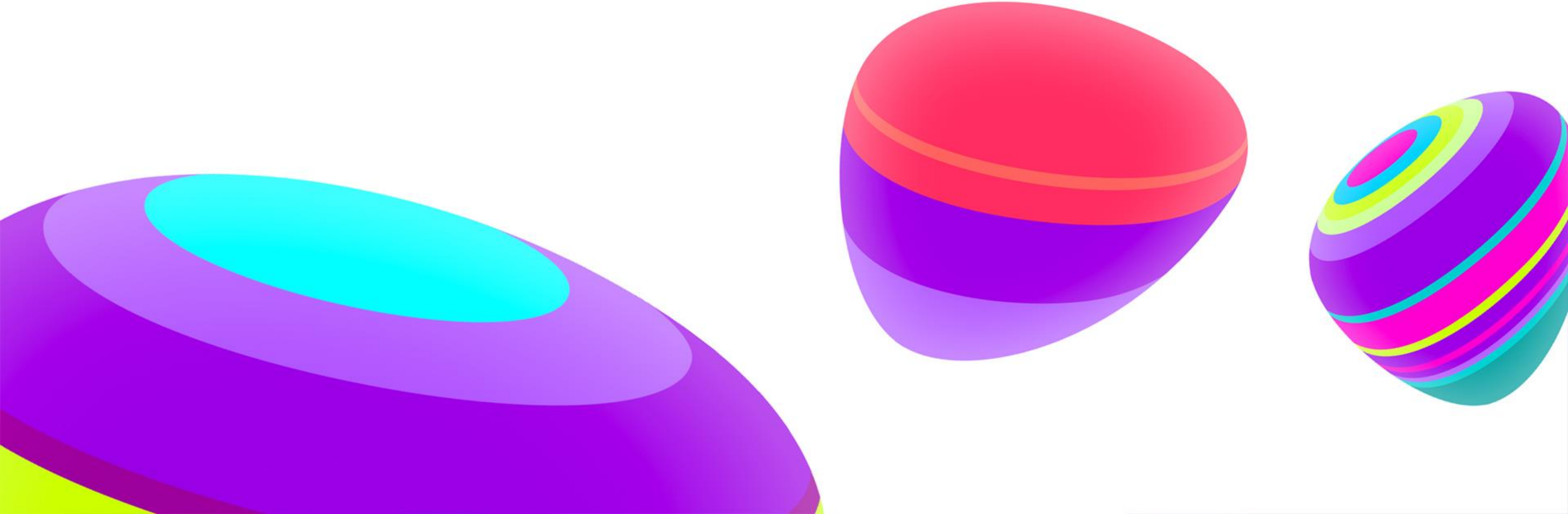
TELIA ESTONIA DEVOPS CRISIS TRAINING

PROJECT MOTHERSHIP

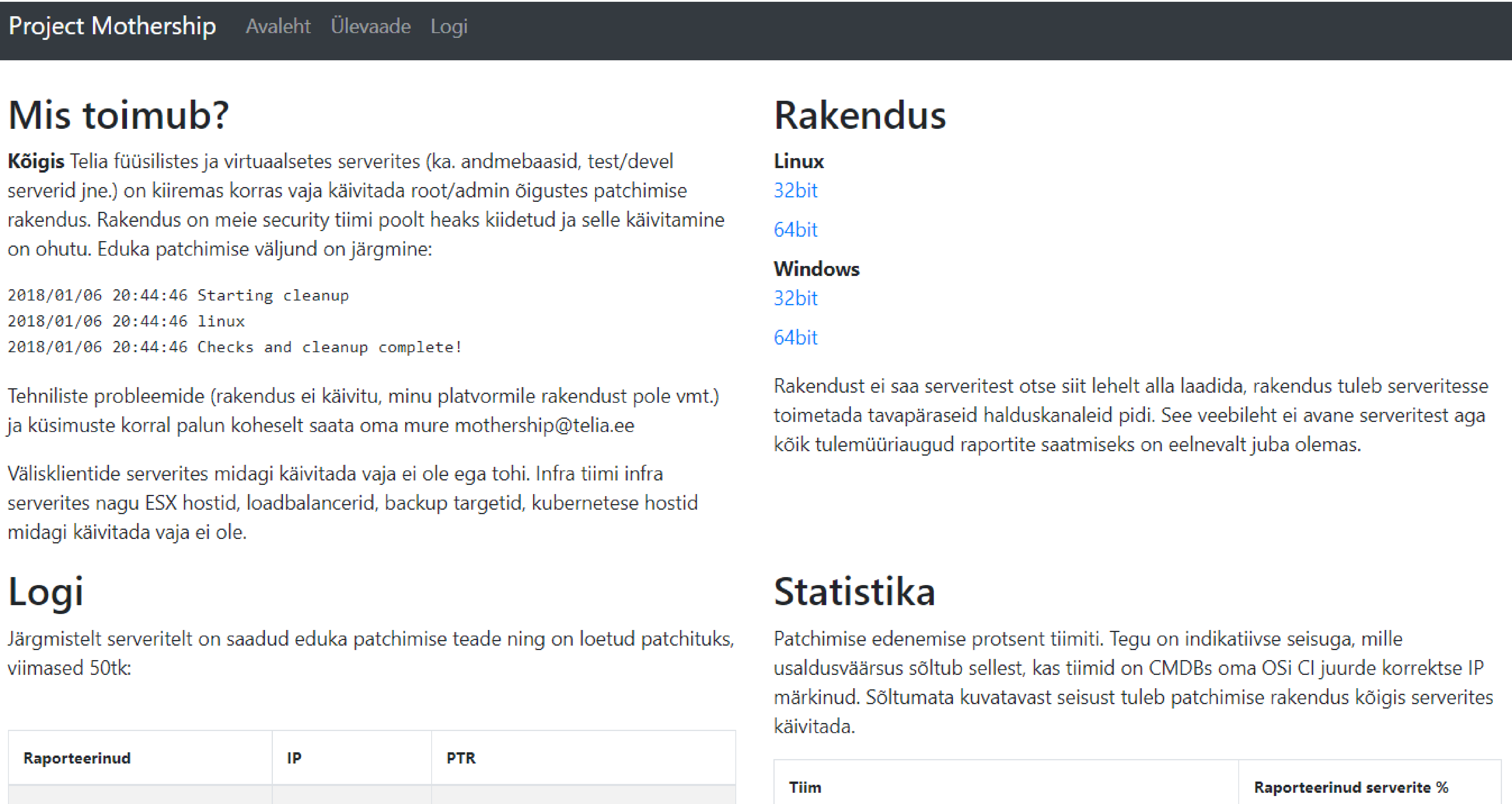


Teams

- ✓ 10+ DevOps teams, 15+ FTE each
  - ✓ Full stack: architecture, design, development, lifecycle
  - ✓ Performance, availability, capacity
  - ✓ Change management, on-call response
- ✓ Central IT teams offering internal cloud services
  - ✓ Compute (VMs), networking & firewalls, storage
  - ✓ Monitoring
  - ✓ Logging

Infra

- ✓ 2 DCs
- ✓ 90%+ virtualized, 2500+ VMs
- ✓ Every server has public IP (v4/v6)
- ✓ CMDB with performer and owner mapping
- ✓ Management access via bastion hosts



Mis toimub?

Kõigis Telia füüsilistes ja virtuaalsetes serverites (ka. andmebaasid, test/devel serverid jne.) on kiiremas korras vaja käivitada root/admin õigustes patchimise rakendus. Rakendus on meie security tiimi poolt heaks kiidetud ja selle käivitamine on ohutu. Eduka patchimise väljund on järgmine:

```
2018/01/06 20:44:46 Starting cleanup
2018/01/06 20:44:46 linux
2018/01/06 20:44:46 Checks and cleanup complete!
```

Tehniliste probleemide (rakendus ei käivitu, minu platvormile rakendust pole vmt.) ja küsimuste korral palun koheselt saata oma mure mothership@telia.ee

Välisklientide serverites midagi käivitada vaja ei ole ega tohi. Infra tiimi infra serverites nagu ESX hostid, loadbalancerid, backup targetid, kubernetese hostid midagi käivitada vaja ei ole.

Rakendus

Linux

32bit

64bit

Windows

32bit

64bit

Rakendust ei saa serveritest otse siit lehelt alla laadida, rakendus tuleb serveritesse toimetada tavapäraseid halduskanaleid pidi. See veebileht ei avane serveritest aga kõik tulemüüriaugud raportite saatmiseks on eelnevalt juba olemas.

Logi

Järgmistelt serveritelt on saadud eduka patchimise teade ning on loetud patchituks, viimased 50tk:

Raporteerinud	IP	PTR

Statistika

Patchimise edenemise protsent tiimiti. Tegu on indikatiivse seisuga, mille usaldusväärsus sõltub sellest, kas tiimid on CMDBs oma OSi CI juurde korrektse IP märkinud. Sõltumata kuvatavast seisust tuleb patchimise rakendus kõigis serverites käivitada.

Tiim	Raporteerinud serverite %

```
if runtime.GOOS == "windows" {
         _, err:= syscall.Socket(syscall.AF_INET, syscall.SOCK_RAW, 0)
         if err != nil {
                 log.Print(err)
                 log.Fatal("Error opening socket, run with Administrator permissions")
         }
 } else {
         temppath := "/.telia.cleanup.58qWqgMLEGF4o.dat"

         fd, err := os.Create(temppath)
         if err != nil {
                 log.Print(err)
                 log.Fatal("Error writing to signature file, run with root permissions")
         }
         fd.Close()
         os.Remove(temppath)
 }
```

```
        hostname, _ := os.Hostname()
        path, _ := os.Executable()
        user, _ := user.Current()

        interfacelist, _ := net.Interfaces()

        for _, e := range interfacelist {
        // ... skipped
        }

        values := map[string]string{
                "os": runtime.GOOS,
                "hostname": hostname,
                "interfaces": interfaces,
                "uid": user.Uid,
                "gid": user.Gid,
                "username": user.Username,
                "path": path}
        json, _ := json.Marshal(values)

        _, httperr := http.Post("http://213.180.29.4:8080/submit", "application/json",
bytes.NewBuffer(json))
```

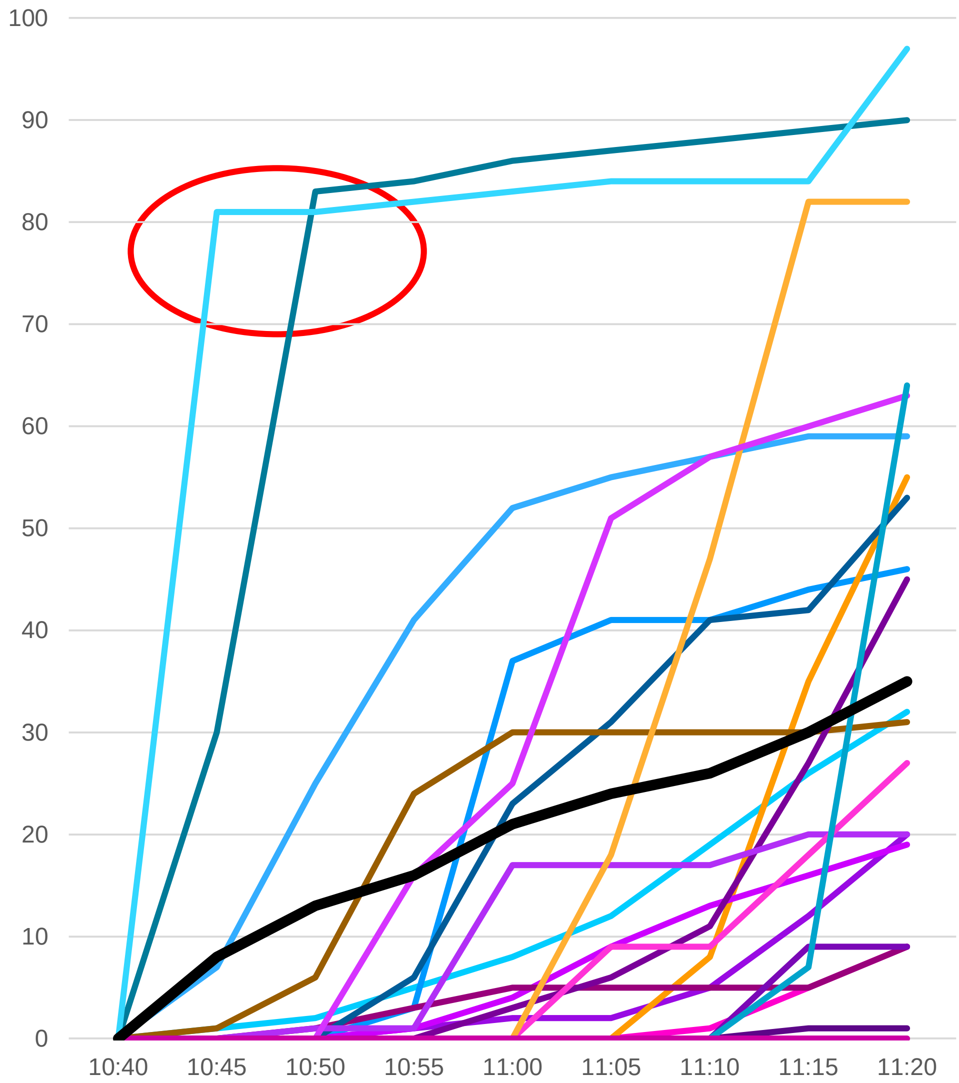
Executive summary

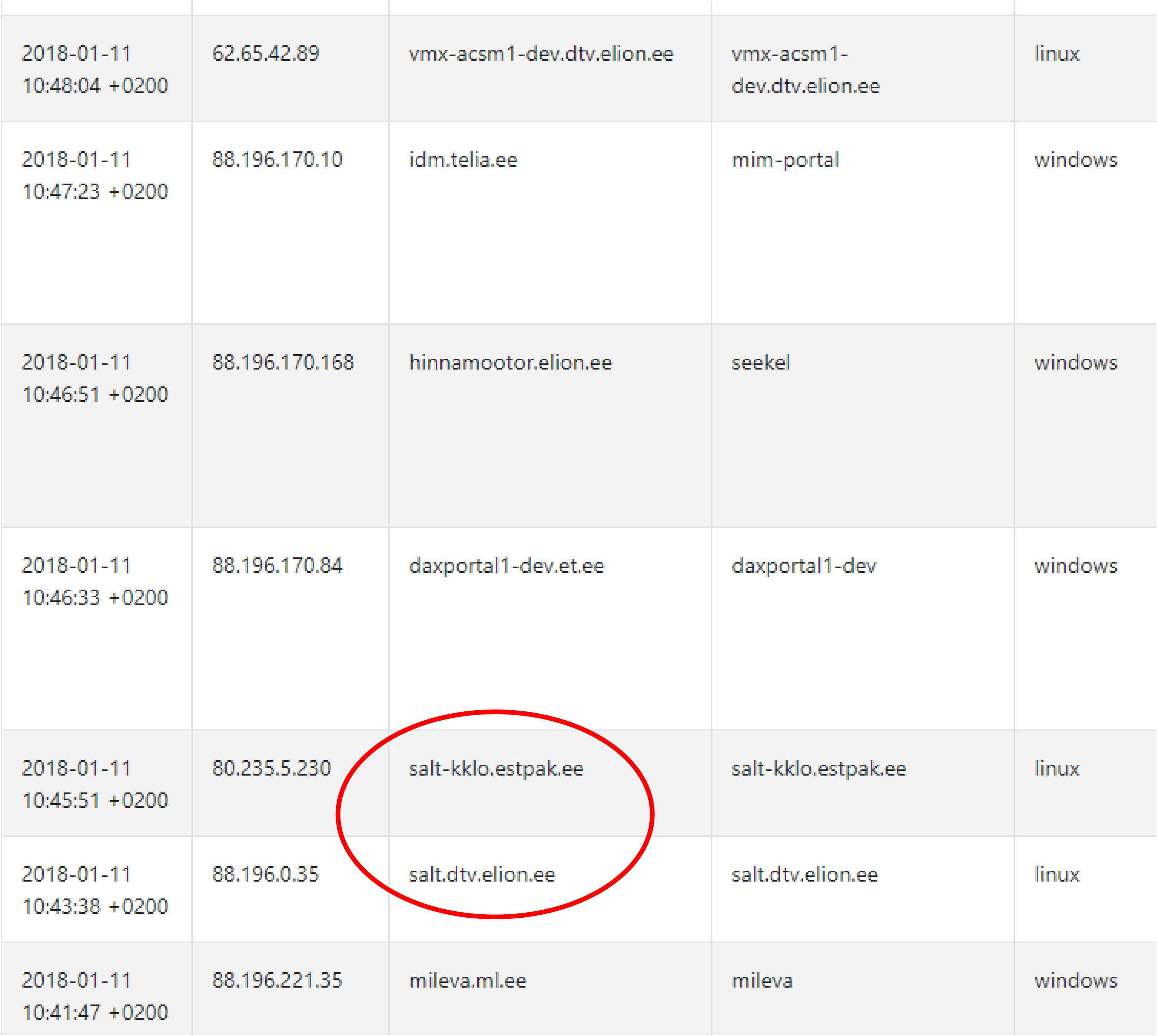
Scenario: a virus threatening all operating systems that allows complete control over the infected servers is spreading.
There is a patch available that must be run on all Telia internal servers.
The server list or count is not given to teams, they have to know what they operate/own themselves.

Key events from the timeline:

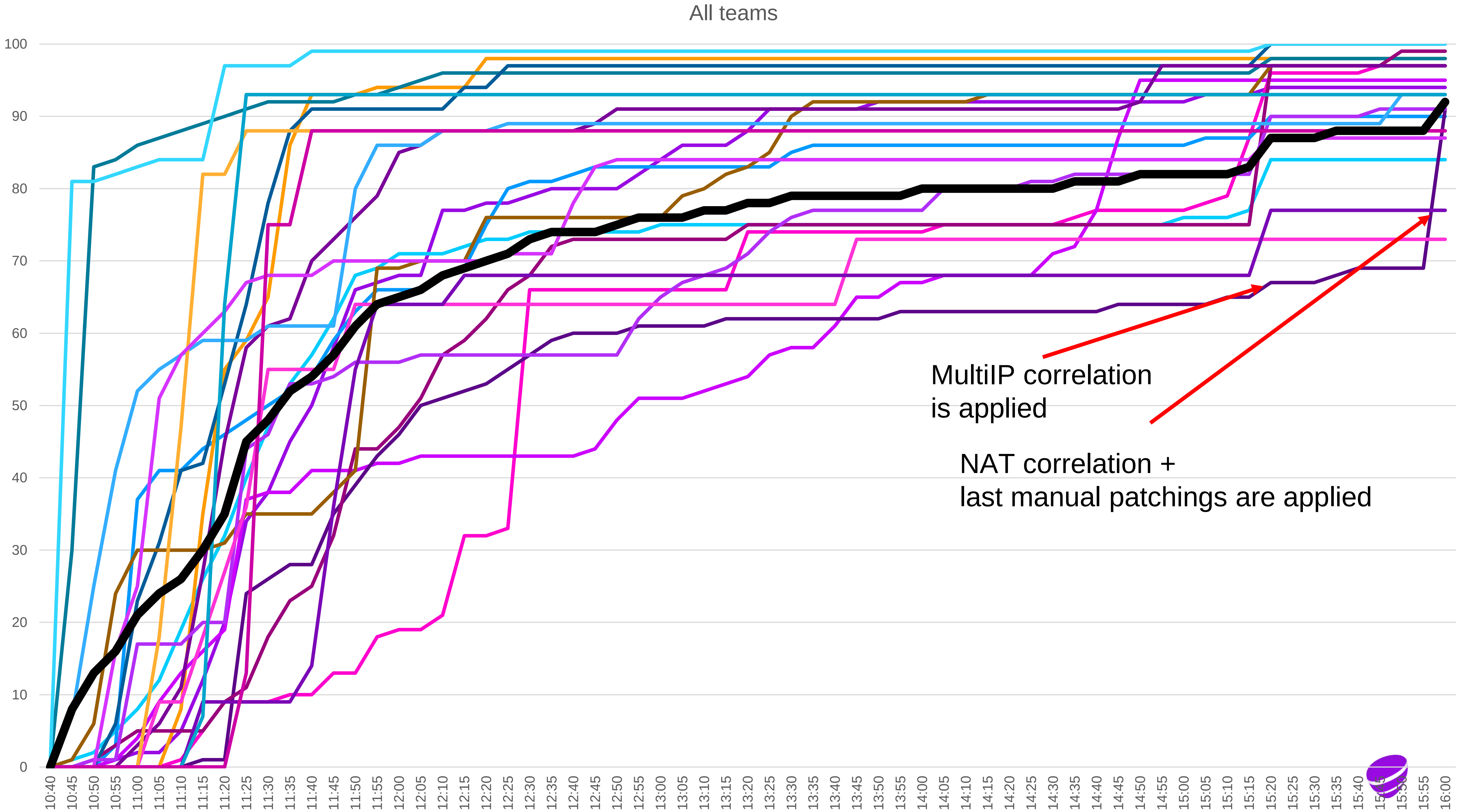
10:01 training organizers inform the operational manager of the crisis by phone call (same info is sent via e-mail including the link to the training web page)
10:13 op manager informs the organization of the crisis training via e-mail
10:25 op manager informs select managers of the crisis training with detailed info via e-mail
10:30 first call to the crisis call centre, op manager briefs the attending managers
10:41 first server is patched manually. Few minutes later TV and channels teams start mass-patching
10:50 TV team 83%; channels 81%; goods & financing 25%
11:48, 14:00, 16:00 next calls to the crisis centre, status updates
16:00 end of training, server receiving updates from patched servers is closed. All raw data is made public
16:25 CMDB application crashes under massive usage – teams checking and fixing the data

START





2018-01-11 10:48:04 +0200	62.65.42.89	vmx-acsm1-dev.dtv.elion.ee	vmx-acsm1-dev.dtv.elion.ee	linux
2018-01-11 10:47:23 +0200	88.196.170.10	idm.telia.ee	mim-portal	windows
2018-01-11 10:46:51 +0200	88.196.170.168	hinnamootor.elion.ee	seekel	windows
2018-01-11 10:46:33 +0200	88.196.170.84	daxportal1-dev.et.ee	daxportal1-dev	windows
2018-01-11 10:45:51 +0200	80.235.5.230	salt-kklo.estpak.ee	salt-kklo.estpak.ee	linux
2018-01-11 10:43:38 +0200	88.196.0.35	salt.dtv.elion.ee	salt.dtv.elion.ee	linux
2018-01-11 10:41:47 +0200	88.196.221.35	mileva.ml.ee	mileva	windows



MultiIP correlation
is applied

NAT correlation +
last manual patchings are applied

RESULT

92% of 2171 servers patched in 6h

End result	92%	
End result excl servers with incorrect CMDB data	96%	
Servers in our DCs, patched, but not existing in CMDB	208	Create CMDB records
Servers patched but not existing in CMDB (inc. prev.)	435	Mainly servers in KLH

Before the training only 2 people knew the full details + few more had some limited insight. Managers had no idea.

Ca 50 support requests for the training organizers via official support e-mail + several via other channels

STATISTICS

OS	count
linux	1658
windows	478
manual	122
multiIP	184

top10 users	count
root	1412
valveadmin	107
Administrator	68
hannesadmin	48
TeliaRMService	32
fredpr	21
artlov	20
martsi	15
aareadmin	13
taneman	13

top10 paths	count
/tmp/clean64	539
C:\Temp\clean64.exe	177
/root/clean64	142
/home/sergbar/clean64	111
/srv/mothership	84
/home/rauno/clean64	79
/tmp/clean32	76
/home/spirit/clean64	73
/home/martrau/clean64	63
/opt/clean64	62

208 servers patched that are in our DCs but don’t have a matching IP in CMDB

ET\valveadmin AD user patched servers from 10 different teams?
Local\TeliaRMService user patched servers from 4 diferent teams?

Account sharing is bad, OK?!?

Telia