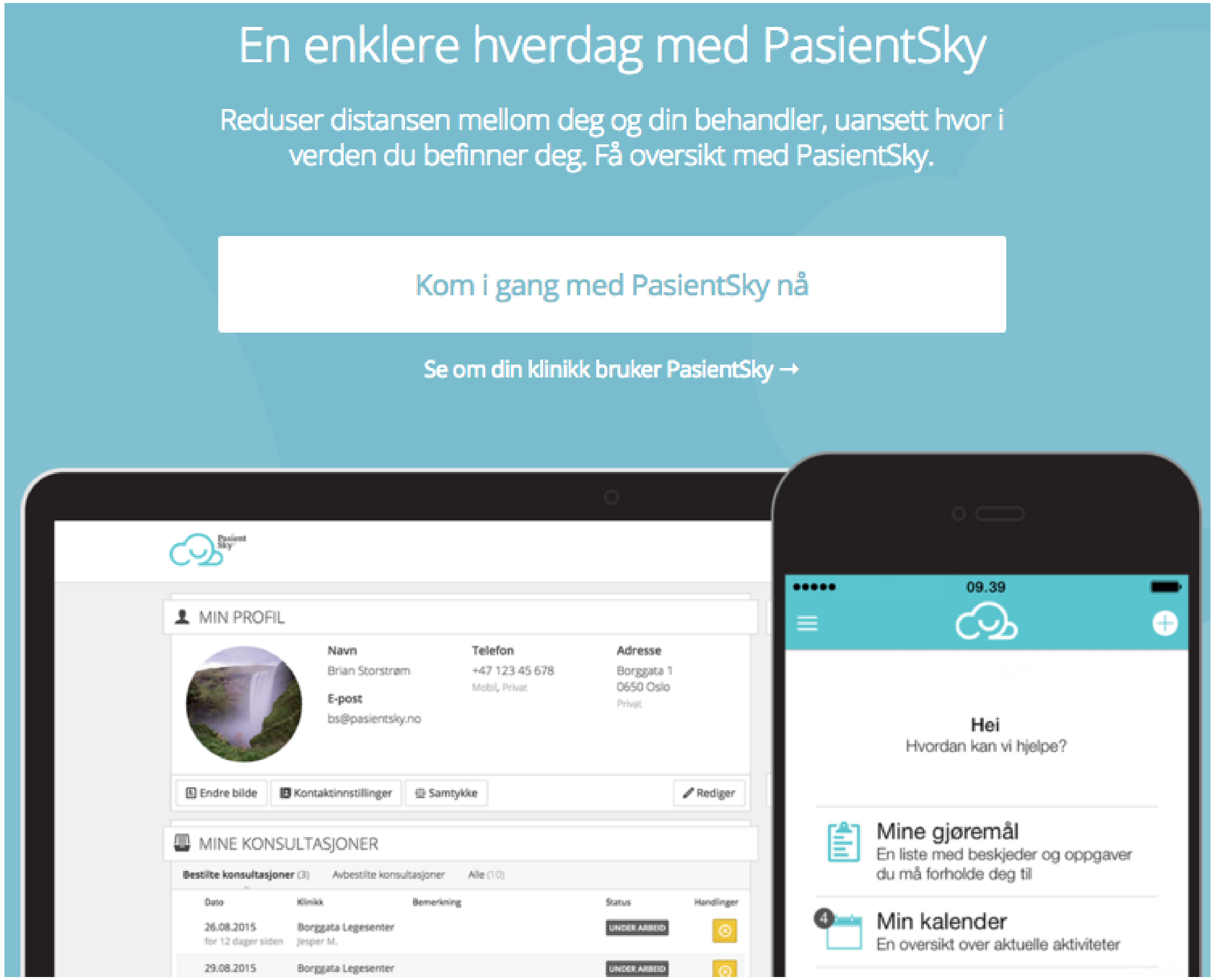
Welcome to

Controlling a High Security Environment with Ansible

Henrik Lund Kramshøj hlk@pasientsky.no

Introduction: En enklere hverdag med PasientSky



En enklere hverdag med PasientSky

Reduser distansen mellom deg og din behandler, uansett hvor i verden du befinner deg. Få oversikt med PasientSky.

Kom i gang med PasientSky nå
Se om din klinikk bruker PasientSky →
Pasient Sky

MIN PROFIL

Navn
Brian Storstrøm

E-post
bs@pasientsky.no

Telefon
+47 123 45 678
Mobil, Privat

Adresse
Borggata 1
0650 Oslo
Privat

Endre bilde
Kontaktinnstillinger
Samtykke
Rediger

MINE KONSULTASJONER

Bestilte konsultasjoner (3)
Avbestilte konsultasjoner
Alle (10)

Dato	Klinikk	Bemerkning	Status	Handlinger
26.08.2015 for 12 dager siden	Borggata Legesenter Jesper M.		UNDER ARBEID	
29.08.2015	Borggata Legesenter		UNDER ARBEID	

Hei
Hvordan kan vi hjelpe?

Mine gjøremål
En liste med beskjeder og oppgaver du må forholde deg til

Min kalender
En oversikt over aktuelle aktiviteter

Obviously this means personal data

Ansible: used for provisioning, cfg mgmt, security

Open Source

Simple playbooks and ad-hoc commands

Well supported on mainstream operating systems

over 200 modules in the core distribution

Supports just about anything which has SSH+Python

`http://www.ansible.com/`

Note: we dont use Tower

Operating systems we use

VMware ESX - pysphere and core module in Ansible, provision 10 servers no problem

Ubuntu Linux - core modules and some 100 changes after first boot

OpenBSD - pushing firewall rulesets, update PF lists and reload daemons consistently

All of the above well supported by Ansible

What we learnt about Ansible

Easy to get started YAML playbooks

Easy to configure services

Roles sometimes suck - to many files in too many directories

Using more flat playbooks are nice

What Ansible brings in a High Security Environment

We can rebuild advanced servers from scratch in 15 minutes

Example We can build a complete Log environment from a single playbook,

- Syslog servers
- PostgreSQL database
- Logstash parser, software and rules
- Elasticsearch indexing servers
- Kibana front end

From a base Ubuntu install with no manual steps, other than starting Ansible

What Ansible brings in a High Security Environment

We can deploy a complete IDS solution in 15 minutes

A complete Suricata IDS environment from a single playbook,

- Suricata IDS
- Rulesets - configuration files the same across environments
- Cron - jobs for updating rules
- Elasticsearch indexing servers
- Kibana front end

From a base Ubuntu install with no manual steps, other than starting Ansible

Templates

We can test the SAME CONFIGS in multiple environments

Using variable group vars, host vars, templates

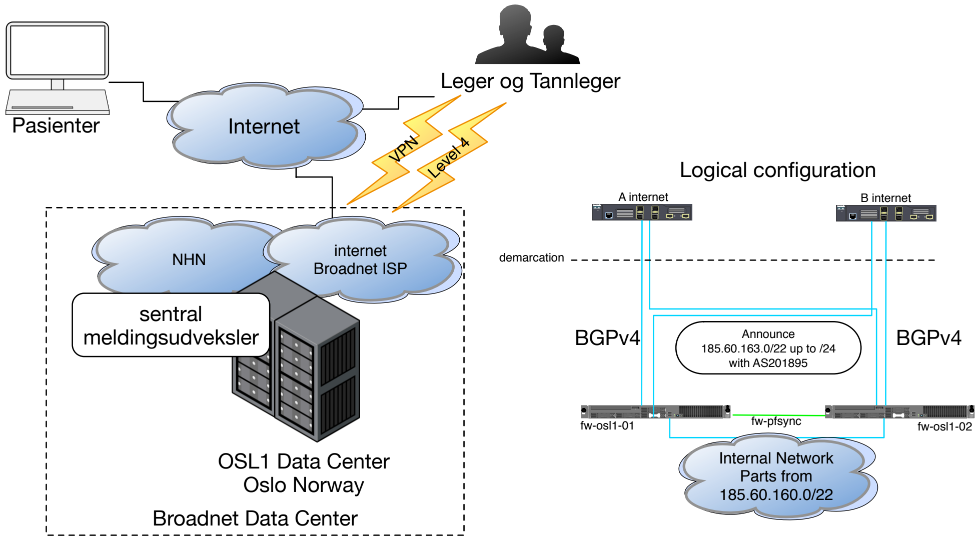
- Site specific data, RFC1918 subnets

No untested changes brought into production

Update security parameters

```
- lineinfile:
    dest=/etc/ssh/sshd_config state=present
    regexp=’PasswordAuthentication’
    line=’PasswordAuthentication no’
  when: ansible_hostname != "vpn-{{ location_name }}-01"
  notify: restart sshd
  tags:
    - sshd
```

Cluster firewalls always consistent



```
- name: copy PF tables
  template: src=roles/infrastructure-firewall/files/pf-tables/ item | basename
  dest=/etc/pf/ item | basename  owner=root group=wheel mode=0600
  with_fileglob:
      - roles/infrastructure-firewall/files/pf-tables/*.list
  notify:
    - reload pf
```

Golden rules

Dont use lineinfile, if changing more than a few, use a template

hlk@patientsky.com

Questions?

Henrik Lund Kramshøj hlk@pasientsky.no

`https://pasientsky.no/`

You are always welcome to send me questions later via email