

SOC EN STOCK



Nicolas Hanteville



```
$ sudo whoami
```

CISO Deputy at vente-privee.com since 2016

Before:

Mainly worked as a security expert and auditor.

I am recruiting

Creating a Security Operations Center (Audit logs, alert and PRI)

Some criteria :

- It must contain all logs for 3 months and at least 1 year of archiving
- An alarm system (with automation capability)
- Incident Response Plan
- Secured
- Easy to use and contribute



But, the products on the market are expensive and not really what we want!

Creating a Security Operations Center

- Yes! But open source and scalable!
- Requires very powerful servers or VMs!!!
- A lot of storage may be needed



Creating a Security Operations Center: But where do you start?

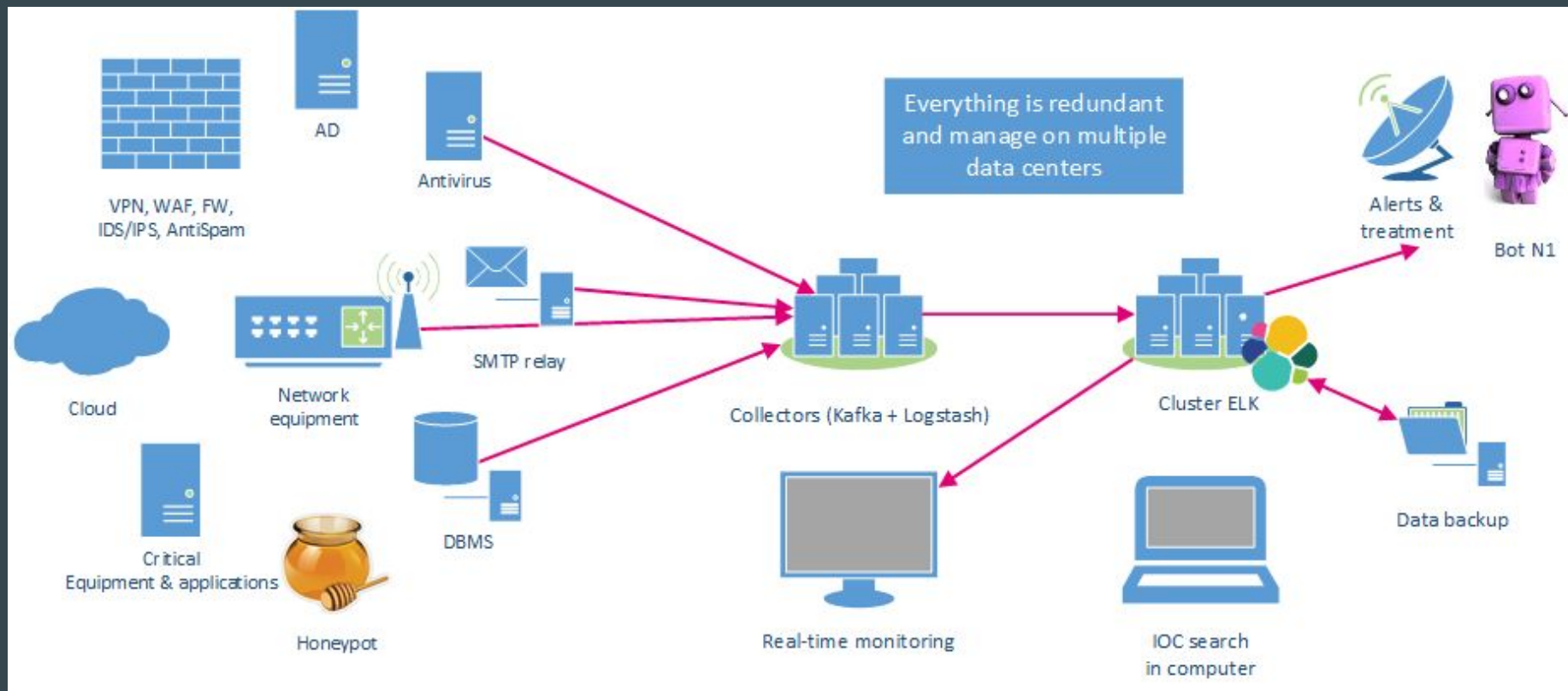
- 1) Identify the critical points (AD, VPN, Firewall/IDS/IPS, Wifi access, WAF, criticals applications, physical access, etc.)
- 2) Normalize log format and structure! (Syslog, names, keywords, search, graph, etc.)
- 3) Create detailed alerts
- 4) Validate incident response plans and automate them as much as possible.
- 5) Check that everything is working properly (New AD, automate agent deployment, statistics on the volume and quality of audit logs, etc.)
- 6) KPI!!!

Most important points

- ❑ Do not go too fast: take time for reflection rather than start all over again 10 times.
- ❑ For a minimum infrastructure it takes at least 6 servers with large capacities (8 TB SSD disk, CPU 8 cores, 64 GB Mem) + Backup and pre-production.
- ❑ Automation => spend time to save time
- ❑ Takes time, time and time!

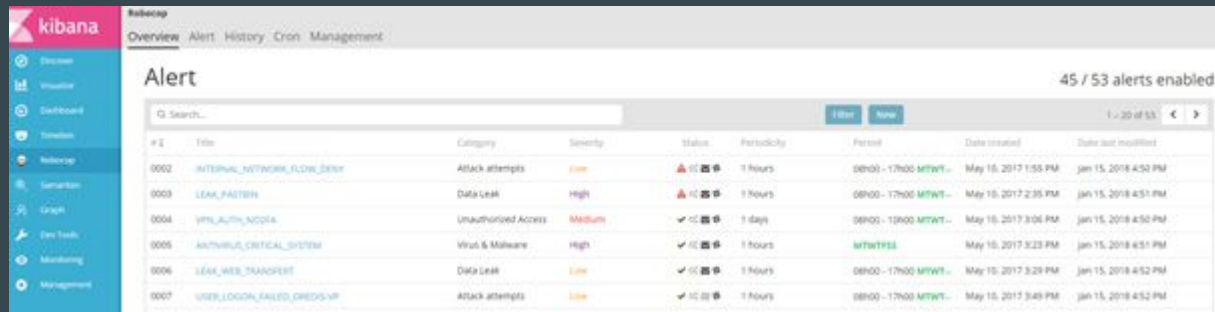


Concretely what we did?



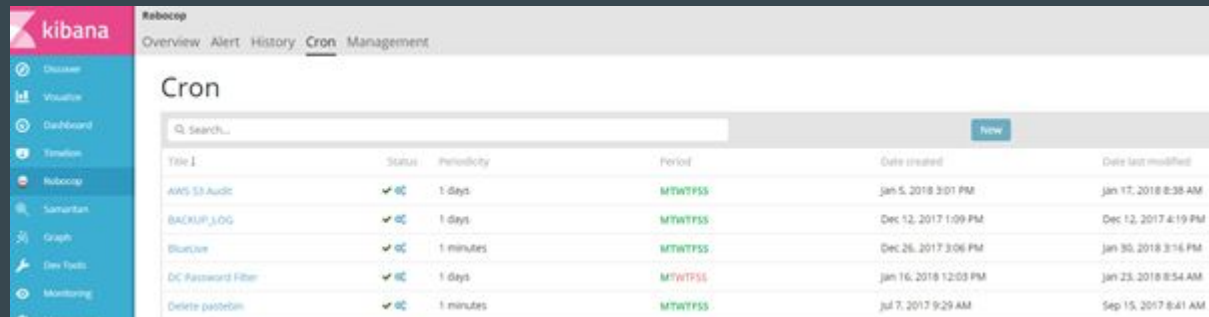
A lot of development...

Kibana plugins to graphically manage and tracking alerts, union request...



The screenshot shows the Kibana Alert page. The left sidebar contains navigation links: Overview, Visualize, Dashboard, Timeline, Rubocop, Samantern, Graph, Dev Tools, Monitoring, and Management. The main content area is titled 'Alert' and shows '45 / 53 alerts enabled'. A search bar and 'Filter' button are at the top. Below is a table of alerts with columns: #, Title, Category, Severity, Status, Periodicity, Period, Date created, and Date last modified.

#	Title	Category	Severity	Status	Periodicity	Period	Date created	Date last modified
0002	INTERNAL_NETWORK_FLOW_DENY	Attack attempts	Low	🔴 🟡 🟢	1 hours	0800 - 1700 MTWTFSS	May 10, 2017 1:55 PM	Jan 15, 2018 4:50 PM
0003	LEAK_FASTEN	Data Leak	High	🔴 🟡 🟢	1 hours	0800 - 1700 MTWTFSS	May 10, 2017 2:35 PM	Jan 15, 2018 4:51 PM
0004	VPN_AUTH_NODS4	Unauthorized Access	Medium	✓ 🟡 🟢	1 days	0800 - 1000 MTWTFSS	May 10, 2017 3:06 PM	Jan 15, 2018 4:50 PM
0005	ANTIVIRUS_CRITICAL_SYSTEM	Virus & Malware	High	✓ 🟡 🟢	1 hours	MTWTFSS	May 10, 2017 3:23 PM	Jan 15, 2018 4:51 PM
0006	LEAK_WEB_TRANSPARENT	Data Leak	Low	✓ 🟡 🟢	1 hours	0800 - 1700 MTWTFSS	May 10, 2017 3:29 PM	Jan 15, 2018 4:52 PM
0007	USER_LOGIN_FAILED_CREDENTIALS	Attack attempts	Low	✓ 🟡 🟢	1 hours	0800 - 1700 MTWTFSS	May 10, 2017 3:49 PM	Jan 15, 2018 4:52 PM



The screenshot shows the Kibana Cron page. The left sidebar is the same as the Alert page. The main content area is titled 'Cron' and shows a table of cron jobs with columns: Title, Status, Periodicity, Period, Date created, and Date last modified.

Title	Status	Periodicity	Period	Date created	Date last modified
AWS S3 Audit	✓ 🟡 🟢	1 days	MTWTFSS	Jan 5, 2018 3:01 PM	Jan 17, 2018 8:38 AM
BACKUP_LOG	✓ 🟡 🟢	1 days	MTWTFSS	Dec 12, 2017 1:09 PM	Dec 12, 2017 4:19 PM
Blurview	✓ 🟡 🟢	1 minutes	MTWTFSS	Dec 26, 2017 3:06 PM	Jan 30, 2018 3:16 PM
DC Password Filter	✓ 🟡 🟢	1 days	MTWTFSS	Jan 16, 2018 12:03 PM	Jan 23, 2018 8:54 AM
Delete patches	✓ 🟡 🟢	1 minutes	MTWTFSS	Jul 7, 2017 9:29 AM	Sep 15, 2017 8:41 AM

A lot of development...


A smart BOT...

to make happy our N1 team :)
and improve response time.

Open Source publication this year (GITHUB,
projects Robocop, Samaritan and more...)
thanks to our Florian²

vente-privee 

Problems encountered

- ❑ Doing everything yourself also means developing with new versions!
 - ❑ ELK 2.x - 5.x - 6.x => Many major changes (structure, functions, GUI)
- ❑ Data must be optimized to reduce disk space and network throughput.
- ❑ IT: The collection agent slows down the server. => 
- ❑ How to update the agent & server configuration? => Ansible
- ❑ Interconnection with market solutions (AV, SIEM, Share, O365, AWS, etc.)
- ❑ Some alerts that seem simple, are very complicated to set up.
- ❑ If you have a SOC you need a team! => 3/5 employees needed for the durability of the team



Thank you very much!

Any question?

nicolas.hanteville@gmail.com

< vp**Tech** /> vente-privee 