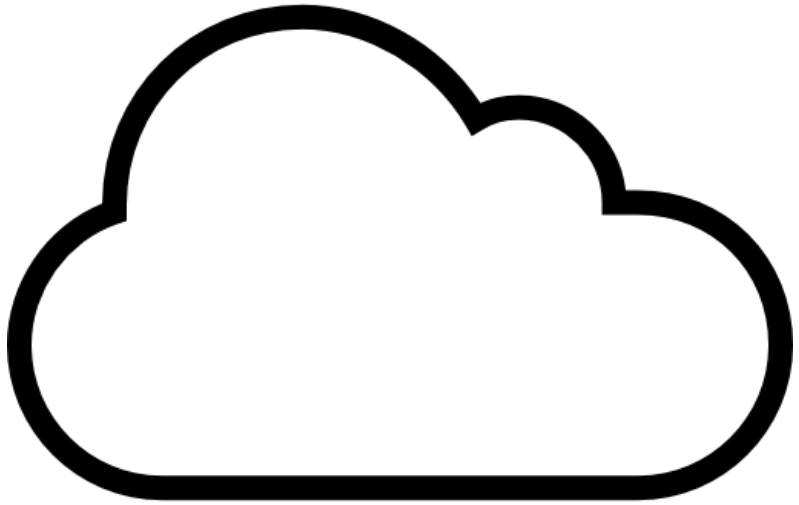
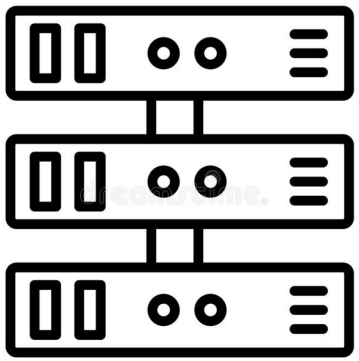
On the Theory and Practice of Vulnerability Remediation

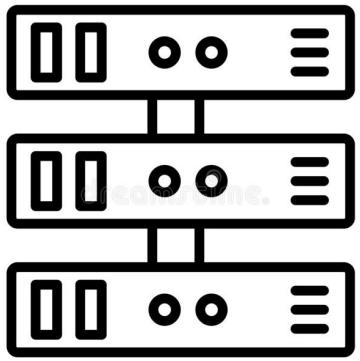
Ariana Mirian
University of California, San Diego
April 26, 2023

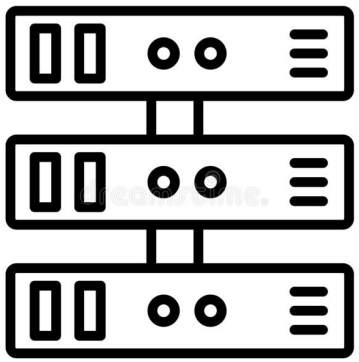
Many organizations have moved infra to the cloud

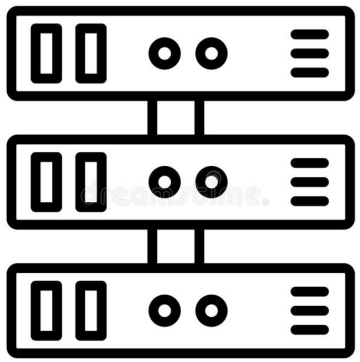


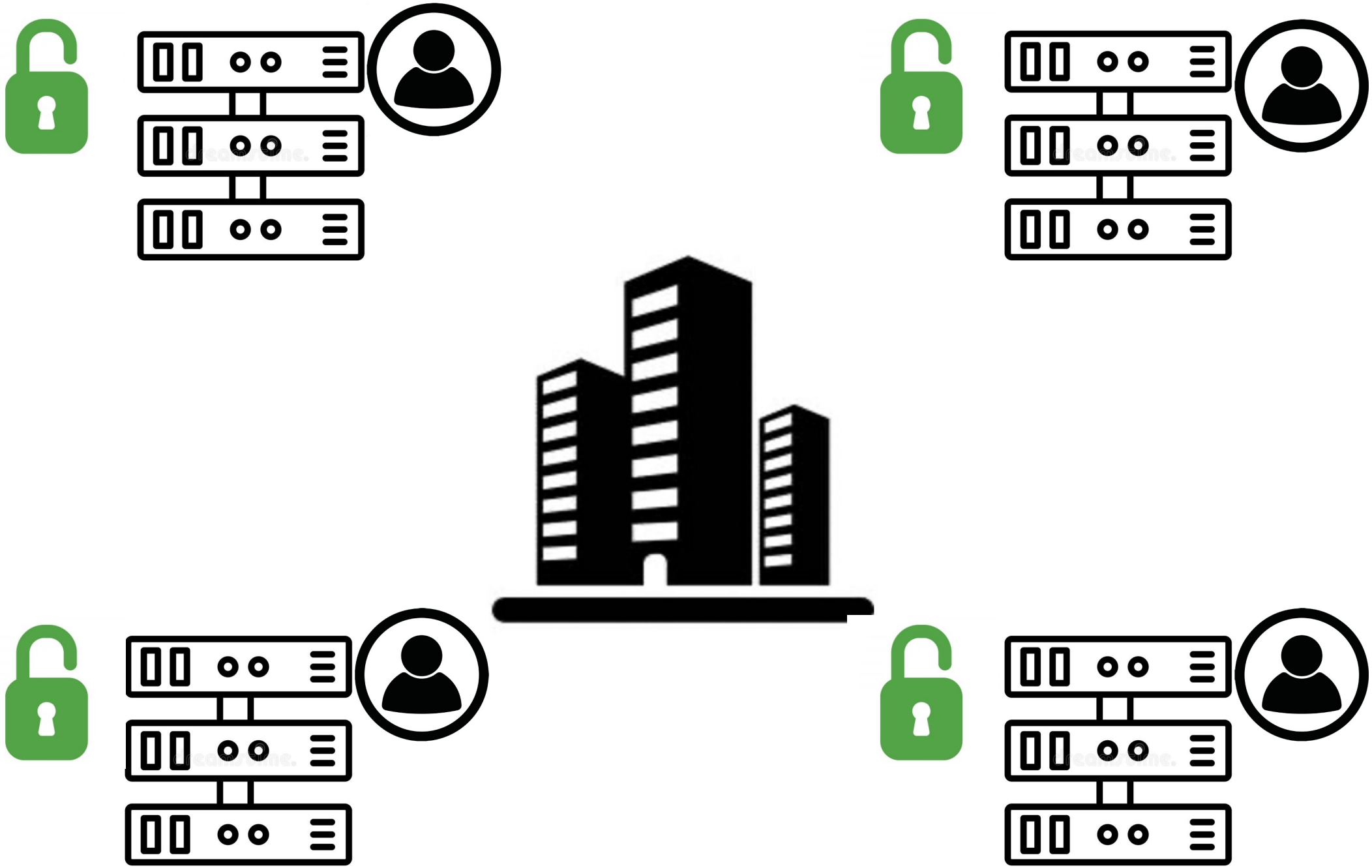
But there are many orgs with legacy machines

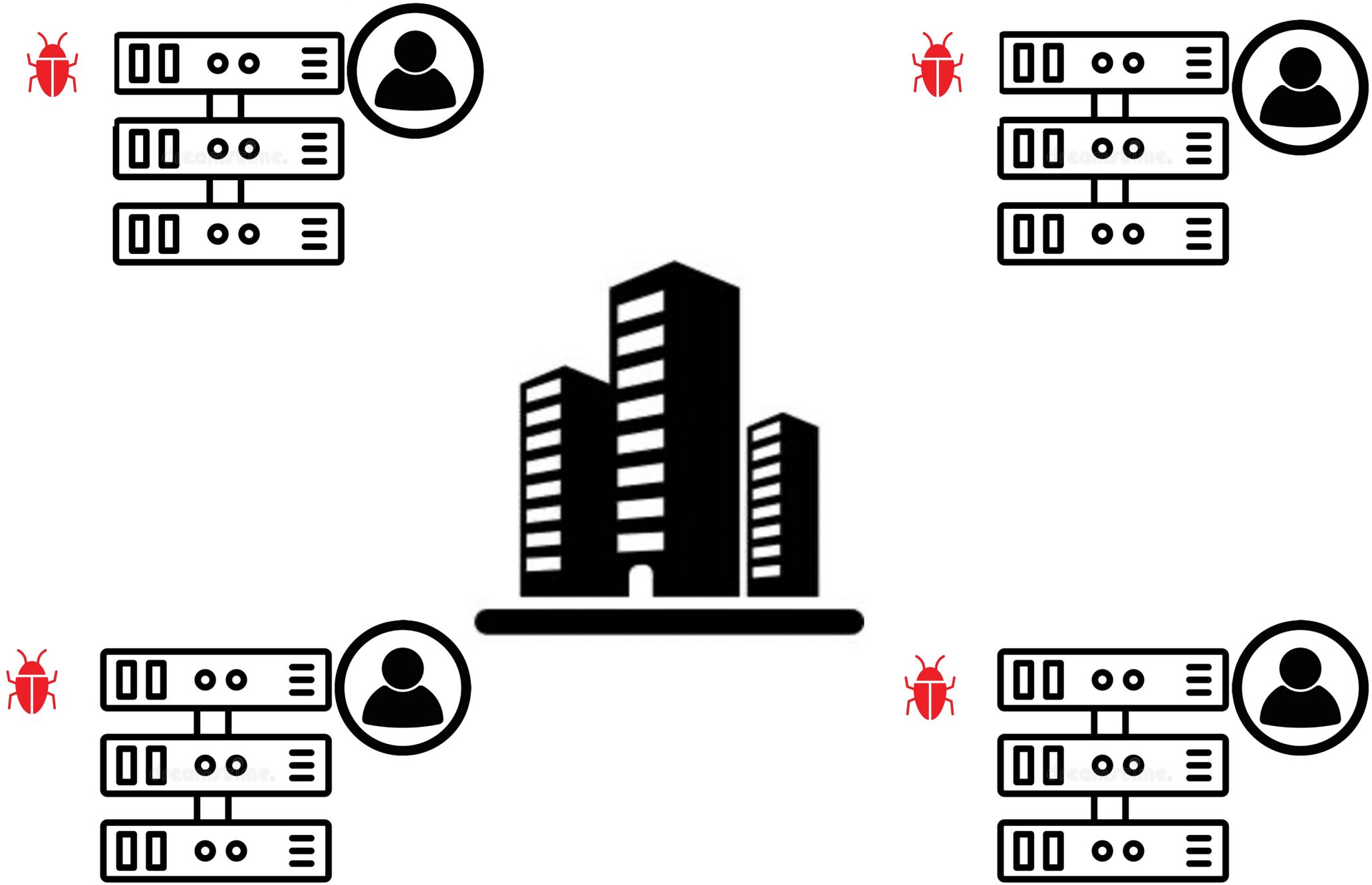












Patching isn’t a new problem, but it persists

What if we tune the process for the human?

How can we make patching a more effective process?

The systems below have active critical (Sev5) and/or high (Sev4) vulnerabilities.

ITS servers are expected to have critical vulnerabilities patched within 24 hours of discovery and high vulnerabilities within 7 business days of discovery or they may be removed from the network. For each system you manage, we have provided the hostname, IP address, severity counts, the age of the oldest vulnerability, and the date it was last detected by Qualys. You have 1 vulnerable host(s). This list is limited to 100 systems of the highest risk.

To review vulnerabilities and create reports for your systems, please review the Collab page to request access to Qualys Security and Compliance Suite: https://collab.ucsd.edu/x/MjpQC.

To update asset metadata, such as contact information, please review the Collab page: https://collab.ucsd.edu/x/TQ7WC.

For any system you are unable to patch within the prescribed window, a patching exemption must be completed. This form can be found here: https://ucsd.kualibuild.com/app/builder/#/app/613beee664209d734d3bd053/run.

Please attend to these promptly.

Technical_Contact	Host_Count	Hostname	IP_Address	Sev5	Sev4	Oldest	Last_Detected
[redacted]	1	[redacted]		1	8	45 day(s)	2022-06-27

The systems below have active critical (Sev5) and/or high (Sev4) vulnerabilities.

ITS servers are expected to have critical vulnerabilities patched within 24 hours of discovery and high vulnerabilities within 7 business days of discovery or they may be removed from the network. For each system you manage, we have provided the hostname, IP address, severity counts, the age of the oldest vulnerability, and the date it was last detected by Qualys. You have 1 vulnerable host(s). This list is limited to 100 systems of the highest risk.

To review vulnerabilities and create reports for your systems, please review the Collab page to request access to Qualys Security and Compliance Suite: https://collab.ucsd.edu/x/MjpQC.

To update asset metadata, such as contact information, please review the Collab page: https://collab.ucsd.edu/x/TQ7WC.

For any system you are unable to patch within the prescribed window, a patching exemption must be completed. This form can be found here: https://ucsd.kualibuild.com/app/builder/#/app/613beee664209d734d3bd053/run.

Please attend to these promptly.

Technical_Contact	Host_Count	Hostname	IP_Address	Sev5	Sev4	Oldest	Last_Detected
[redacted]	1	[redacted]		1	8	45 day(s)	2022-06-27

Old notification was not ideal

Did not list vulnerabilities or additional details

Required system admins to perform extra steps to get necessary information

Adds an amount of friction in order to execute

There are Microsoft Windows Security Update vulnerabilities across 3 system(s) that you manage. A list of the vulnerabilities is attached to this email. Please help make our online community at UCSD safer by following these remediation steps. If you have any follow up questions or thoughts, please feel free to reply back to this email.

If you have patched this system before, please use that method. For further guidance, refer to the information below.

If using a Windows client machine, using the graphical interface:
Windows 11: click on Start > Settings > Windows Update > Check for updates.
Windows 10: click on Start > Settings > Update & Security > Windows Update> Check
Windows 8: click on Settings >Change PC settings>Update and recovery>Windows Update>Check now

If you manage a Windows server, follow these instructions for finding the KB (listed in the attached CSV) on the Microsoft Catalog website and importing it into WSUS for patching:
https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/manage/wsus-and-the-catalog-site#the-microsoft-update-catalog-site

You can verify this by visiting https://support.microsoft.com/en-us/windows/windows-update-faq-8a903416-6f45-0718-f5c7-375e92dddeb2 or by searching for "Microsoft Windows Security Update" or "Microsoft WSUS" in your search engine (e.g. Google, DuckDuckGo, Bing).

There are Microsoft Windows Security Update vulnerabilities across 3 system(s) that you manage. A list of the vulnerabilities is attached to this email. Please help make our online community at UCSD safer by following these remediation steps. If you have any follow up questions or thoughts, please feel free to reply back to this email.

If you have patched this system before, please use that method. For further guidance, refer to the information below.

If using a Windows client machine, using the graphical interface:
Windows 11: click on Start > Settings > Windows Update > Check for updates.
Windows 10: click on Start > Settings > Update & Security > Windows Update> Check
Windows 8: click on Settings >Change PC settings>Update and recovery>Windows Update>Check now

If you manage a Windows server, follow these instructions for finding the KB (listed in the attached CSV) on the Microsoft Catalog website and importing it into WSUS for patching: https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/manage/wsus-and-the-catalog-site#the-microsoft-update-catalog-site

You can verify this by visiting https://support.microsoft.com/en-us/windows/windows-update-faq-8a903416-6f45-0718-f5c7-375e92dddeb2 or by searching for "Microsoft Windows Security Update" or "Microsoft WSUS" in your search engine (e.g. Google, DuckDuckGo, Bing).

How do we make patching a more efficient process?

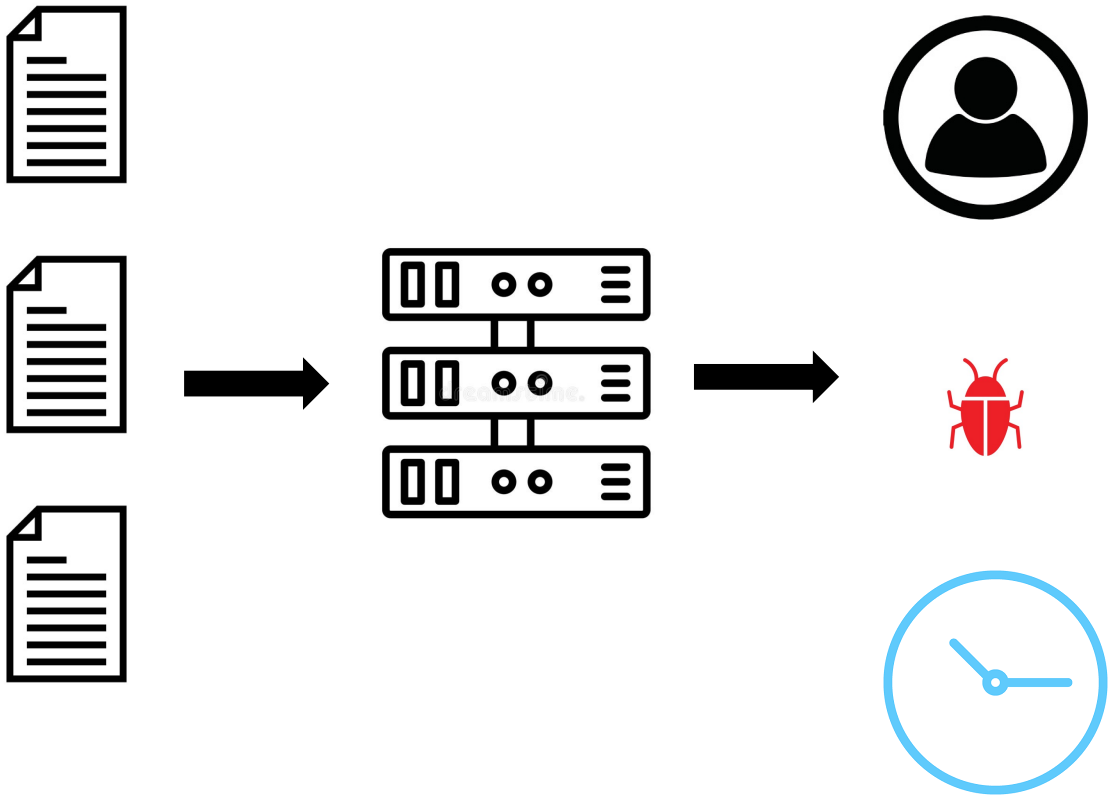
Examined old notification

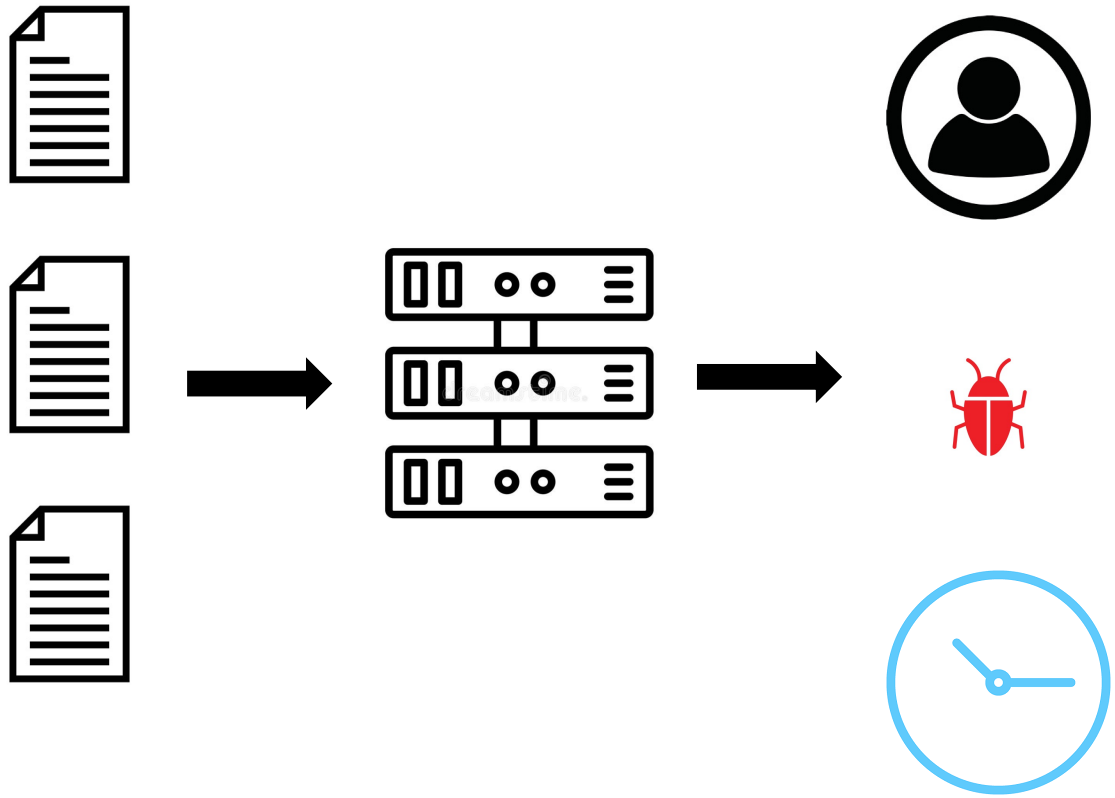
- Propose changes to reduce effort and time from system administrators

Craft new notifications

- Actionable items
- Focus on one vulnerability
- List all machines and the vulnerability type in an attached CSV

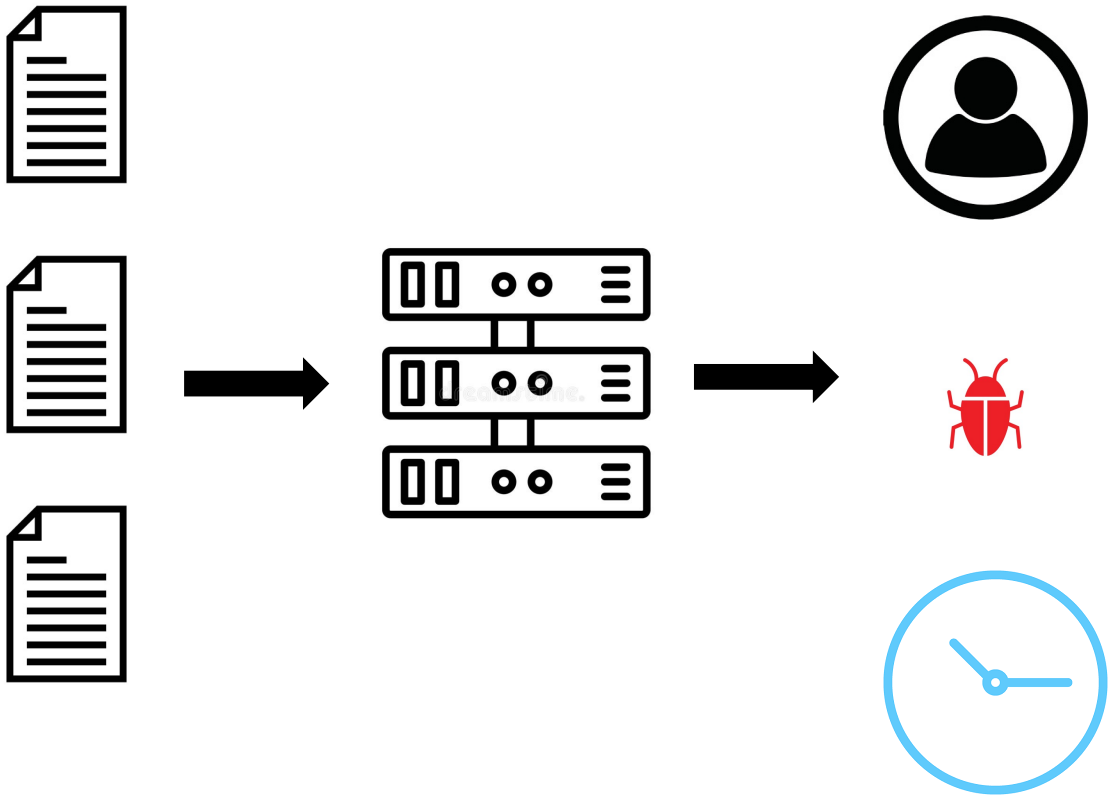
Analyze subsequent data

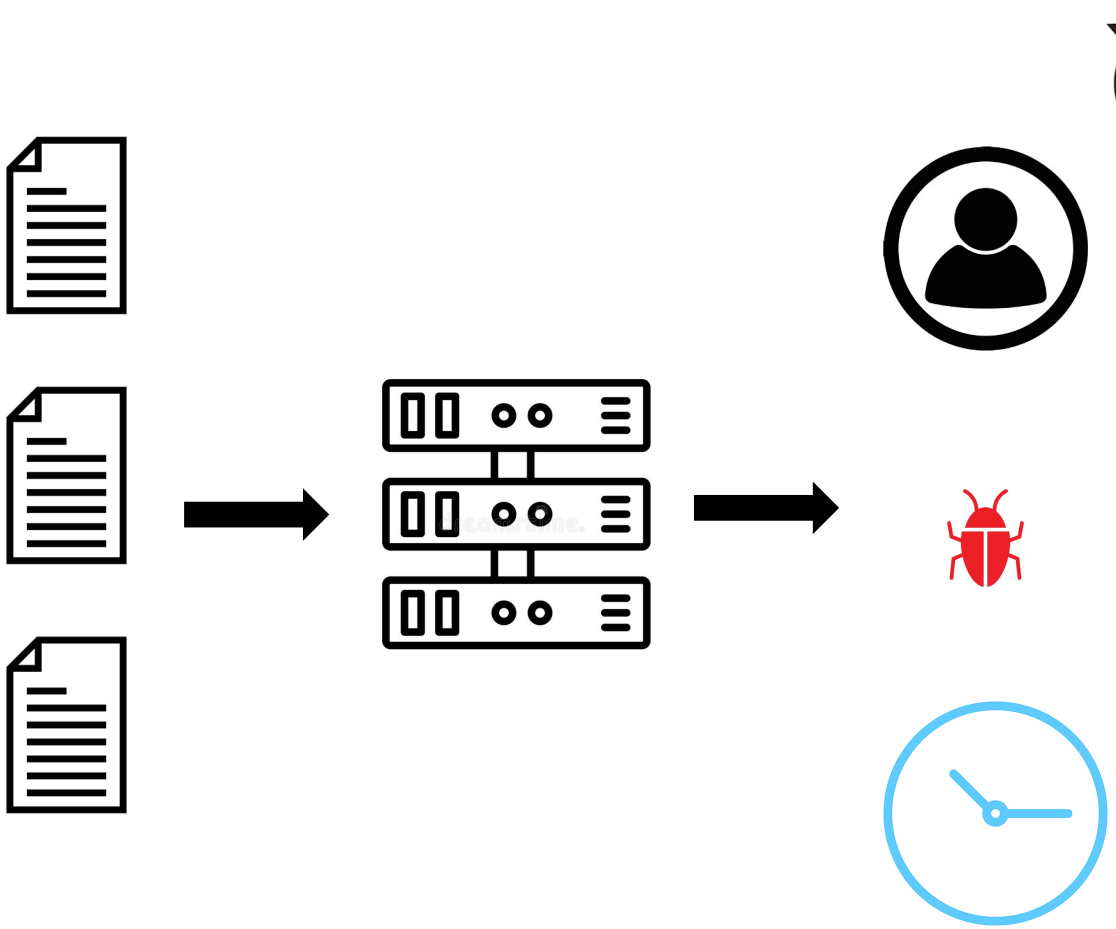




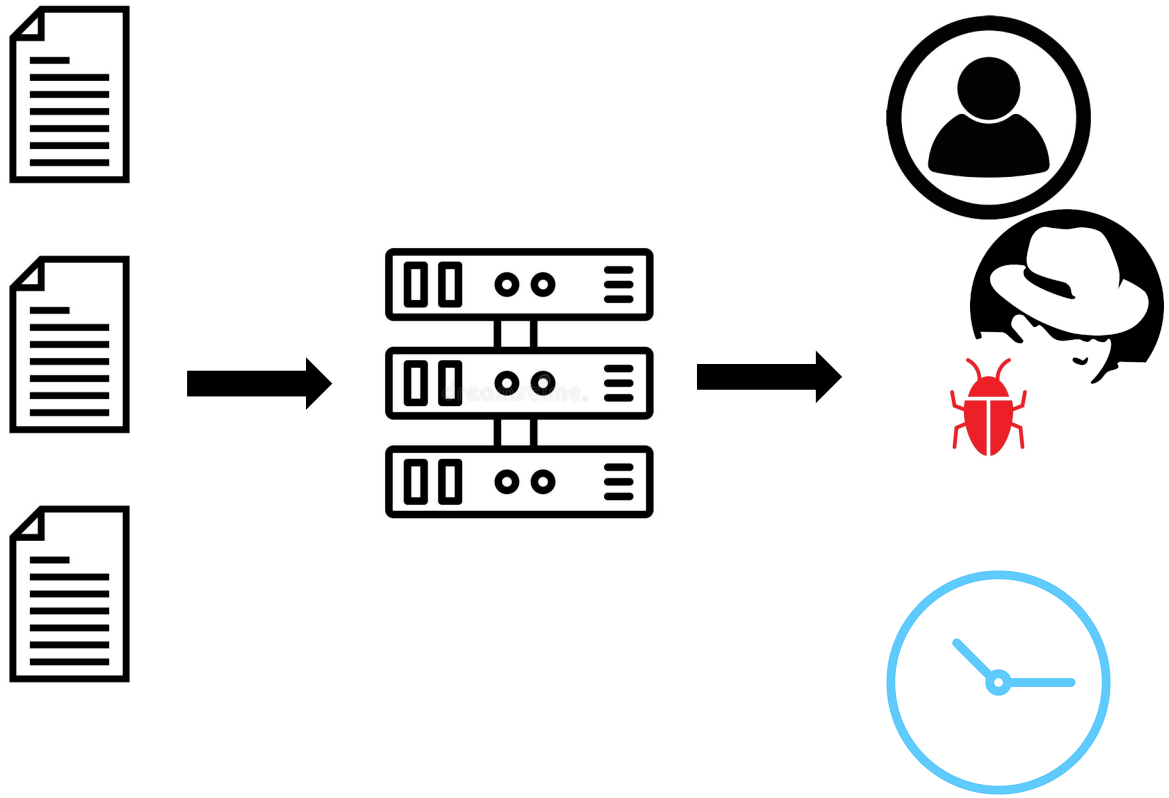
Increase from 3% patching to 78%

Why was the patch rate ONLY at 78%?



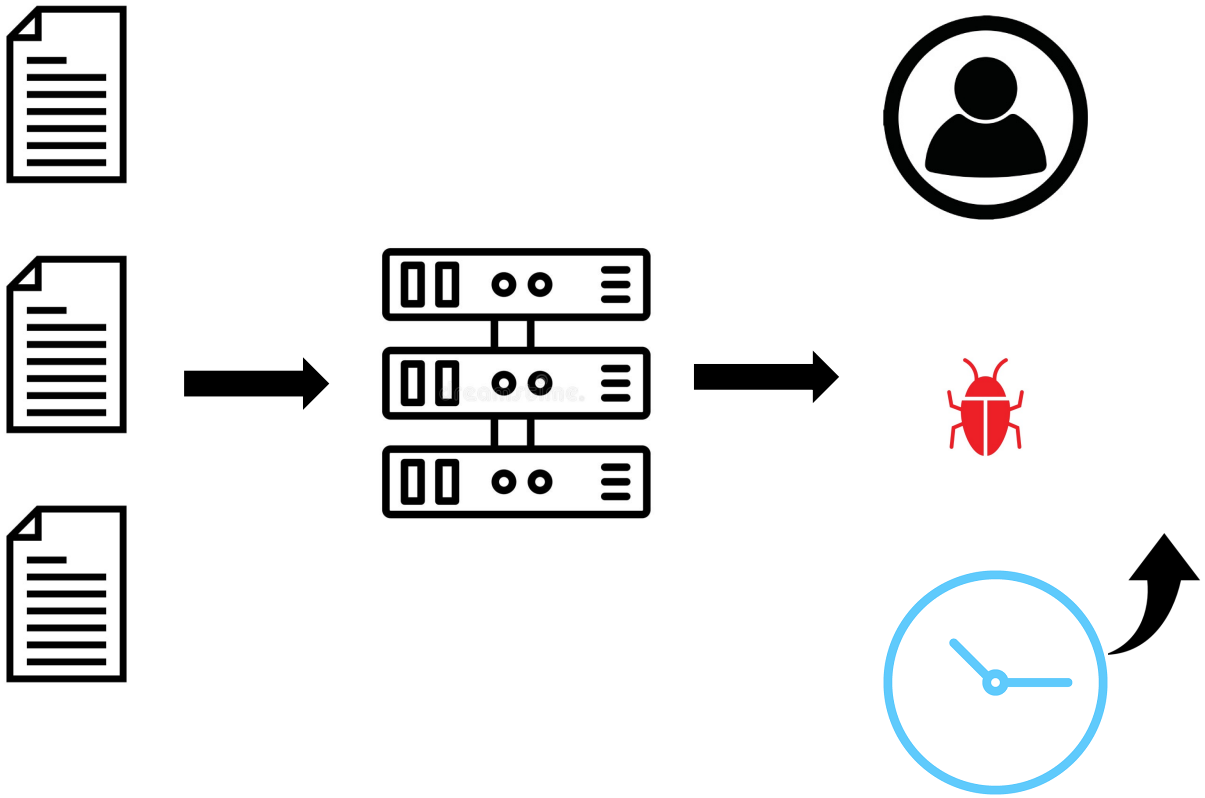


Some contacts are much better at patching



Some contacts are much better at patching

Certain vuln families get patched more

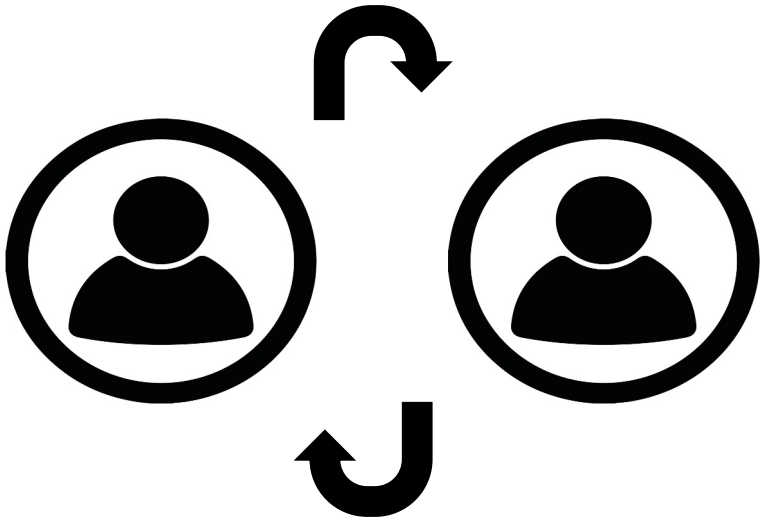


Some contacts are much better at patching

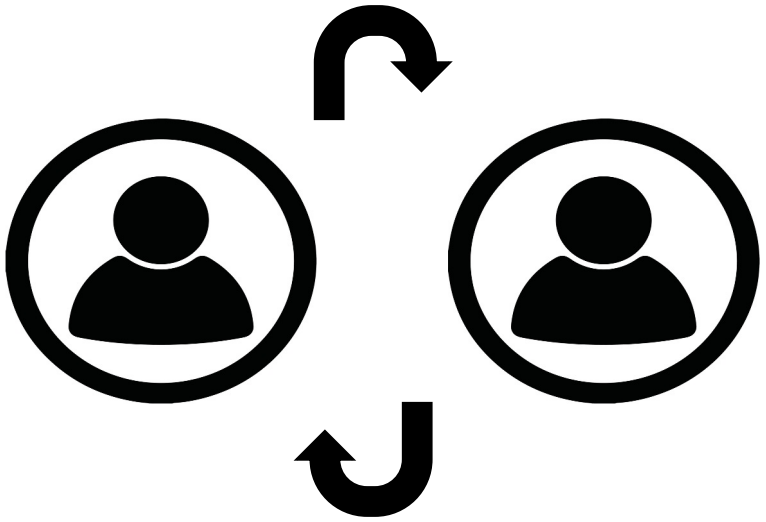
Certain vuln families get patched more

Some vuln families take more time to patch

Conducted semi-structured interviews with system administrators to add qualitative view to quantitative data



Conducted semi-structured interviews with system administrators to add qualitative view to quantitative data

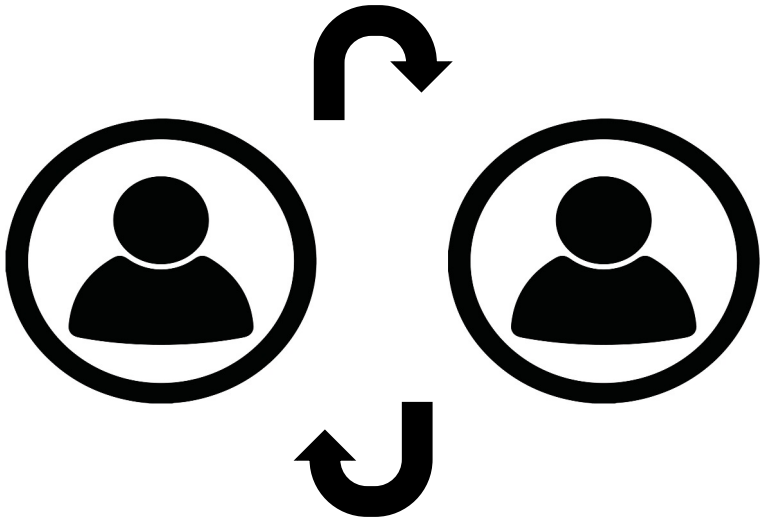


Monotonicity of email made it easy to ignore

Many teams have exceptions

Notifications fall outside of their patch cycle

Conducted semi-structured interviews with system administrators to add qualitative view to quantitative data



Positive sentiment towards new notification

Room for improvement/better integrations

Increasing efficacy of patching

Applied basic principles to reduce work for sys admins

Increase patch rate from 3% to 78%

Interviews found positive sentiment towards new notification, and discrepancies in different systems

Questions?

arianamirian.com

arianamirian28@gmail.com

@arimirian

@amirian@infosec.exchange

On the Theory and Practice of Vulnerability Remediation

Ariana Mirian
University of California, San Diego
April 26, 2023