

DIY

Patch Management

FLORIAN JUNGE (@SHANTYCODE)

INGO BENTE (@INGOBENTE)

BSIDES MUNICH 2018



Patching

Isn't that solved?



Nope, it's not.

REMEMBER THOSE RANSOMWARE NEWS IN 2017?



https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

Example WannaCry

- WannaCry hit the world on May 12 2017
- It spread via a vulnerability called EternalBlue
- EternalBlue was fixed by Microsoft on March 14 2017

Example WannaCry

- WannaCry hit the world on **May 12 2017**
- It spread via a vulnerability called EternalBlue
- EternalBlue was fixed by Microsoft on **March 14 2017**



2 months between patch and outbreak

I.E. YOU CAN WORRY LESS ABOUT ODAYS :)



Patching is hard

AT LEAST IN MANY REAL WORLD SCENARIOS.



But why?

I MEAN IT WORKS ON OUR FAMILY MEMBERS COMPUTERS, TOO.



Constraints

LEGACY: END OF LIFE OS THAT IS NOT PATCHABLE.



Constraints

AVAILABILITY: HOW TO REBOOT THAT HYPERVISOR CLUSTER?



Constraints

MONEY: IT WORKS WITHOUT THE PATCH, DOESN'T IT?



So what now?

LET'S TAKE A GLIMPSE INTO OUR WORLD.



SinnerSchrader Ecosystem



In a world where ...

- N tenants
- M tech stacks
- N x M requirements



In a world where ...

- Heterogenous infrastructure
- OS-wise mostly Debian and Ubuntu
- Packed into VMs and Containers
- Yes, there is also some serverless stuff :)



In a world where ...

Inconsistent patch management

NEVER, SOMETIMES, REGULARLY.



In a world where ...

Commercial scanners?

NO BUDGET. WE ARE NOT THAT ENTERPRISY.

Lessons learned ... so far

- Installation is easy
- Patching is hard
- Knowing when to patch is even harder



Not cool

SO WE WANTED TO CHANGE THAT.

Solution - the easy part


- Manually scan for all the CVEs
- Automate CVE scans (i.e. daily)
- Gather all the logs

Solution - the tricky part

- Dashboard everything
- Get metrics that CXOs can understand
- Take action (i.e. patch) and check the metrics
- Lean back ... for now



Building blocks

- 
- CVE scanner to audit VMs
 - Integration to config management
 - Central logging and dashboarding

Spot the vuln - the audit

- Vulnerability databases
- Vulnerability scanner
- Vulnerability subscriptions
- Freemium pricing model
- Nice people :)



Spot the vuln - the audit

- nmap plugin
- Burp plugin
- getsplloit
- API



Spot the vuln - CVE scanner

- Get installed packages
- Audit each for CVEs
- Get CVSS scores



Demo

VULNERS.COM API

Orchestration via config management

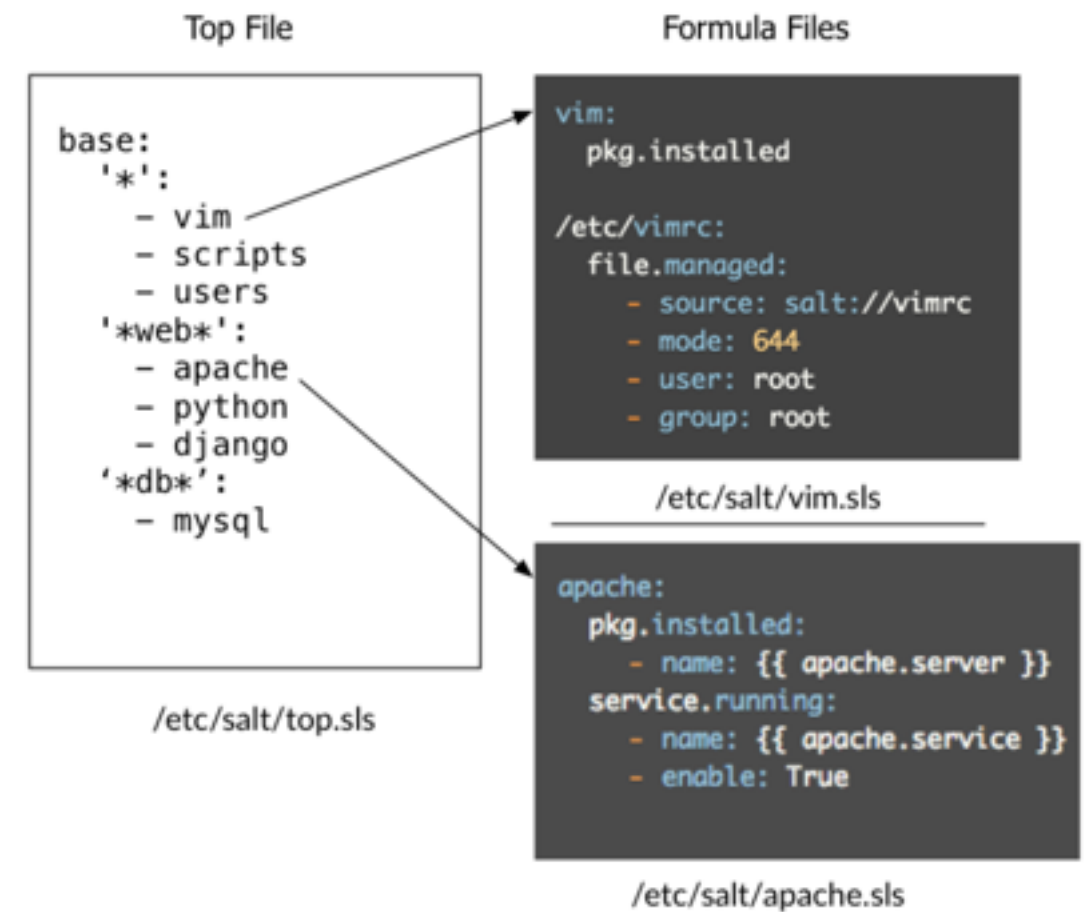
- Do it!
- Our solution: SaltStack
- Codify your update strategy



<https://docs.saltstack.com/en/getstarted/overview.html>

Orchestration

- Define systems with formula
- Minion matching
- Template engine



<https://docs.saltstack.com/en/getstarted/overview.html>

Three patch management flavours

- Unattended upgrades
- Orchestrated updates
- Patch Day



https://en.wikipedia.org/wiki/Neapolitan_ice_cream

Centralized Logging

- **E**lasticsearch
- **L**ogstash
- **K**ibana

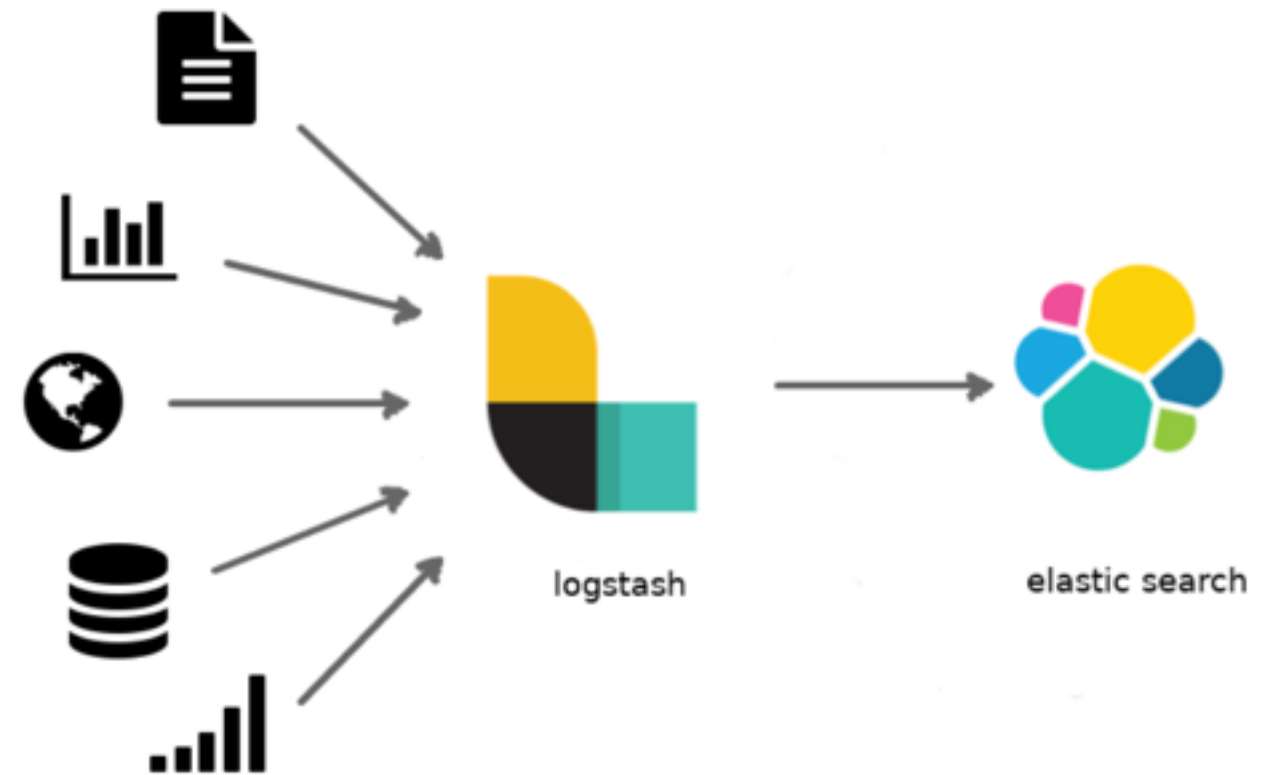
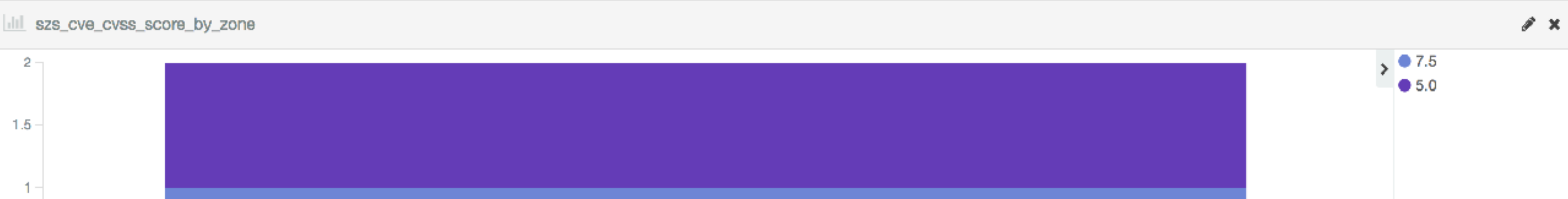
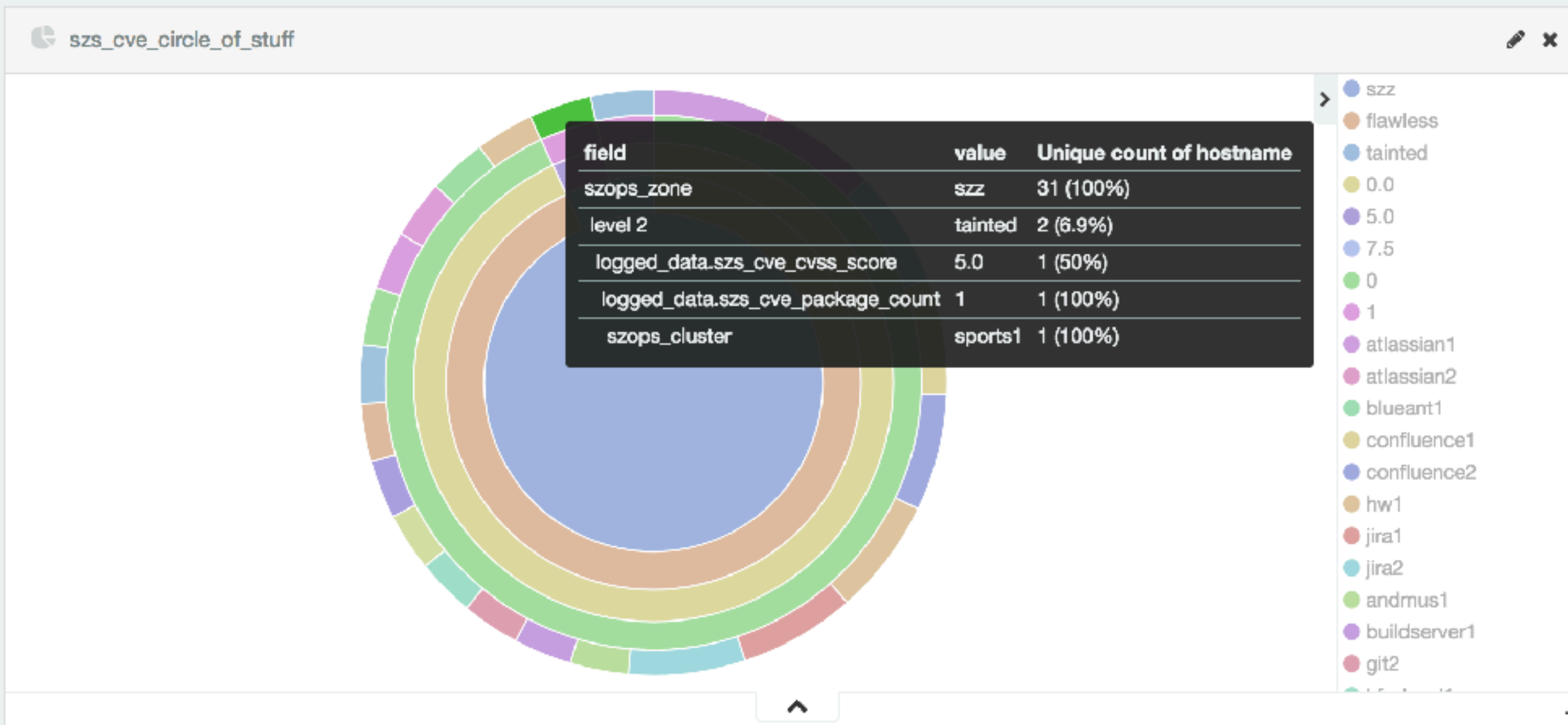
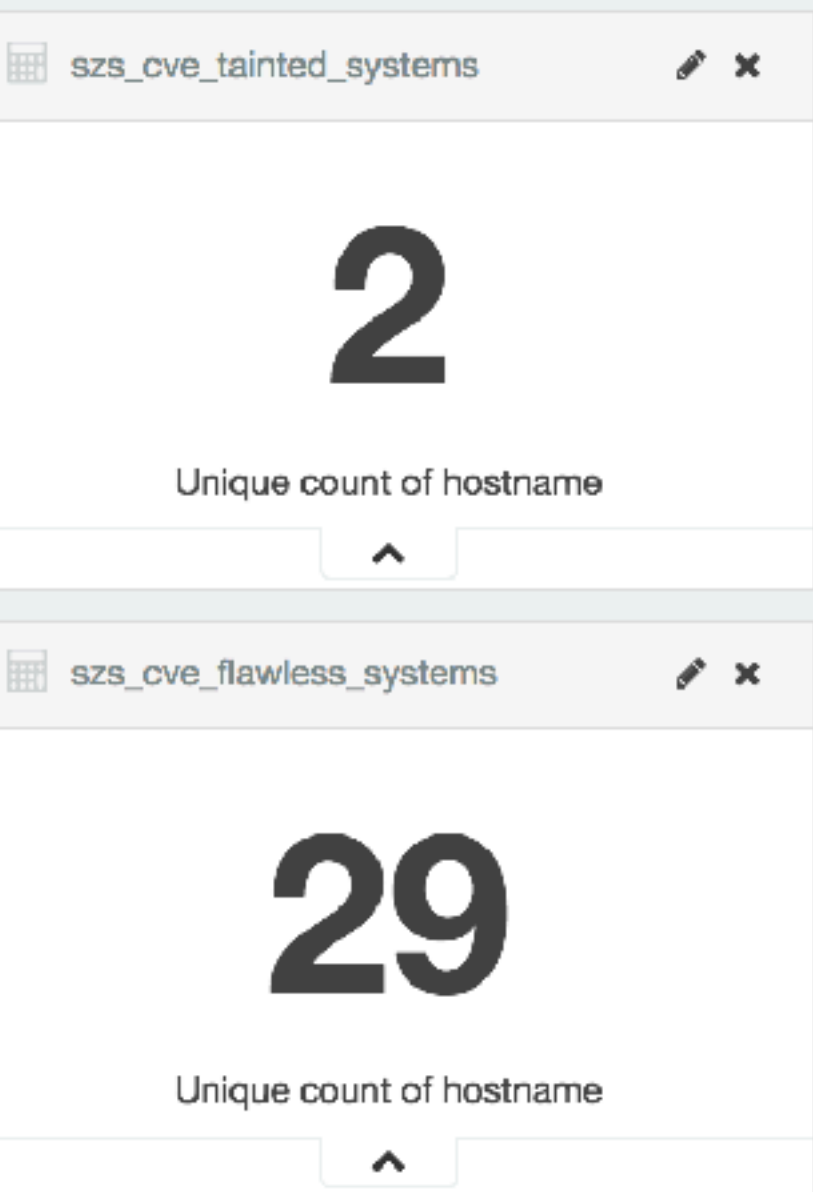


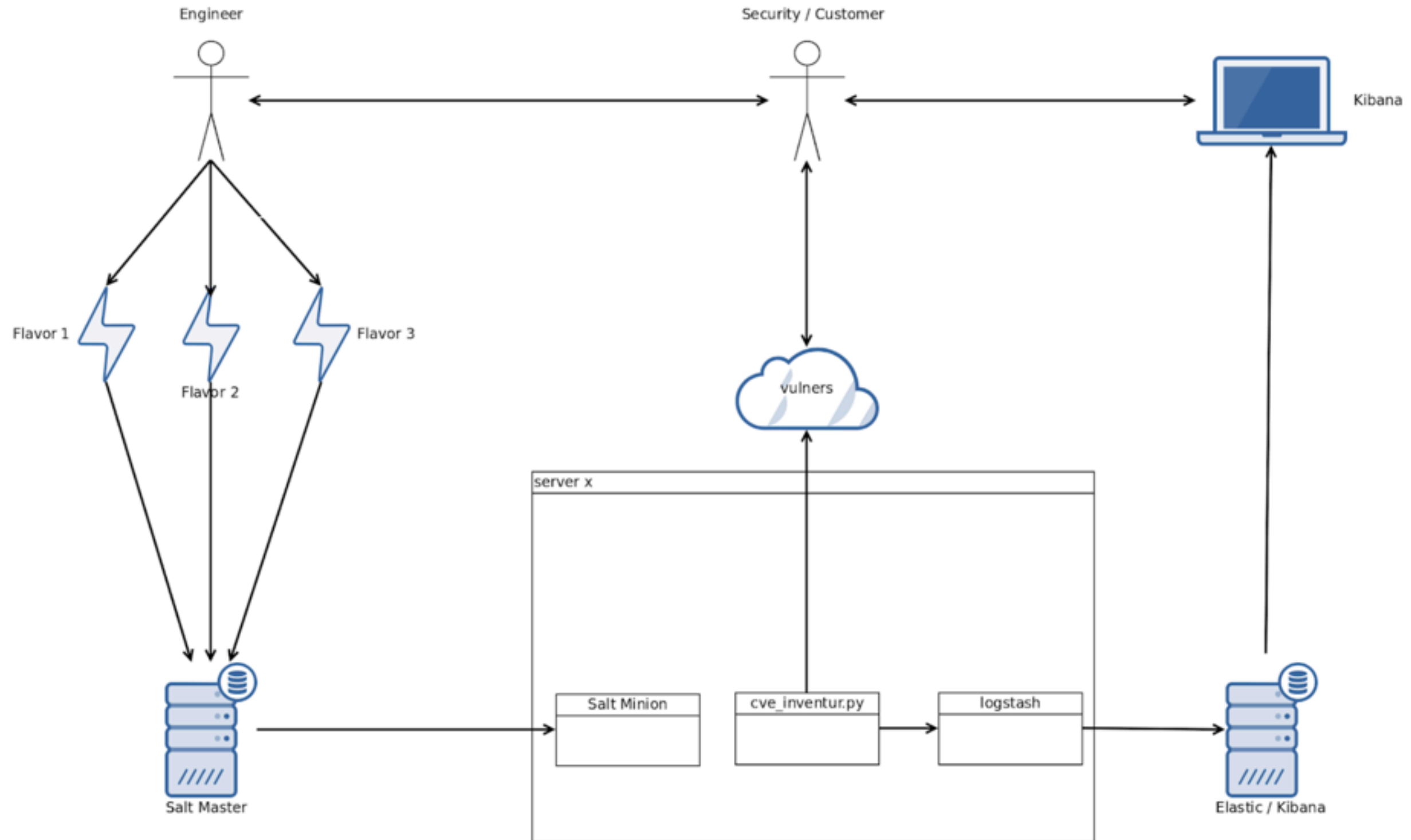
figure based on <https://www.elastic.co/guide/en/logstash/current/introduction.html>



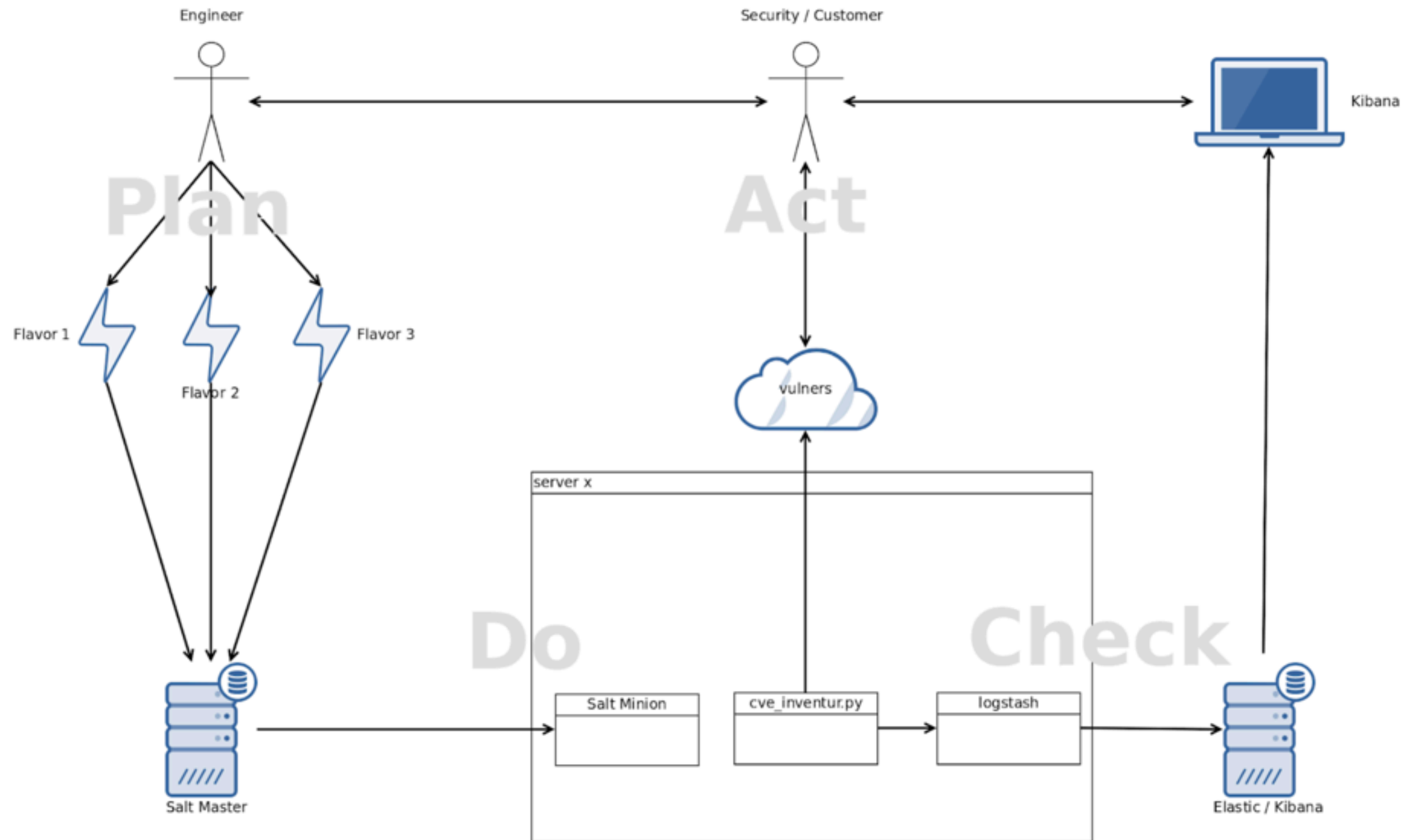
Demo

KIBANA.SZOPS.DE

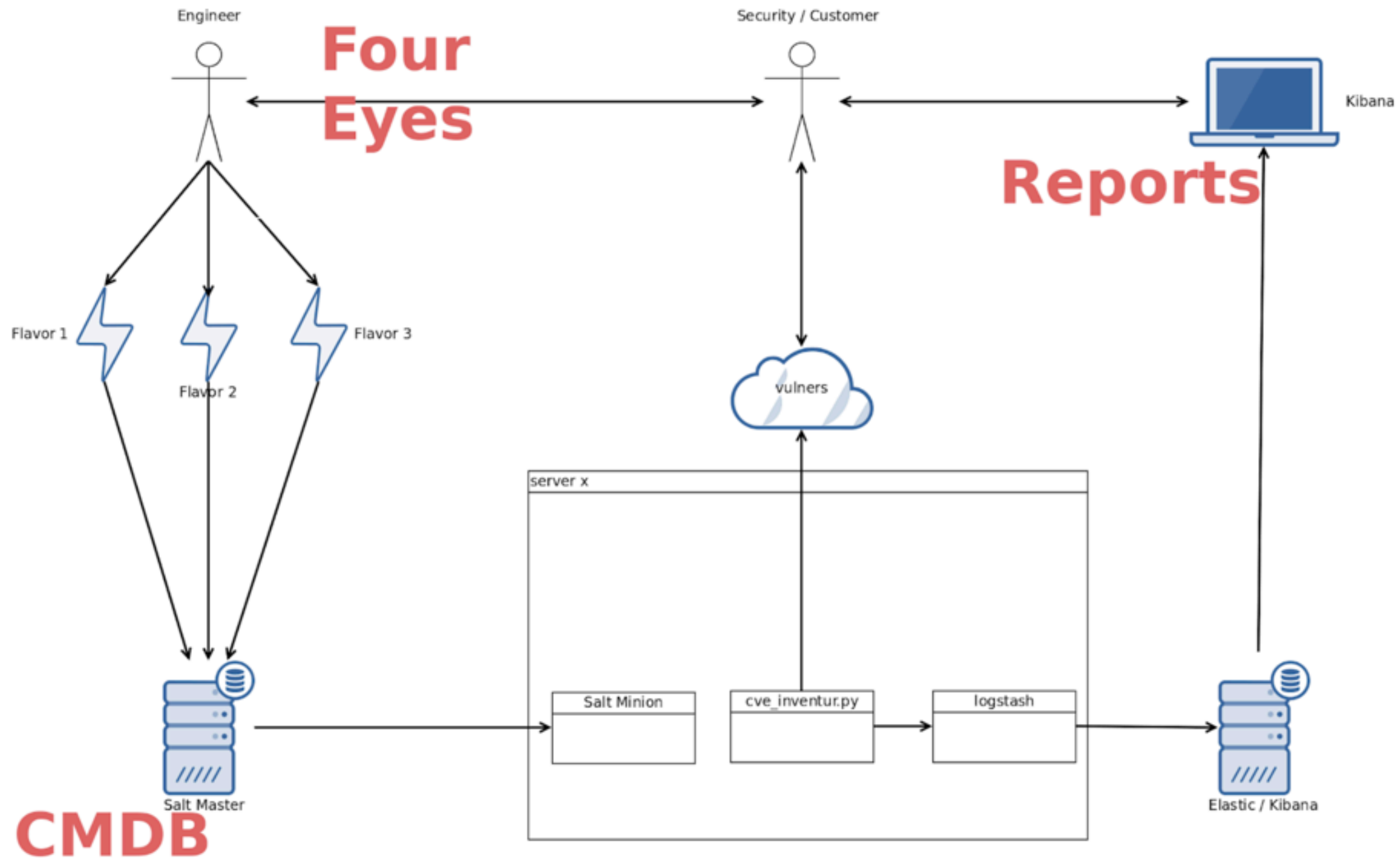
The big picture



The big picture



The big picture





Limitations



There are some limitations

AKA STUFF THAT COMPLIANCE FOLKS LIKELY WON'T FIND,
BUT THAT YOU KNOW IS THERE ...

Tales from the kernel

```
root@[REDACTED]:~# dpkg -l | grep linux-  
ii linux-firmware 1.127.24 all Firmware for Linux kernel drivers  
ii linux-image-3.13.0-39-generic 3.13.0-39.66 amd64 Linux kernel image for version 3.13.0 on 64 bit x86 SMP  
ii linux-image-3.8.0-35-generic 3.8.0-35.50 amd64 Linux kernel image for version 3.8.0 on 64 bit x86 SMP  
ii linux-image-extra-3.13.0-39-generic 3.13.0-39.66 amd64 Linux kernel extra modules for version 3.13.0 on 64 bit x86 SMP  
ii linux-image-extra-3.8.0-35-generic 3.8.0-35.50 amd64 Linux kernel image for version 3.8.0 on 64 bit x86 SMP  
root@[REDACTED]:~# uname -a  
Linux [REDACTED] 3.13.0-39-generic #66-Ubuntu SMP Tue Oct 28 13:30:27 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux  
root@[REDACTED]:~# █
```

- Notice version encoded in package name
- This confuses vulners (no CVEs)
- As well as unattended upgrades (yep, no upgrades)

Tales from the kernel - the fix

```
root@██████:~# dpkg -l | grep linux-
ii  linux-firmware      1.127.24      all      Firmware for Linux kernel drivers
ii  linux-image-3.13.0-144-generic 3.13.0-144.193 amd64    Linux kernel image for version 3.13.0 on 64 bit x86 SMP
ii  linux-image-3.13.0-39-generic  3.13.0-39.66  amd64    Linux kernel image for version 3.13.0 on 64 bit x86 SMP
ii  linux-image-3.8.0-35-generic   3.8.0-35.50   amd64    Linux kernel image for version 3.8.0 on 64 bit x86 SMP
ii  linux-image-extra-3.13.0-144-generic 3.13.0-144.193 amd64    Linux kernel extra modules for version 3.13.0 on 64 bit x86 SMP
ii  linux-image-extra-3.13.0-39-generic  3.13.0-39.66  amd64    Linux kernel extra modules for version 3.13.0 on 64 bit x86 SMP
ii  linux-image-extra-3.8.0-35-generic   3.8.0-35.50   amd64    Linux kernel image for version 3.8.0 on 64 bit x86 SMP
ii  linux-image-generic           3.13.0.144.154 amd64    Generic Linux kernel image
root@██████:~# uname -a
Linux ██████ 3.13.0-144-generic #193-Ubuntu SMP Thu Mar 15 17:03:53 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
root@██████:~# █
```

- Install the meta package linux-image-generic

Reboot hassle

```
root@██████:~# dpkg -l|grep linux-image
ii  linux-image-3.13.0-121-generic  3.13.0-121.170      amd64      Linux kernel image for version 3.13.0 on 64 bit x86 SMP
ii  linux-image-3.13.0-137-generic  3.13.0-137.186      amd64      Linux kernel image for version 3.13.0 on 64 bit x86 SMP
ii  linux-image-3.8.0-29-generic    3.8.0-29.42~precise amd64      Linux kernel image for version 3.8.0 on 64 bit x86 SMP
ii  linux-image-extra-3.13.0-121-generic 3.13.0-121.170      amd64      Linux kernel extra modules for version 3.13.0 on 64 bit x86 SMP
ii  linux-image-extra-3.13.0-137-generic 3.13.0-137.186      amd64      Linux kernel extra modules for version 3.13.0 on 64 bit x86 SMP
ii  linux-image-generic            3.13.0.137.146      amd64      Generic Linux kernel image
ii  linux-image-generic-lts-raring    3.13.0.137.146      amd64      Generic Linux kernel image
root@██████:~# uname -a
Linux ████████ 3.13.0-121-generic #170-Ubuntu SMP Wed Jun 14 09:04:33 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
root@szz-f07:~# uptime
15:10:52 up 176 days, 23 min,  1 user,  load average: 0.09, 0.06, 0.05
root@██████:~# █
```

- Running old kernel although newer one is installed

Reboot hassle - the fix

```
root@██████:~# dpkg -l|grep linux-image
ii  linux-image-3.13.0-121-generic      3.13.0-121.170      amd64      Linux kernel image for version 3.13.0 on 64 bit x86 SMP
ii  linux-image-3.13.0-137-generic      3.13.0-137.186      amd64      Linux kernel image for version 3.13.0 on 64 bit x86 SMP
ii  linux-image-3.8.0-29-generic        3.8.0-29.42~precise amd64      Linux kernel image for version 3.8.0 on 64 bit x86 SMP
ii  linux-image-extra-3.13.0-121-generic 3.13.0-121.170      amd64      Linux kernel extra modules for version 3.13.0 on 64 bit x86 SMP
ii  linux-image-extra-3.13.0-137-generic 3.13.0-137.186      amd64      Linux kernel extra modules for version 3.13.0 on 64 bit x86 SMP
ii  linux-image-generic                 3.13.0.137.146      amd64      Generic Linux kernel image
ii  linux-image-generic-lts-raring       3.13.0.137.146      amd64      Generic Linux kernel image
root@██████:~# uname -a
Linux ████████ 3.13.0-121-generic #170-Ubuntu SMP Wed Jun 14 09:04:33 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
root@szz-f07:~# uptime
15:10:52 up 176 days, 23 min,  1 user,  load average: 0.09, 0.06, 0.05
root@██████:~# █
```

- Monitor uptime of your servers ;-)
- The two metrics that matter for host security by Diogo Monica



Next steps

Next steps

- Fix some quirks ;-)
- Container checks with Claire
- AWS integration
- nsp check

Alternatives

- OpenVAS / vuls
- <https://github.com/0x4D31/salt-scanner>
- Your-typical-Enterprise-Distribution-Mgmt-here
- Reverse uptime & Golden image freshness

- Kirill Ermakov from Vulners.com(@isox_xx)
- Christoph Trautwein (@trautw) & the S2 ops crew



Thanks!