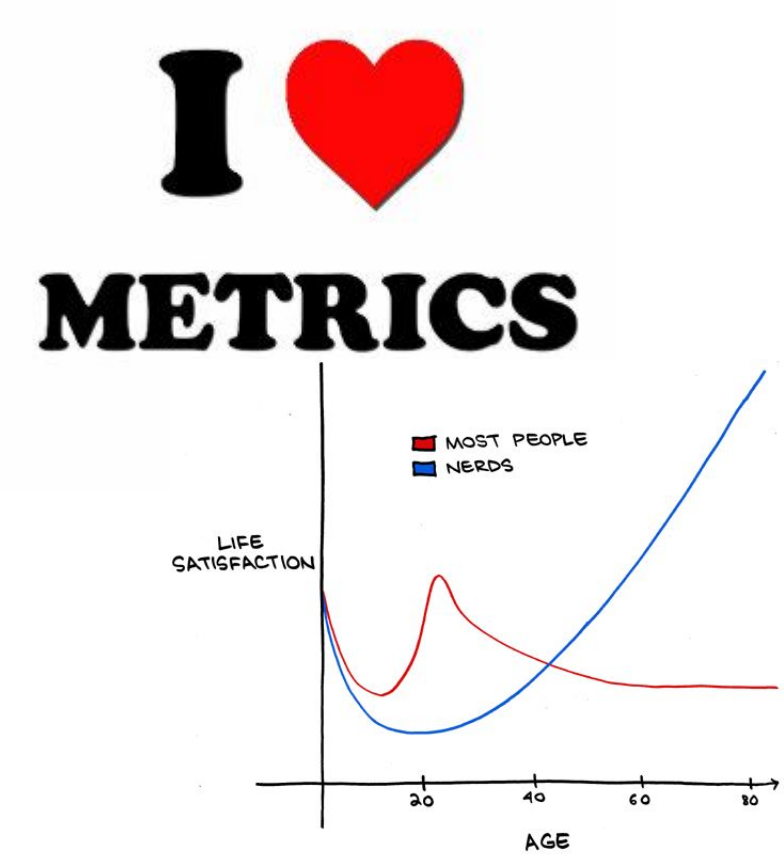
Integrations

This is where you'll build most of your integrations.

Internal Intelligence

Consider which internal tools can provide intelligence

- Discovery and Broadcast protocols (BOOTP, Windows Browser, etc)
- DHCP, DNS or AD Servers
- Network Devices (Switch, Router, Firewalls, etc)
- <Insert tool name> logs
- **Flow Data**
  - *Plenty of intelligence exploring flow data!*



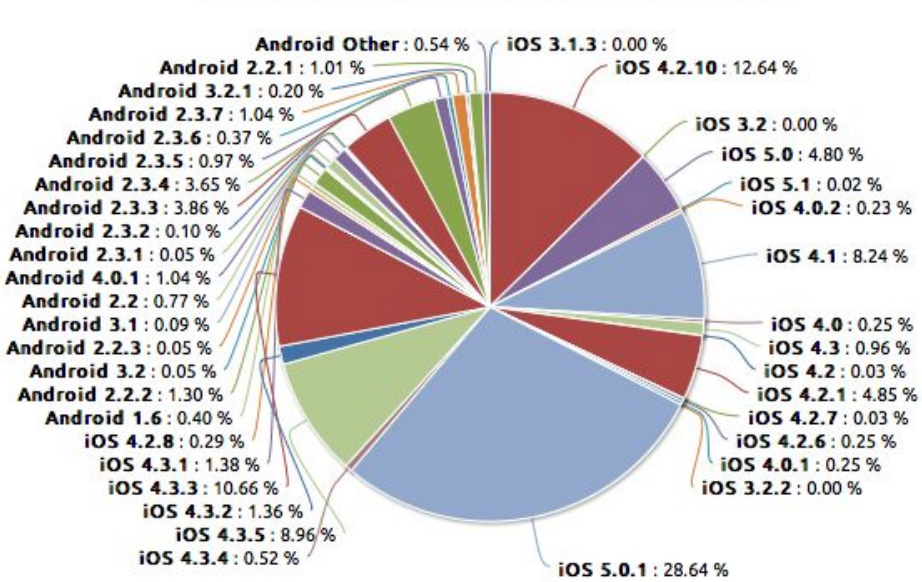
Metrics & Data

Collect Metrics
Metrics will help you figure out how your org is doing.

Data-Powered Reinforcement
Your actions are easier to justify with the data.

Graphs are Fun
I’m a Nerd, I’ll admit it.

Metrics & Data : Graphs



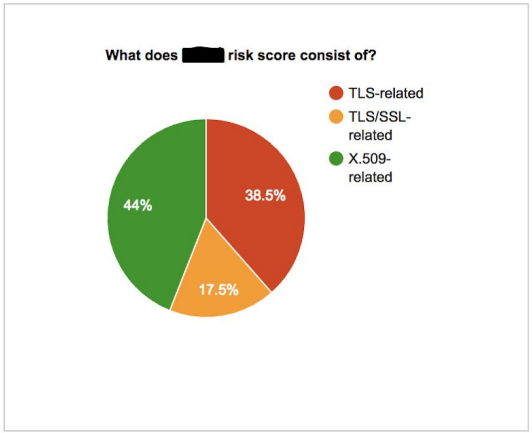
DON'T DO THIS

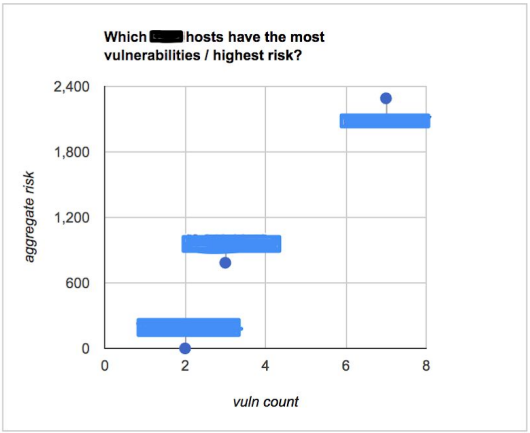
Keep in mind your audience

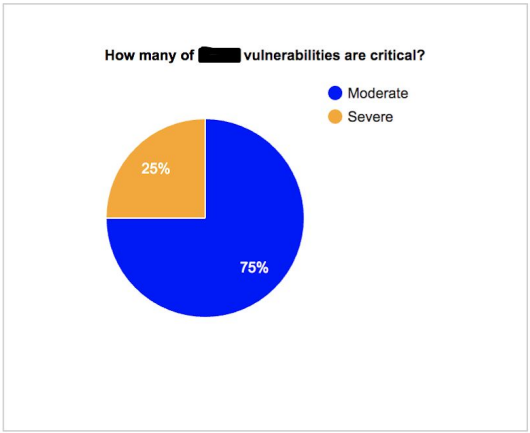
Does Management need X ?

Does it convey the right message?

Metrics & Data : Better Graphs







Make it simple

Less is more. Don’t try to put every single item on your charts !


TRIAGE

Triage : Prerequisites

Know your software stack

To be effective during triage, document your software stack. Don't waste time on things that don't impact

Get to know your environment

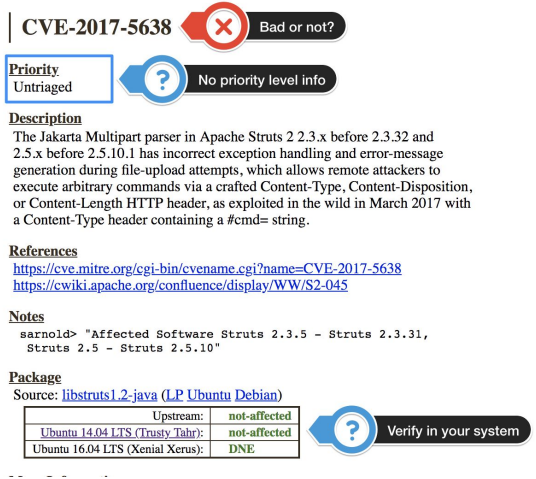
Get familiar with your applications and the architecture, it matters!

Triage : CVE Considerations

Again, don't rely blindly on CVSS Scores

Does this vulnerability impact your environment?

If so, how, where, what?



A remote attacker could possibly...

Is there a public exploit? How complex is the vulnerability?

Temporal and Environmental Scores Matter.

Know how this vuln affects your environment. The Temporal and Environmental Sections of CVSS3 can help objectify that risk.

Triage : Understanding your Vulnerability Data

Validate and verify your findings

Most scan tools use application and port banners to identify vulnerabilities. Validate the findings!

Did you actually connect to X service to confirm?

Does the version impacted match that of the one installed on the system?

Don’t make Big Triage Decisions on Unvalidated Data

Triage : With Friends

Build healthy partnerships with your Org. teams

Security is everyone's problem, be kind. You will need their help and they will need yours!

When in doubt, it’s not only OK to ask, you should!

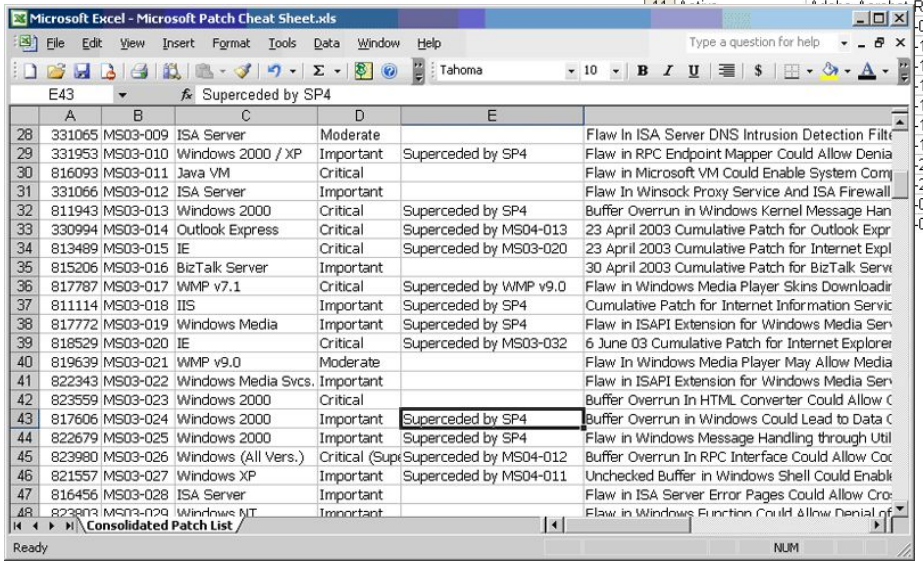
Reach out to your organization teams for answers. They are the subject matter expert!

Tools

Toolset : The Basics

Your trusty: Spreadsheet

	A	B	C	D	E
1	#Status	Patch Name	Impact	Patched C	Not Patche
2	Active	Adobe Acrobat Reader 6.0.2 update	Critical	0	0
3	Active	Adobe Acrobat Reader 6.0.3 Update	Critical	0	0
4	Active	Adobe Acrobat Reader 6.0.4 Update	Critical	0	0
5	Active	Adobe Acrobat Reader 6.0.5 Update	Critical	0	0
6	Active	Adobe Acrobat Reader 6.0.6 Update	Recommended	0	0
7	Active	Adobe Acrobat Reader 7.0.1 Update	Critical	0	0
8	Active	Adobe Acrobat Reader 7.0.2 Update	Critical	0	0
9	Active	Adobe Acrobat Reader 7.0.5 Update (SEE NOTES)	Critical	0	0
10	Active	Adobe Acrobat Reader 7.0.7 Update (SEE NOTES)	Critical	0	0
		Reader 7.0.8 (Update) (Rev 4)	Critical	0	0
		-07 Dreamweaver Server Behavior SQL Injection vulnerability	Critical	0	0
		-12 Flash Player 9.0.r47 for FireFox (Upgrade) (All Languages)	Critical	0	0
		-12 Flash Player 9.0.r47 for IE (Upgrade) (All Languages) (Rev 3)	Critical	0	2
		-12 Flash Player 9.0.r47 for IE (Upgrade) (All Languages) (Rev 3)	Critical	0	0
		-12 Flash Player 9.0.r47 for Netscape (Upgrade) (All Languages) (Rev 2)	Critical	0	0
		-12 Flash Player 9.0.r47 for Netscape (Upgrade) (All Languages) (Rev 2)	Critical	0	0
		-13 Photoshop CS3 Update for Windows	Critical	0	0
		-20 Flash Player 9.0.r115 for IE (Upgrade) (All Languages)	Critical	0	0
		-20 Flash Player 9.0.r115 for IE (Upgrade) (All Languages)	Critical	0	2
		-01 Contribute CS3 update FLVPlayer_Progressive.swf file for Windows	Critical	0	0
		-01 Dreamweaver CS3 update FLVPlayer_Progressive.swf file for Windows	Critical	0	0



	A	B	C	D	E	
28	331065	MS03-009	ISA Server	Moderate		Flaw In ISA Server DNS Intrusion Detection Filt
29	331953	MS03-010	Windows 2000 / XP	Important	Superceded by SP4	Flaw in RPC Endpoint Mapper Could Allow Denia
30	816093	MS03-011	Java VM	Critical		Flaw in Microsoft VM Could Enable System Com
31	331066	MS03-012	ISA Server	Important		Flaw In Winsock Proxy Service And ISA Firewall
32	811943	MS03-013	Windows 2000	Critical	Superceded by SP4	Buffer Overrun in Windows Kernel Message Han
33	330994	MS03-014	Outlook Express	Critical	Superceded by MS04-013	23 April 2003 Cumulative Patch for Outlook Expr
34	813489	MS03-015	IE	Critical	Superceded by MS03-020	23 April 2003 Cumulative Patch for Internet Expl
35	815206	MS03-016	BizTalk Server	Important		30 April 2003 Cumulative Patch for BizTalk Serve
36	817787	MS03-017	WMP v7.1	Critical	Superceded by WMP v9.0	Flaw in Windows Media Player Skins Downloadir
37	811114	MS03-018	IIS	Important	Superceded by SP4	Cumulative Patch for Internet Information Servic
38	817772	MS03-019	Windows Media	Important	Superceded by SP4	Flaw in ISAPI Extension for Windows Media Serv
39	818529	MS03-020	IE	Critical	Superceded by MS03-032	6 June 03 Cumulative Patch for Internet Explorer
40	819639	MS03-021	WMP v9.0	Moderate		Flaw In Windows Media Player May Allow Media
41	822343	MS03-022	Windows Media Svcs.	Important		Flaw in ISAPI Extension for Windows Media Serv
42	823559	MS03-023	Windows 2000	Critical		Buffer Overrun In HTML Converter Could Allow C
43	817606	MS03-024	Windows 2000	Important	Superceded by SP4	Buffer Overrun in Windows Could Lead to Data C
44	822679	MS03-025	Windows 2000	Important	Superceded by SP4	Flaw in Windows Message Handling through Util
45	823980	MS03-026	Windows (All Vers.)	Critical (Supe	Superceded by MS04-012	Buffer Overrun In RPC Interface Could Allow Coc
46	821557	MS03-027	Windows XP	Important	Superceded by MS04-011	Unchecked Buffer in Windows Shell Could Enabl
47	816456	MS03-028	ISA Server	Important		Flaw in ISA Server Error Pages Could Allow Cro
48	823803	MS03-029	Windows NT	Important		Flaw in Windows Function Could Allow Denial of

Extremely useful when working with new data.

Tooling : About Network Scanning

Discovery Scan Strategies

Start small, use a simple port list or the most common, TCP

Use results to *augment* your inventory data, validate, repeat, win!

Do **NOT** engage in vulnerability scans until you have reviewed discovery data

Firewalls and fragile devices

Remember, you can get data (host, service, OS) from other sources (flow, bro, etc.), use it!

Courtesy of Alejandro Hernández
@nitr0usmx

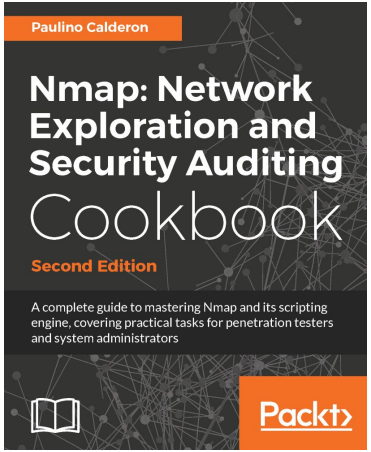
Toolset : More on Network Scanning

Authenticated or Unauthenticated Scans

Do you really, **really**, need authenticated scans?
Have you tuned, reviewed, and validated your scan templates?
Keep your templates up-to-date!

Secure your scanning infrastructure!

IPv6 - Network Reconnaissance in IPv6 Networks
https://tools.ietf.org/html/rfc7707



Toolset : Ongoing Considerations

Technology is constantly changing
Are your tools still effective?

Find the tools that work for you
Evaluate the tools your organization has, can any of those tools be reused? Can you adapt them accordingly?

Before you introduce new tools
Make sure the basic requirements of your program are covered first, unless these new tools complement it

Toolset : Approach

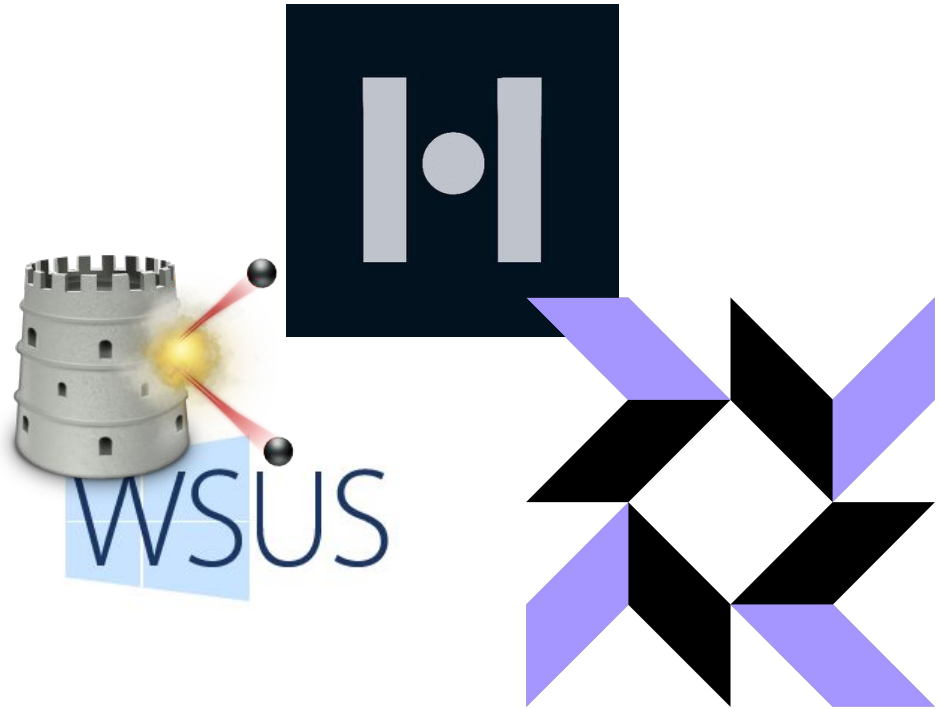
Avoid the “one tool fits all” mentality.

No need to reinvent the wheel

Plenty of awesome Open Source tools out there

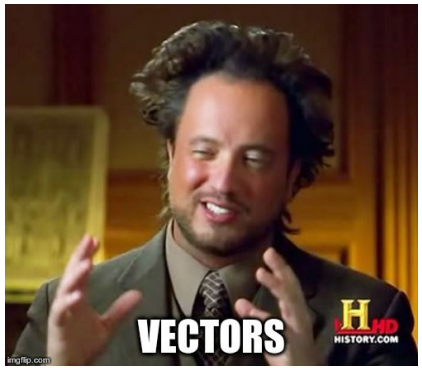
Tooling : Internal Intelligence Options

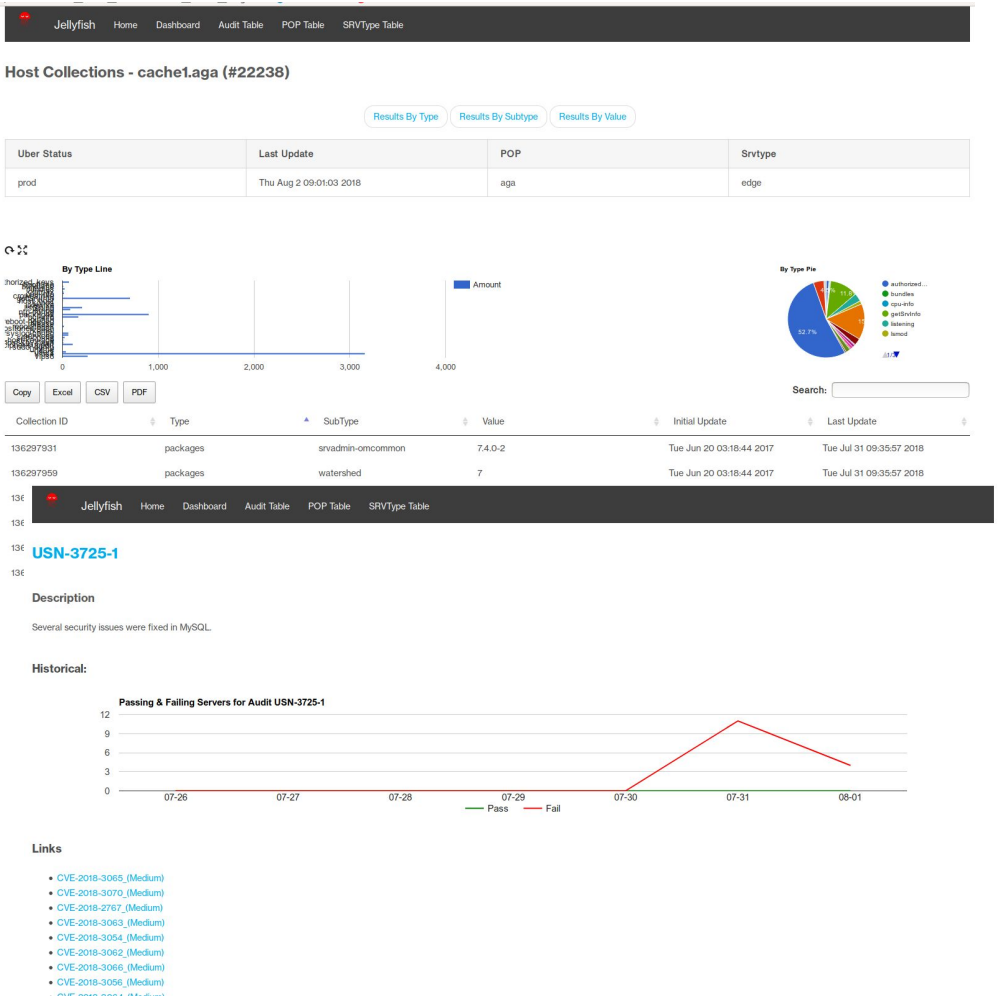
- Lots of Potential Tooling:
  - HubbleStack
  - Katello and RH Satellite
  - OSQuery
  - Lynis
  - YASAT
  - Zeus
  - WSUS (Windows)
- Evaluate your needs and build, buy, combine or modify to suit them.
- There is no Ring of Power.



MAN O' WAR

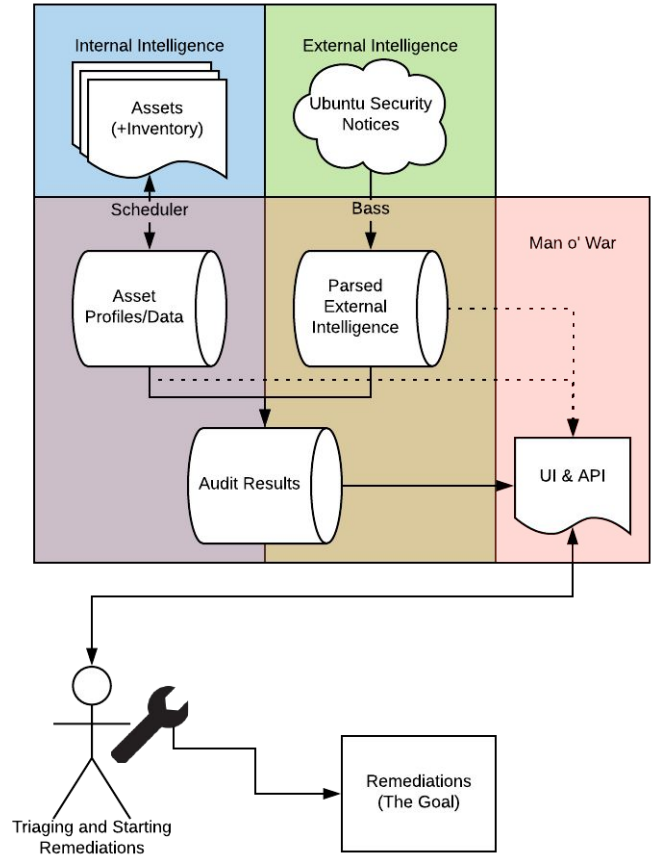
- BSD Licensed Internal Intelligence System we Wrote
- Link
- One of a Number of tools you could use.
- Missing some helper tools (haven't got them opened yet).





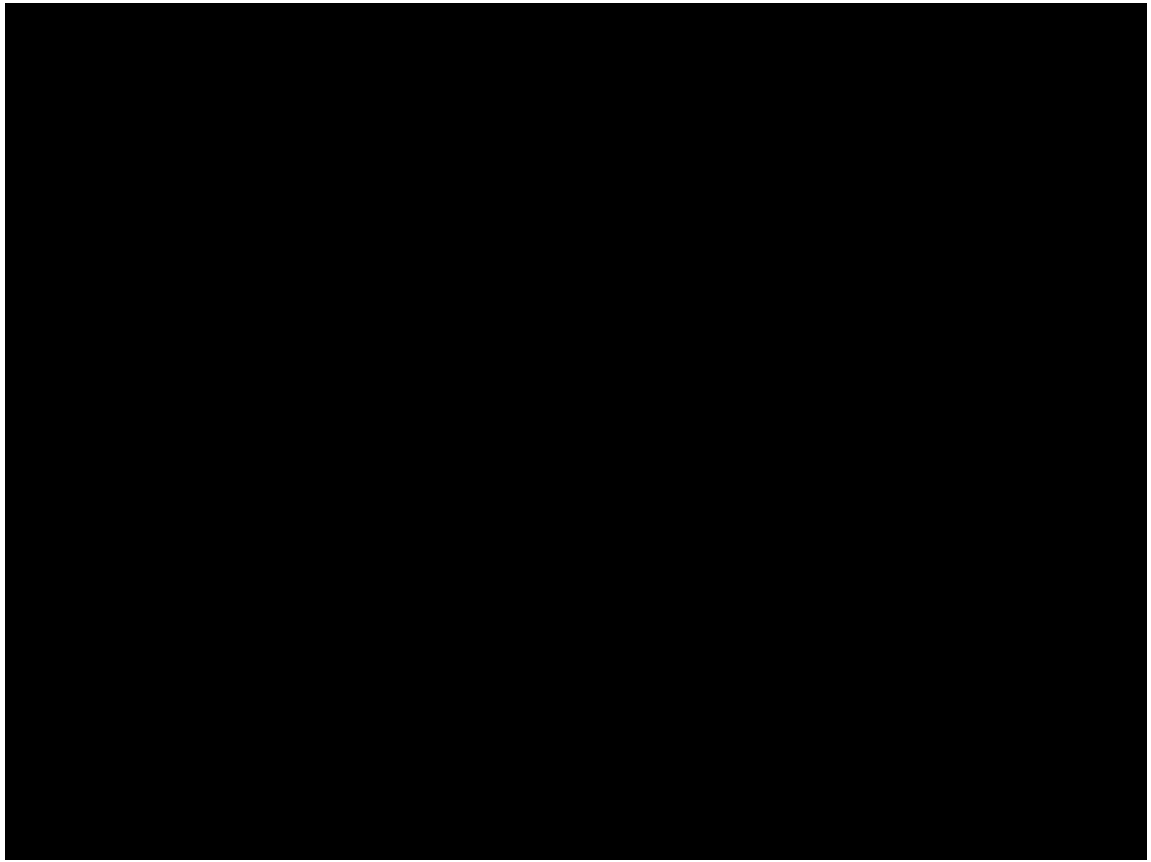
Man o' War - Theory Tie In

- Helps you manage internal and external intelligence sources.
- Parses and checks your external intel into valid comparisons.
- Provides a friendly(ish) way to access the data in question.



Man o' War - Demo Agenda

- Going to take you through an example of triaging.
- Start with the Upstream vulns.
- Show how it profiles.
- Show Auditing
  - Using Example USN-3765-1 a recent Curl Vuln
- Show some “unstructured” Investigation Data Available
- Conclusions



Backup Demo Video


Remediation
and
mitigation

Interacting With The Org - Two Paths

Work Assignment

- Sometimes you gotta “Cut Tickets” to the asset owners to fix things.
- You get/have to be the bad guy sometimes here.
- **Try to Avoid a “Shame Culture”.**

Self-Service

- Present your findings as accurately as you can to your org. Think Dashboards.
- If the culture works, teams will “self-resolve” issue you find.
- Data **Accuracy is important here.** False positives lower trust in your team.

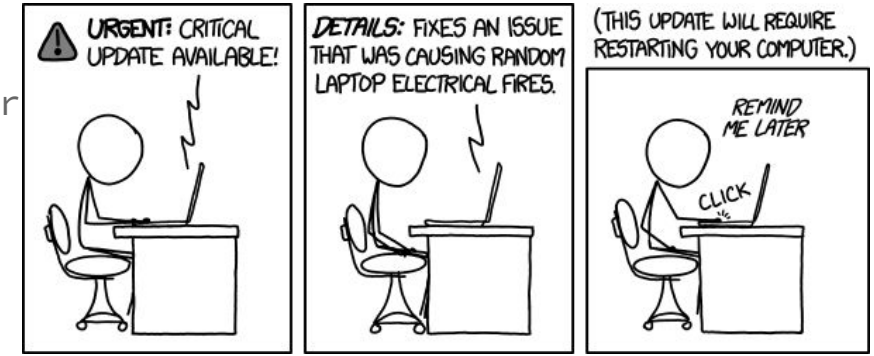
Remediation or Mitigation

Patching Capabilities

What are your current capabilities?
How fast can you deploy x patch?
How accurately can you validate proper patch installation?

You may not be able to patch

What mitigation controls are available?



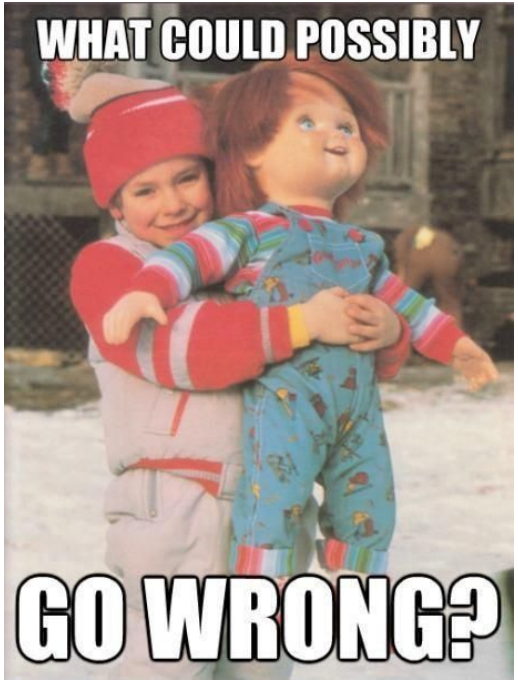
Decision Documentation

Document decisions

The organization may need to take drastic decisions, make sure they are documented!

Pitfalls

When things go wrong



One day, things will go (very) bad

- Don’t panic!
- Don’t blame or shame
- Conduct lessons learned.
  Apply, improve, repeat. Iterations!

Next Level IDeas

Gamify Remediation Efforts

Vulnerability and remediation score board

Consider it if you are already providing self service vulnerability data, make it fun.

May not work in your organization!

Everyone loves Swag!

Courtesy of www.customink.com

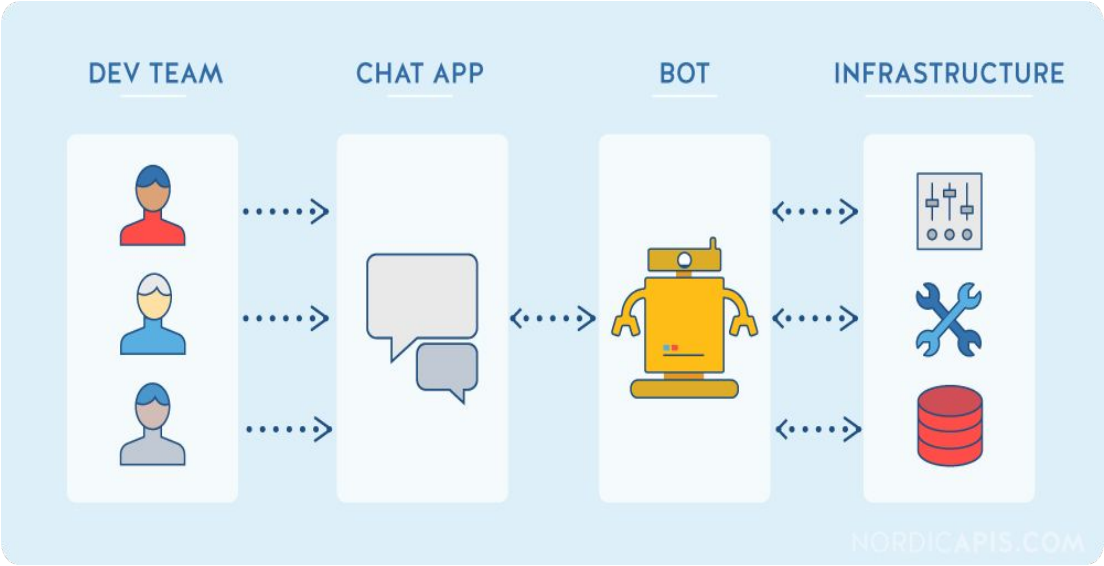
Automation

Automate your goals

Orchestration and ChatOps opportunities

Be cautious

Secure your pipeline!



Courtesy of www.addteq.com

Bug bounty

Be ready for some serious work

If you don’t have the proper prerequisites (as discussed earlier) Don’t do it!

How NOT to Measure your Program Success

Final Notes & Takeaways

Don’t Shame

When In Doubt, Ask

Don’t Blindly Trust Upstream Scoring

Validate Your Data

Improve Incrementally (OODA)

Don’t Get Bogged Down

Questions ?

Additional Resources

Resources Links:

- Toolset 2.0 Additional Tools!
  - https://goo.gl/Vut2pm
- Link to Slides
  - To Be Posted