Swiss Post Cybersecurity

TLP:CLEAR

Nobody's Watching

When Self-Managed Becomes Unmanaged

Antony ANCELIN

SwissCyberStorm 2026

$ Whoami

TLP:CLEAR

Antony ANCELIN

- ~10 years of experience in **InfoSec**
- @ **French Armed Forces**
  Offensive & Forensics
- @ **Swiss Post Cybersecurity**
  Incident Responder

csirt@swisspost-cybersecurity.ch

swisspost-cybersecurity.ch/en

The usual suspects

The usual picture

TLP:CLEAR

What we have in mind when thinking about shadow IT

Unapproved SaaS

Unmanaged network

Personal devices

Personal file sharing

Messaging apps

AI tools

What we see in IR

TLP:CLEAR

The usual picture

tools, apps, devices

What we see in IR

TLP:CLEAR

The usual picture

tools, apps, devices

IR cases

networks, servers, appliances

What we see in IR

TLP:CLEAR

The usual picture
tools, apps, devices

IR cases
networks, servers, appliances

Off the security team's roadmap

What we see in IR

TLP:CLEAR

The usual picture
tools, apps, devices

IR cases
networks, servers, appliances

Off the security team’s roadmap

Technical and governance gap

The other IT

The company

TLP:CLEAR

1,000+ employees

Security team

CISO

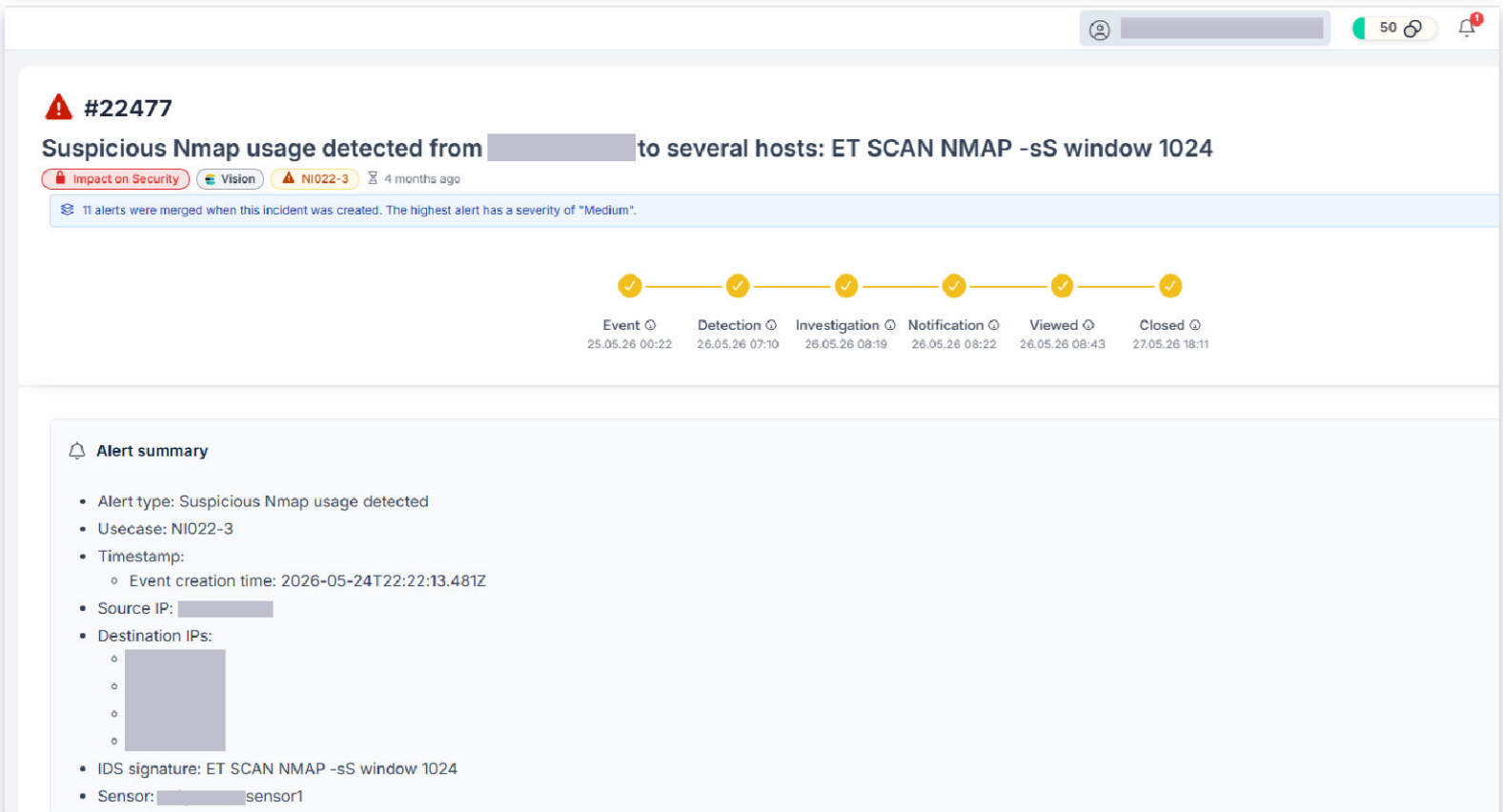
Logging policy

EDR

SOC

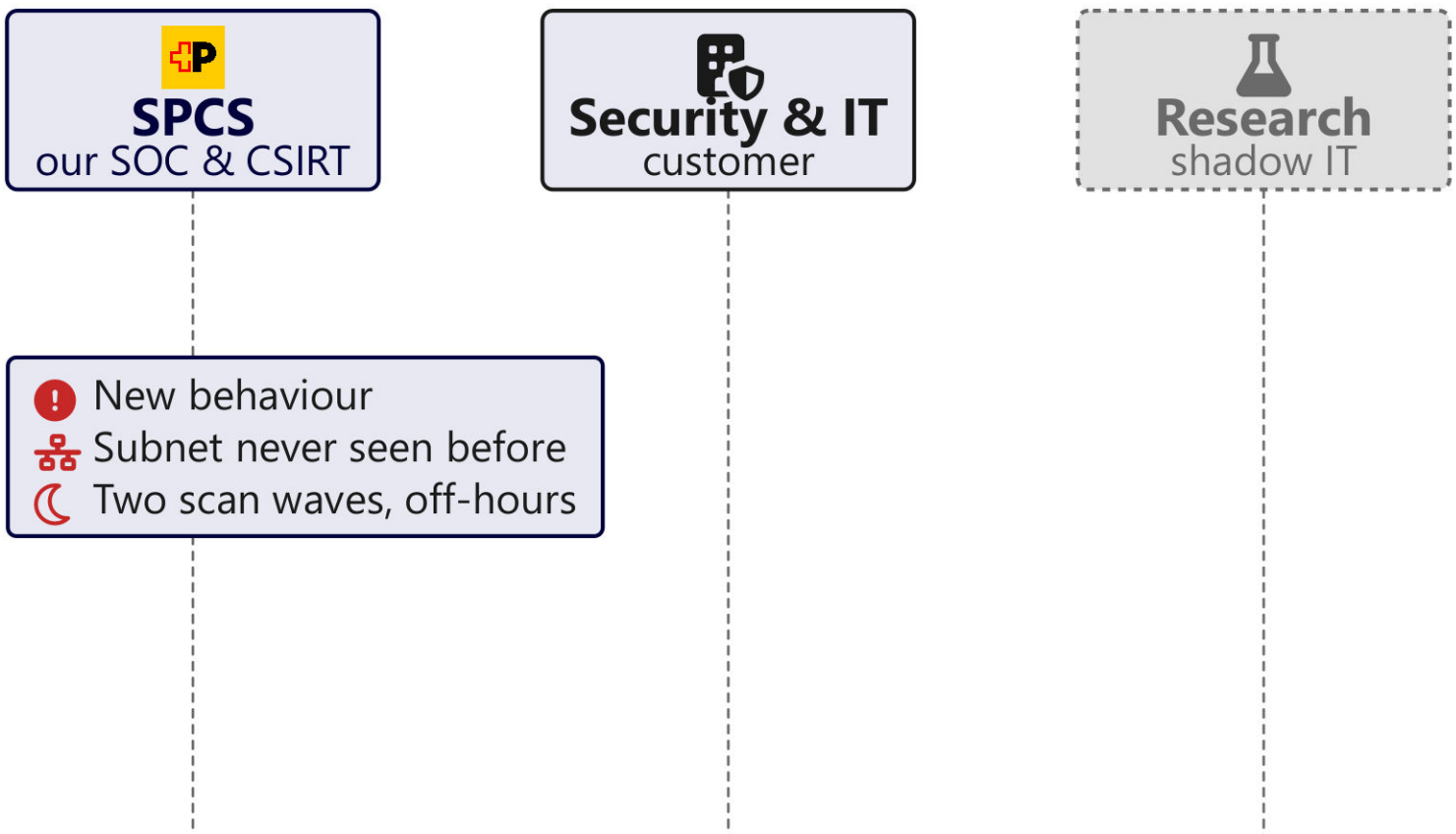
How it started

TLP:CLEAR



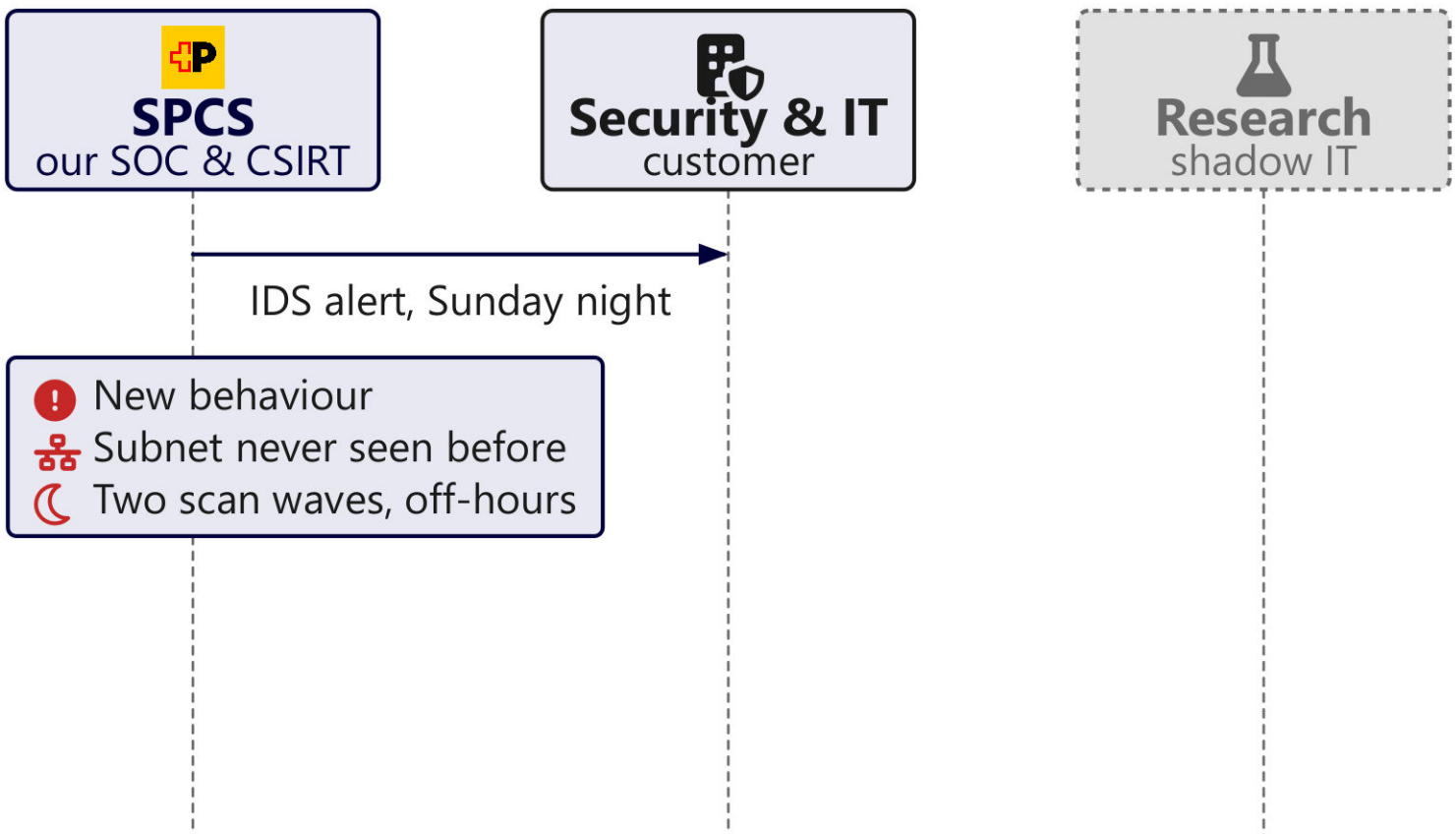
Slow escalation...

TLP:CLEAR



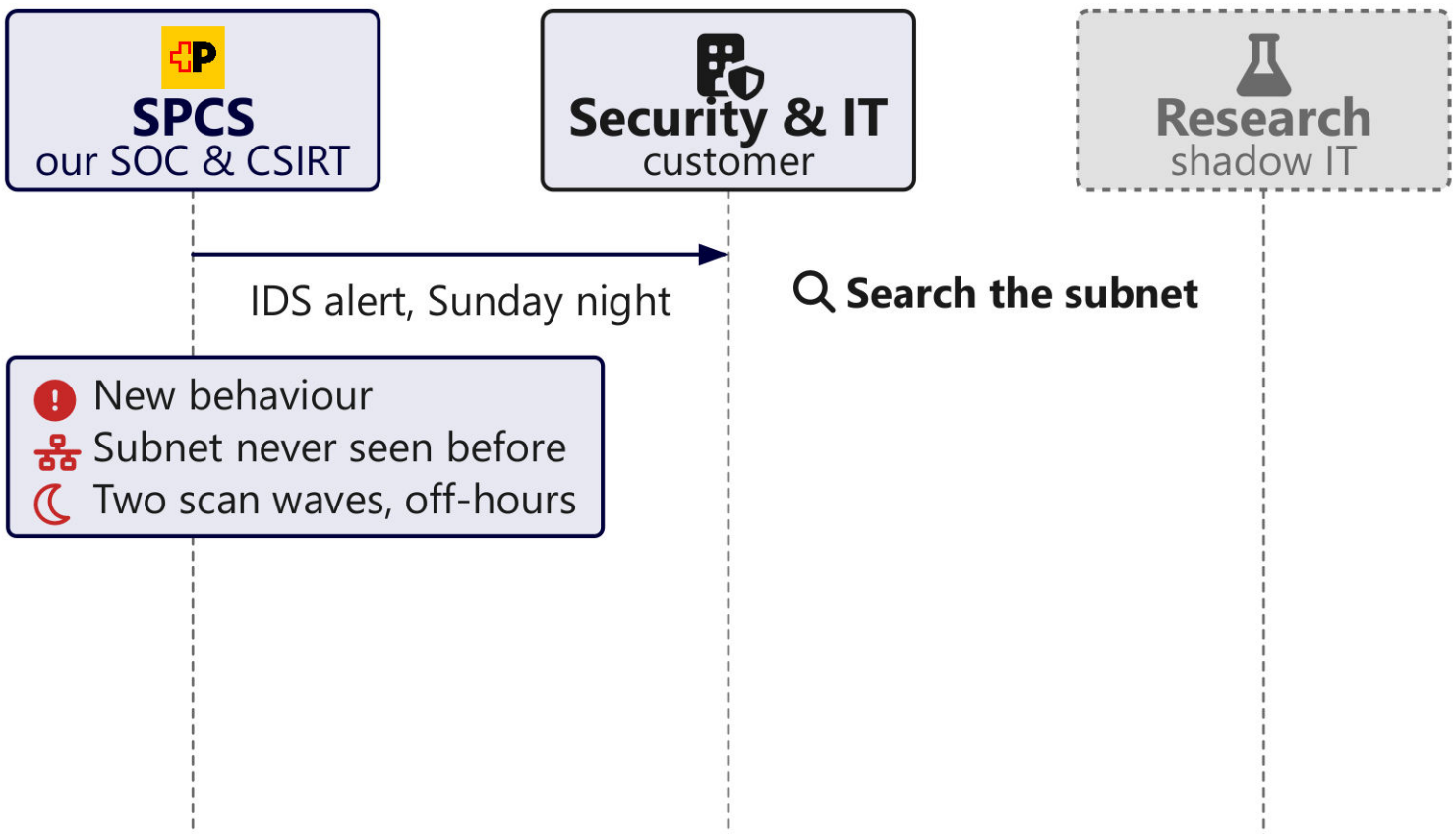
Slow escalation...

TLP:CLEAR



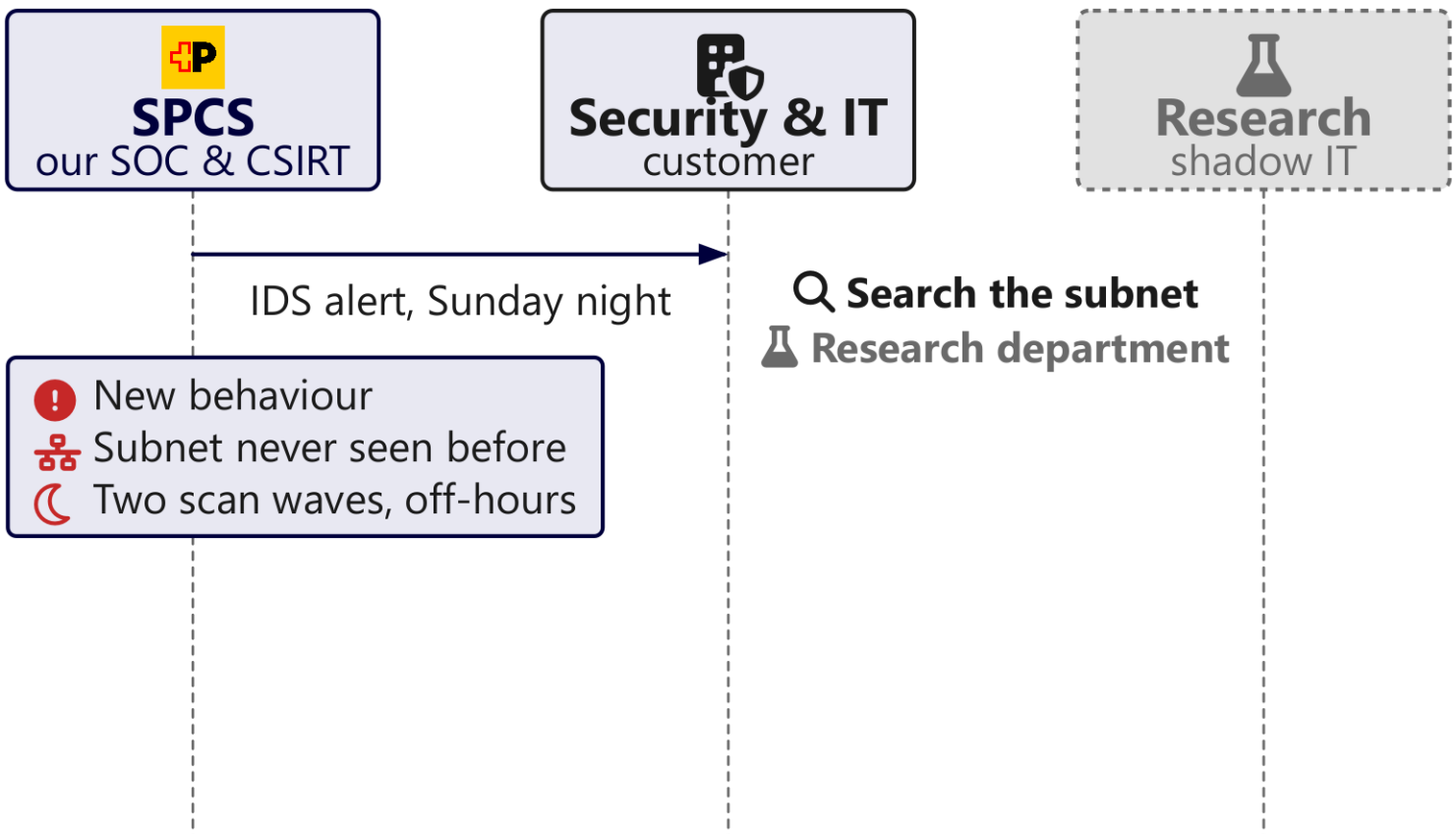
Slow escalation...

TLP:CLEAR



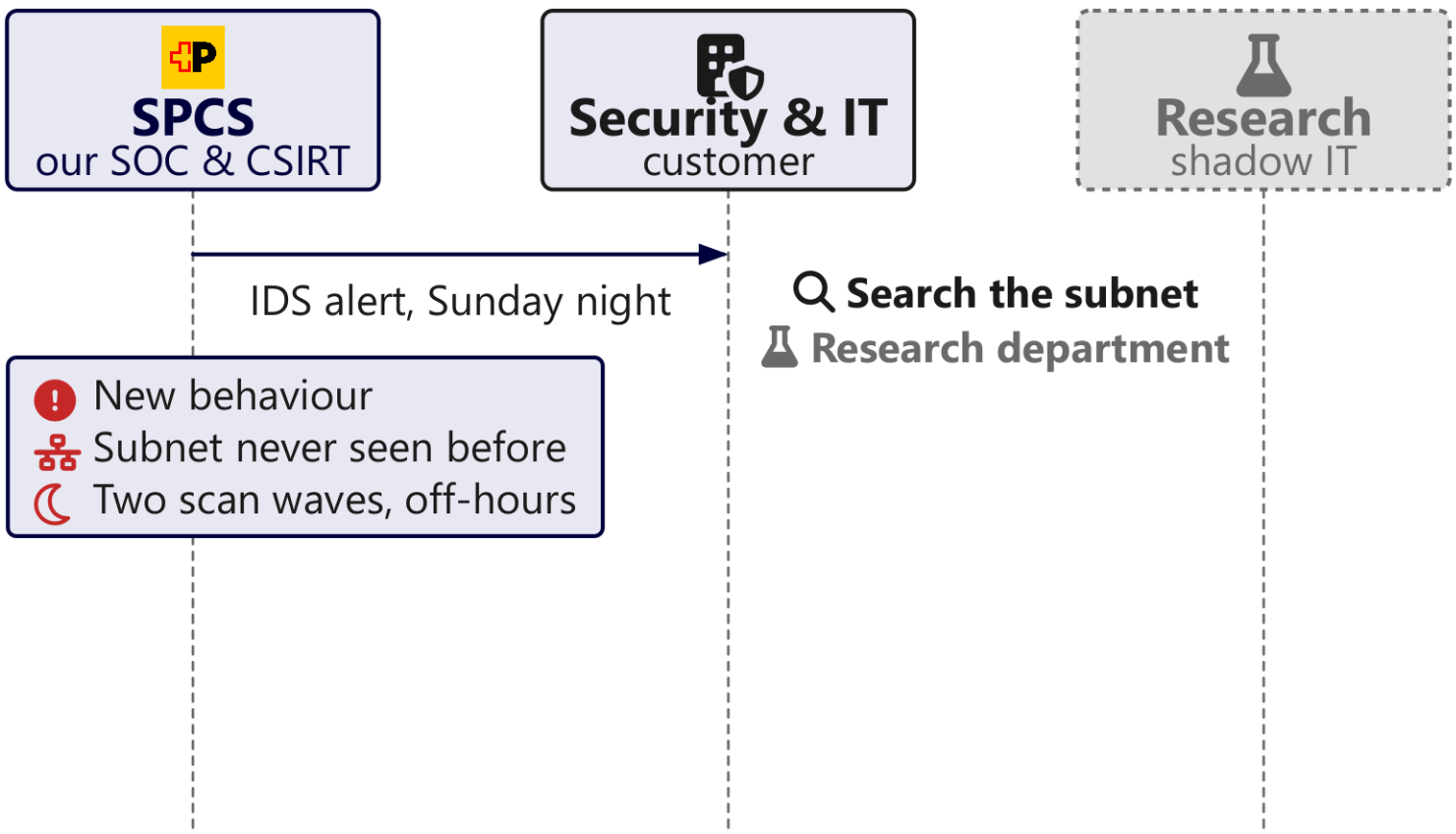
Slow escalation...

TLP:CLEAR



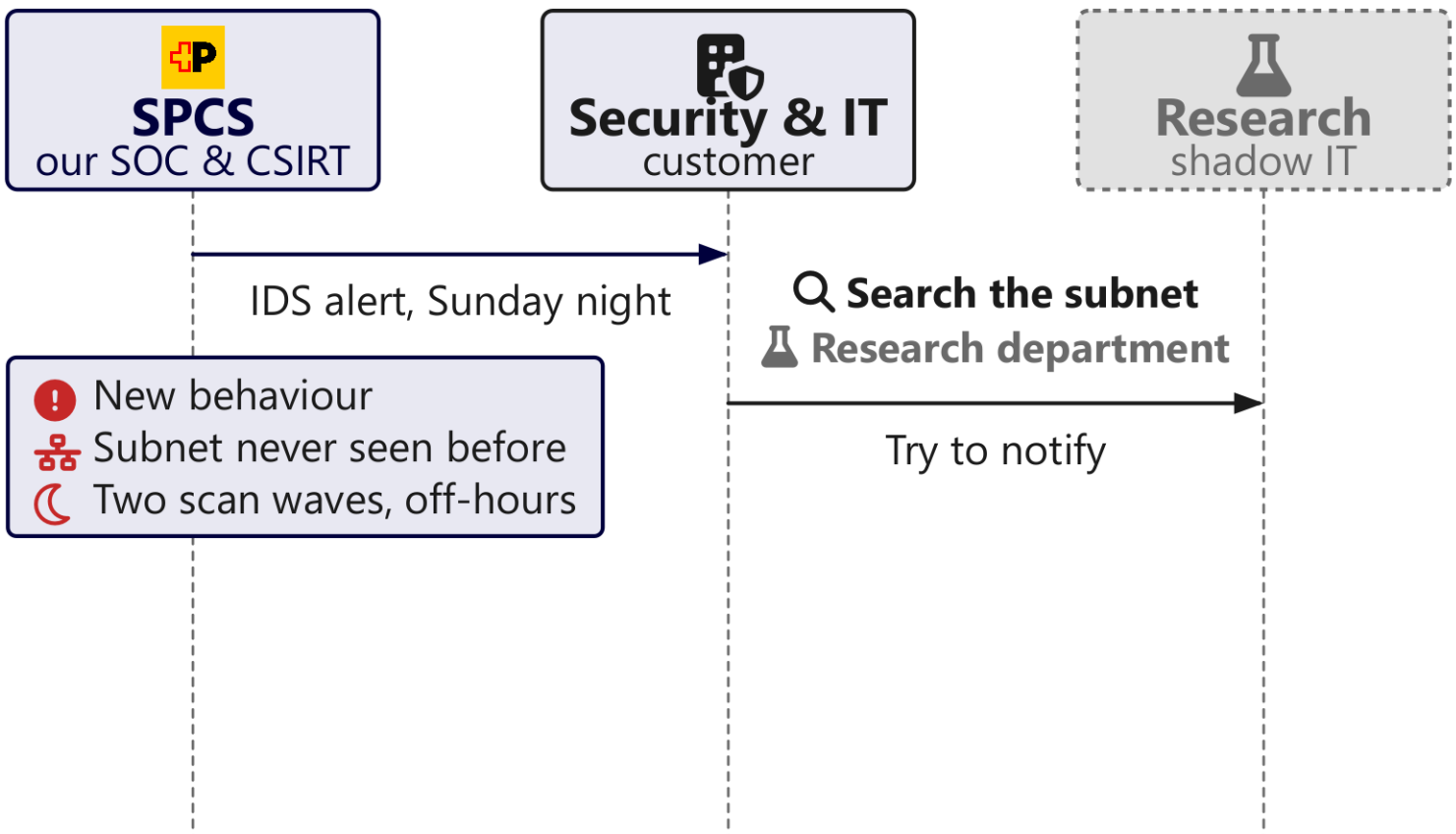
Slow escalation...

TLP:CLEAR



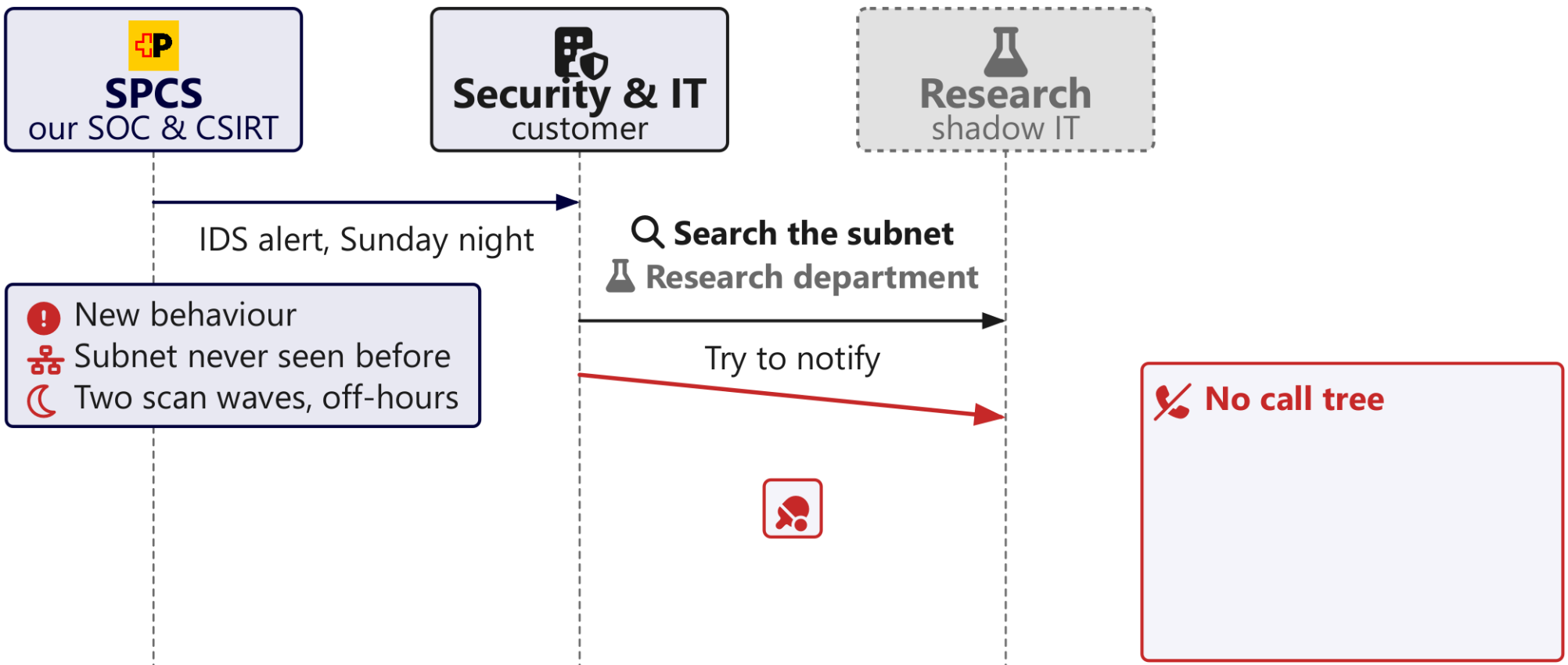
Slow escalation...

TLP:CLEAR



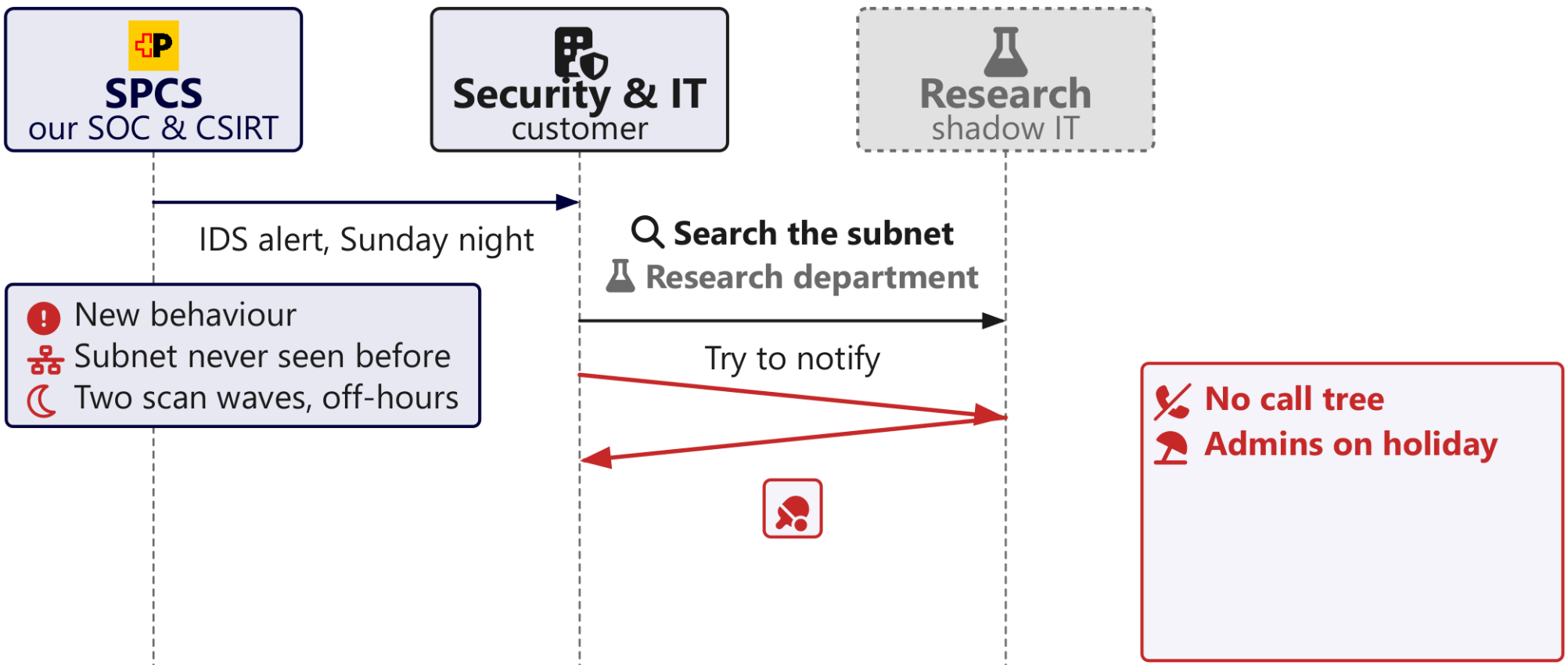
Slow escalation...

TLP:CLEAR



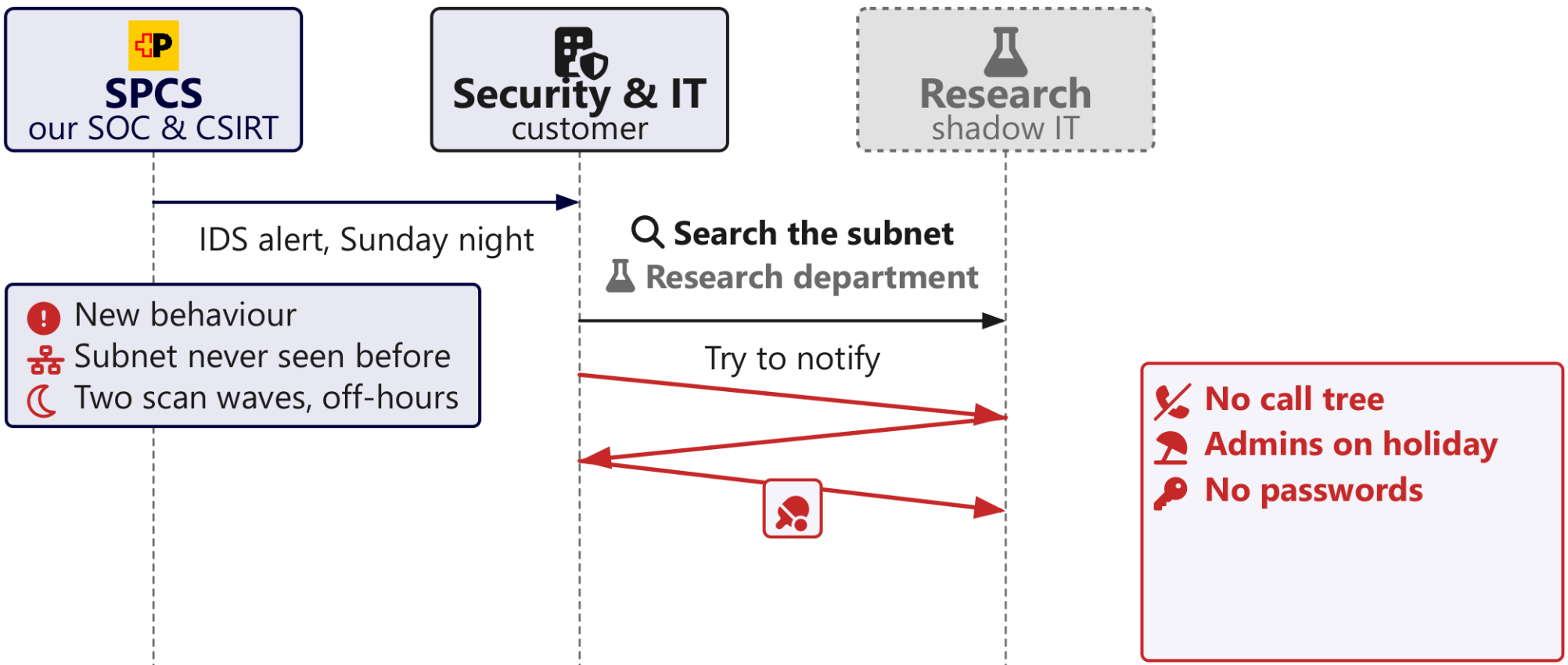
Slow escalation...

TLP:CLEAR



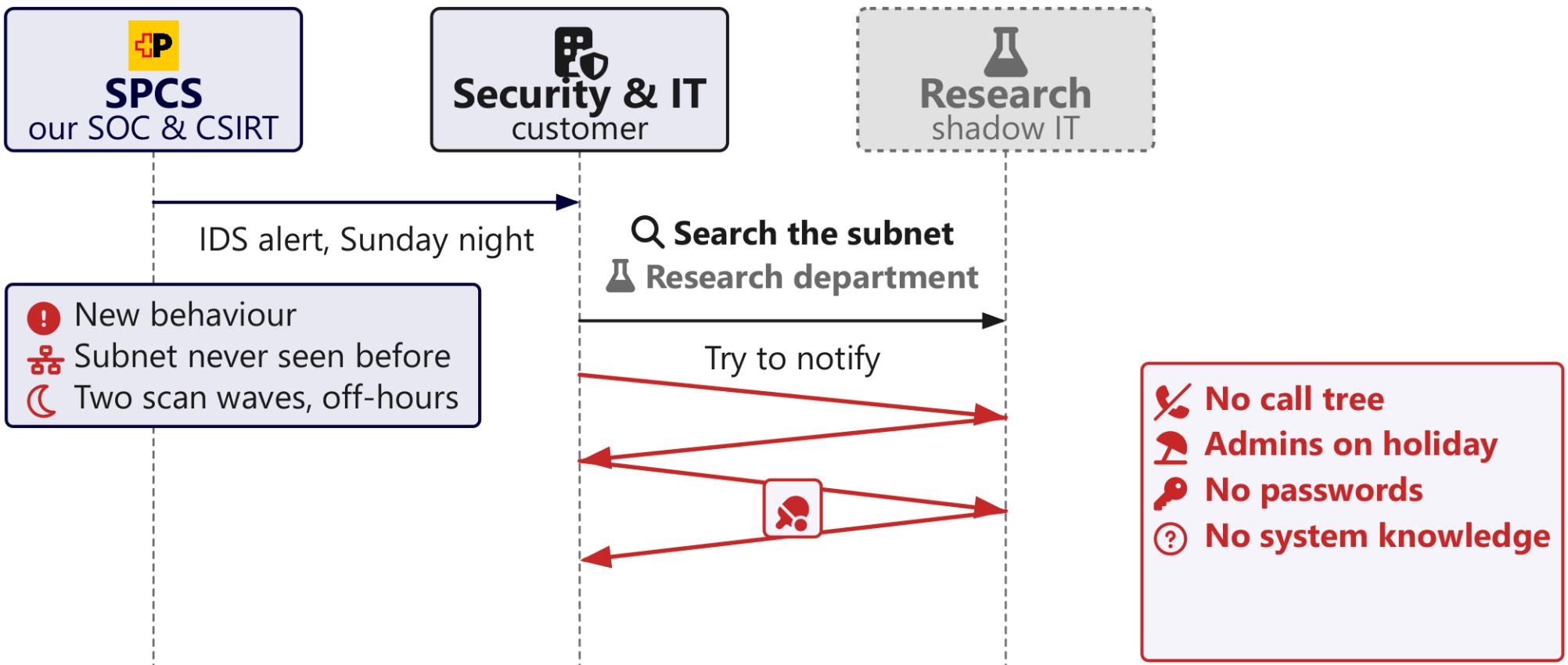
Slow escalation...

TLP:CLEAR



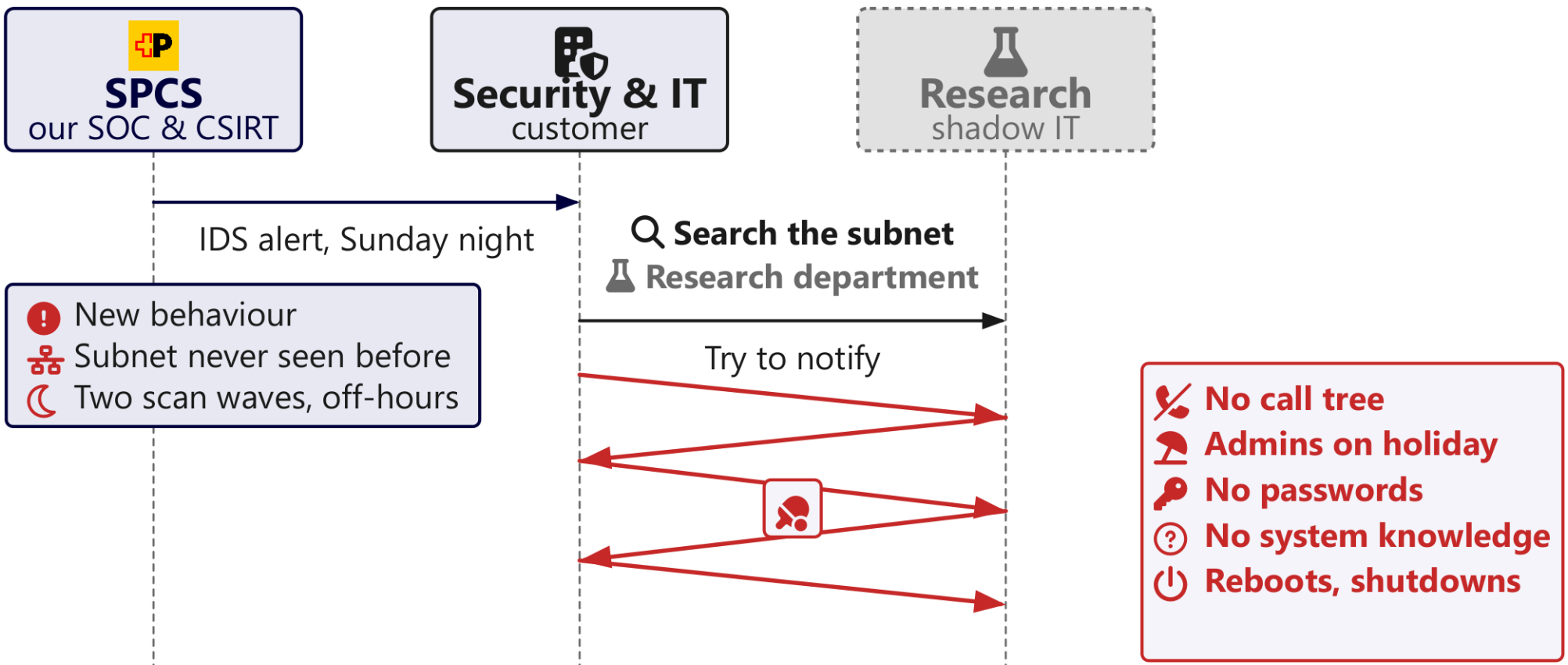
Slow escalation...

TLP:CLEAR



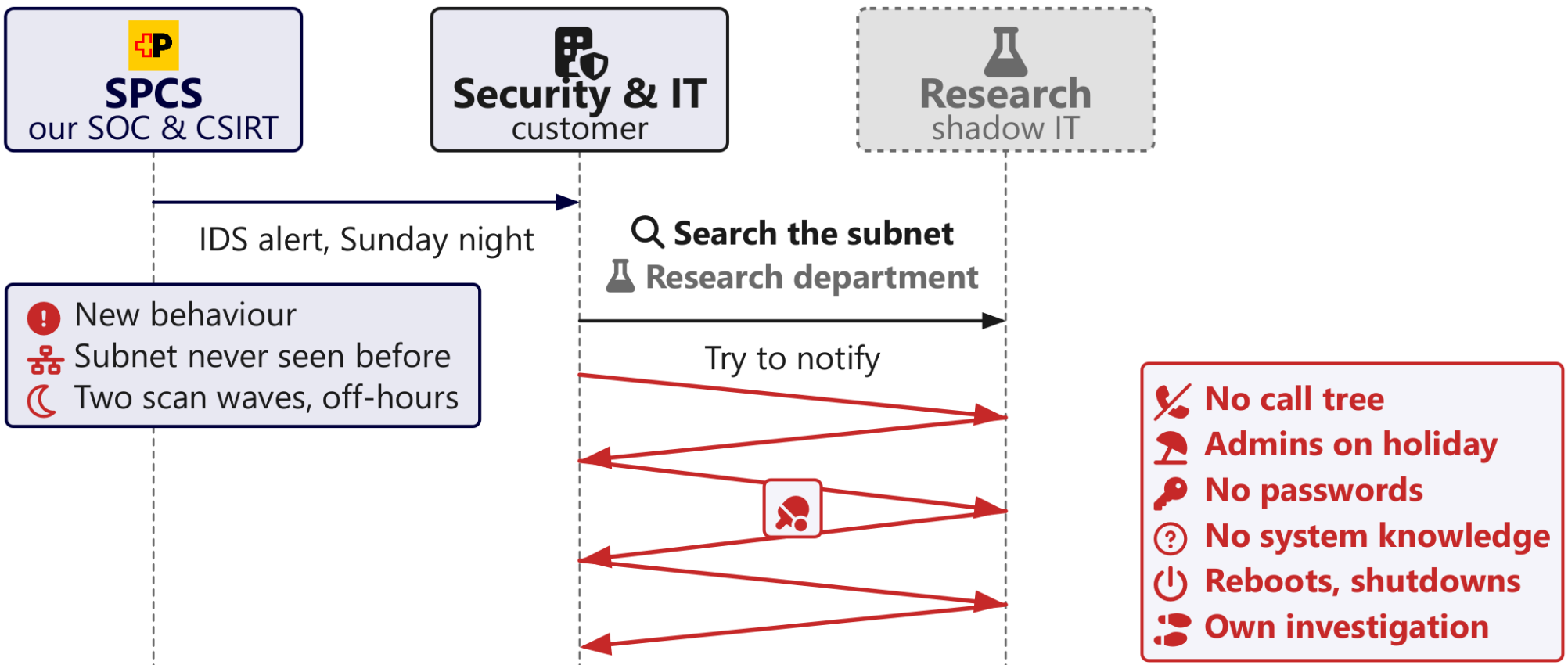
Slow escalation...

TLP:CLEAR



Slow escalation...

TLP:CLEAR



Slow escalation...

TLP:CLEAR

SPCS
our SOC & CSIRT

Security & IT
customer

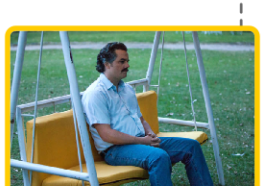
Research
shadow IT

IDS alert, Sunday night

- New behaviour
- Subnet never seen before
- Two scan waves, off-hours

Search the subnet
Research department

Try to notify

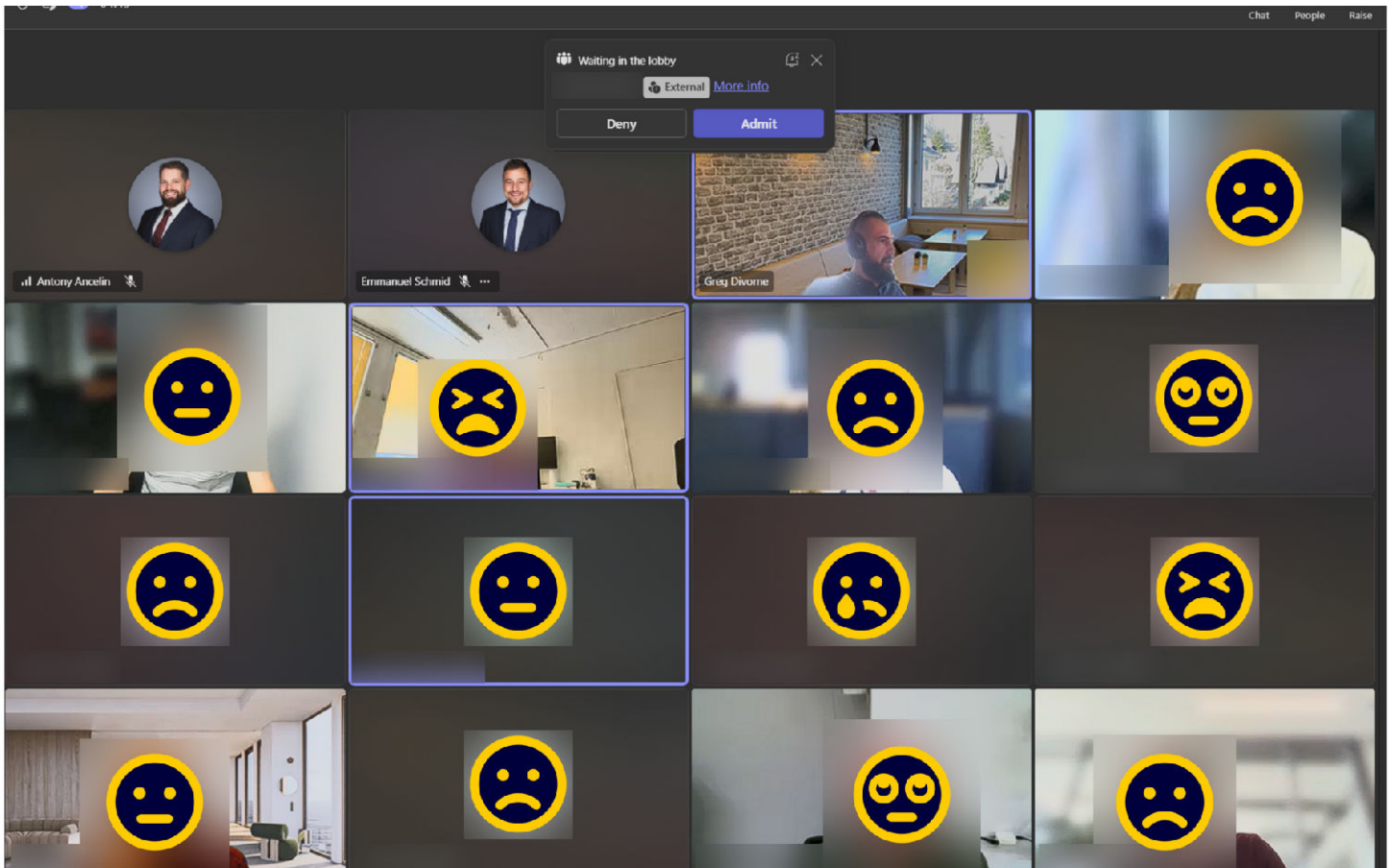


CSIRT
Escalated, +2 days

- **No call tree**
- **Admins on holiday**
- **No passwords**
- **No system knowledge**
- **Reboots, shutdowns**
- **Own investigation**

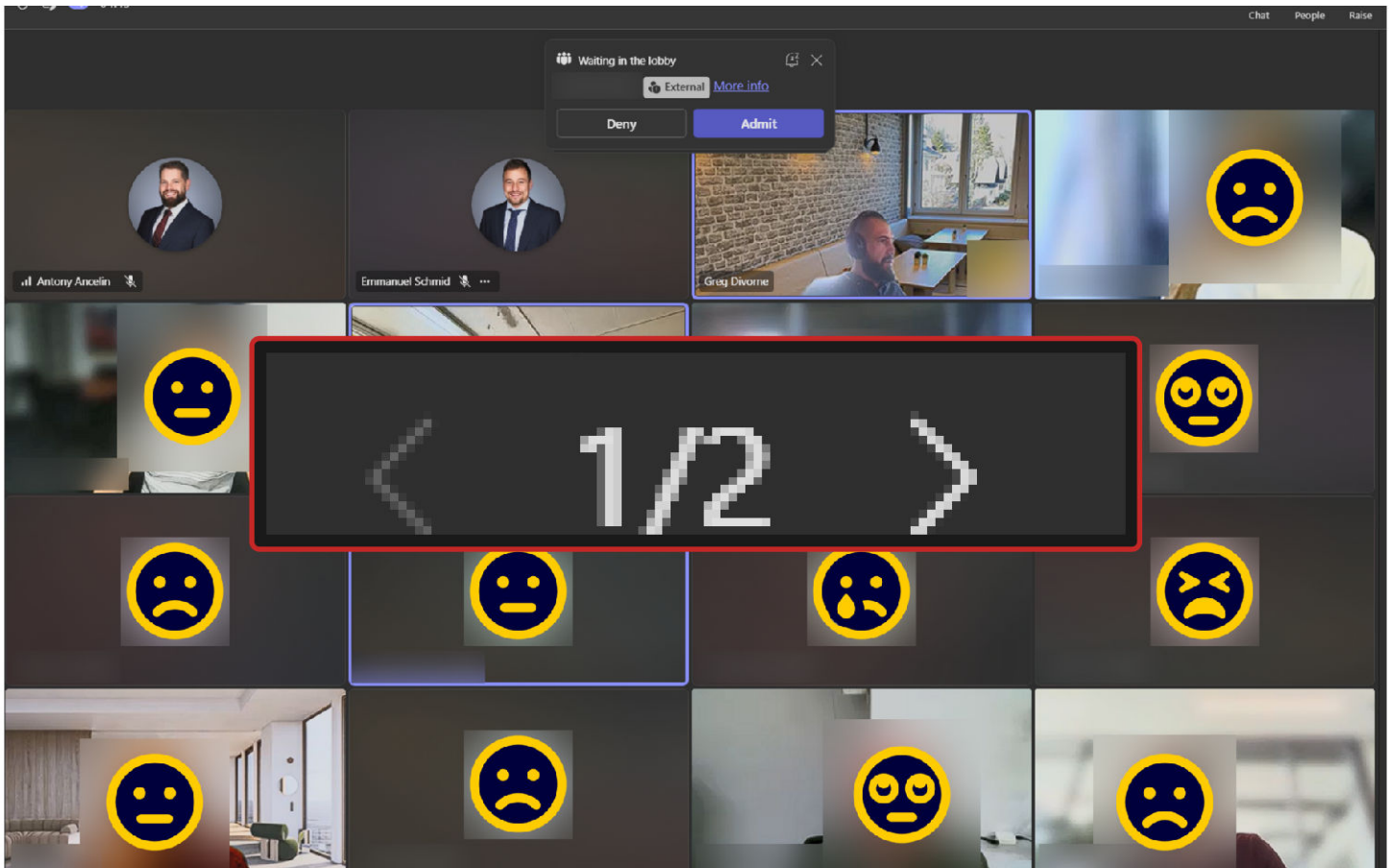
The (very) small call

TLP:CLEAR



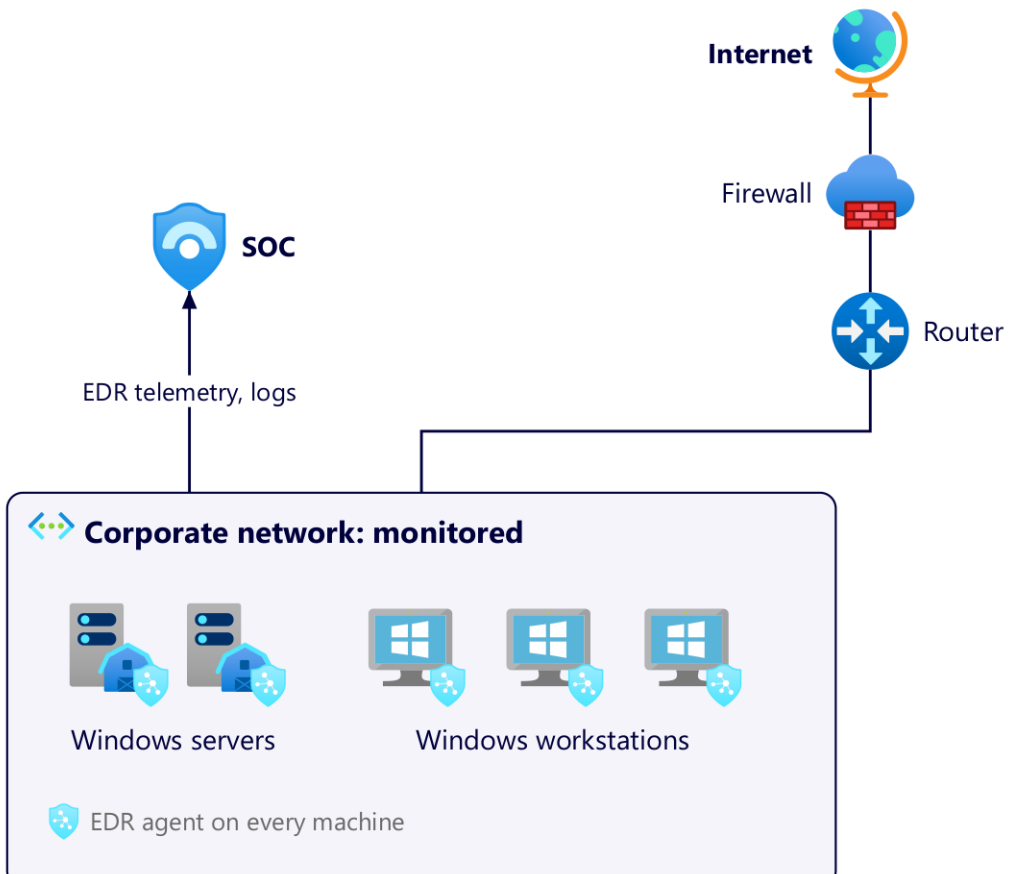
The (very) small call

TLP:CLEAR



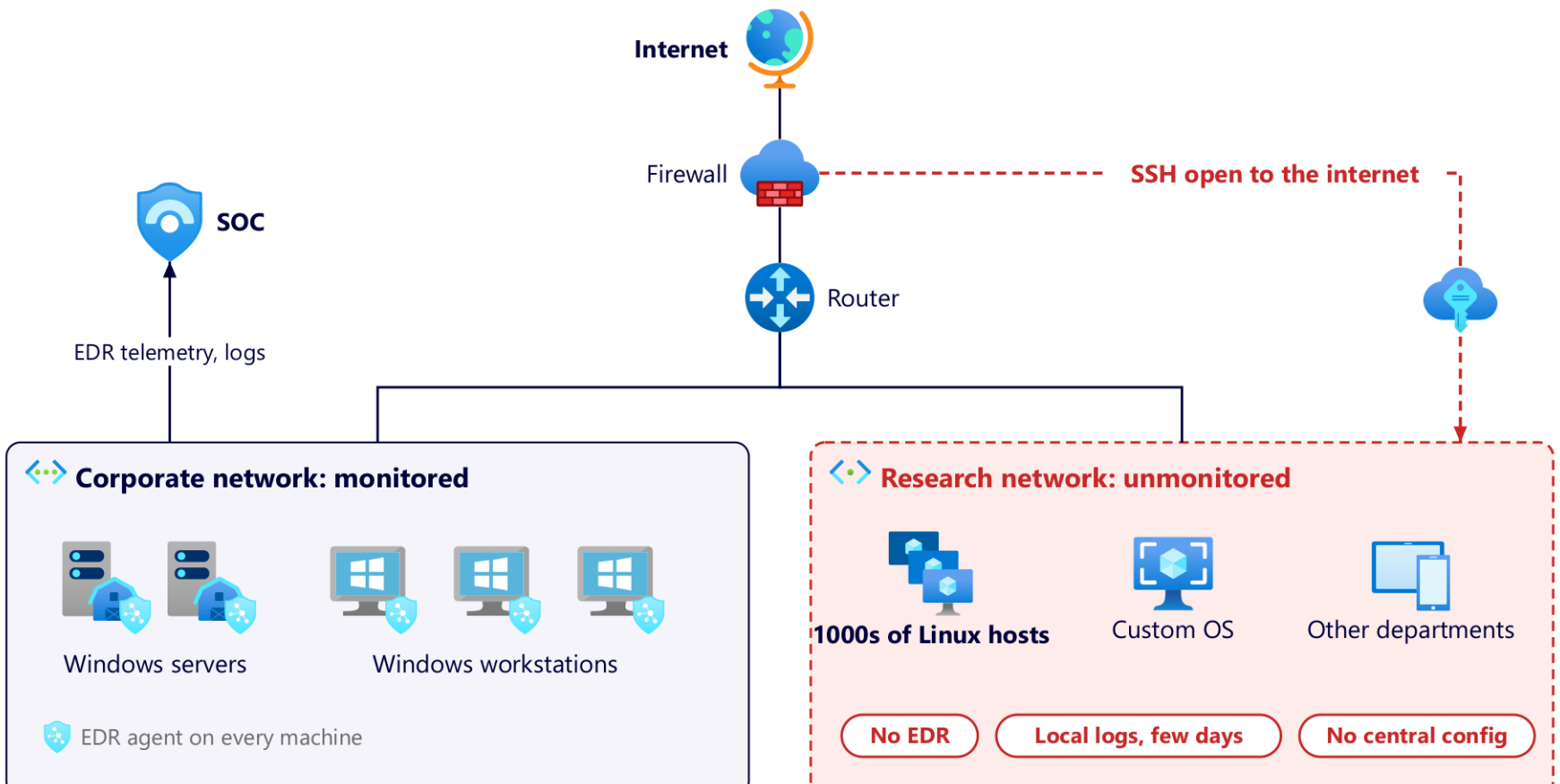
What is really there

TLP:CLEAR



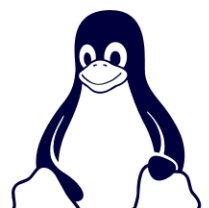
What is really there

TLP:CLEAR



Getting visibility

TLP:CLEAR



Past — **Now** — From now on

- Past artifacts, if still there
- Quarantine: nftables, iptables
- Logs raw actions
- Follow the attacker, hunt IOCs
- Containment and remediation calls

Visibility, the hard way

TLP:CLEAR

Visibility, the hard way

TLP:CLEAR

- ✕ No asset inventory
- ✕ ~5 years old, by former staff
- ✕ Admins to be found

Visibility, the hard way

TLP:CLEAR

- ✕ No asset inventory
- ✕ ~5 years old, by former staff
- ✕ Admins to be found

- ✕ No config tool, deploy by hand
- ✕ Kernels too old

Visibility, the hard way

TLP:CLEAR

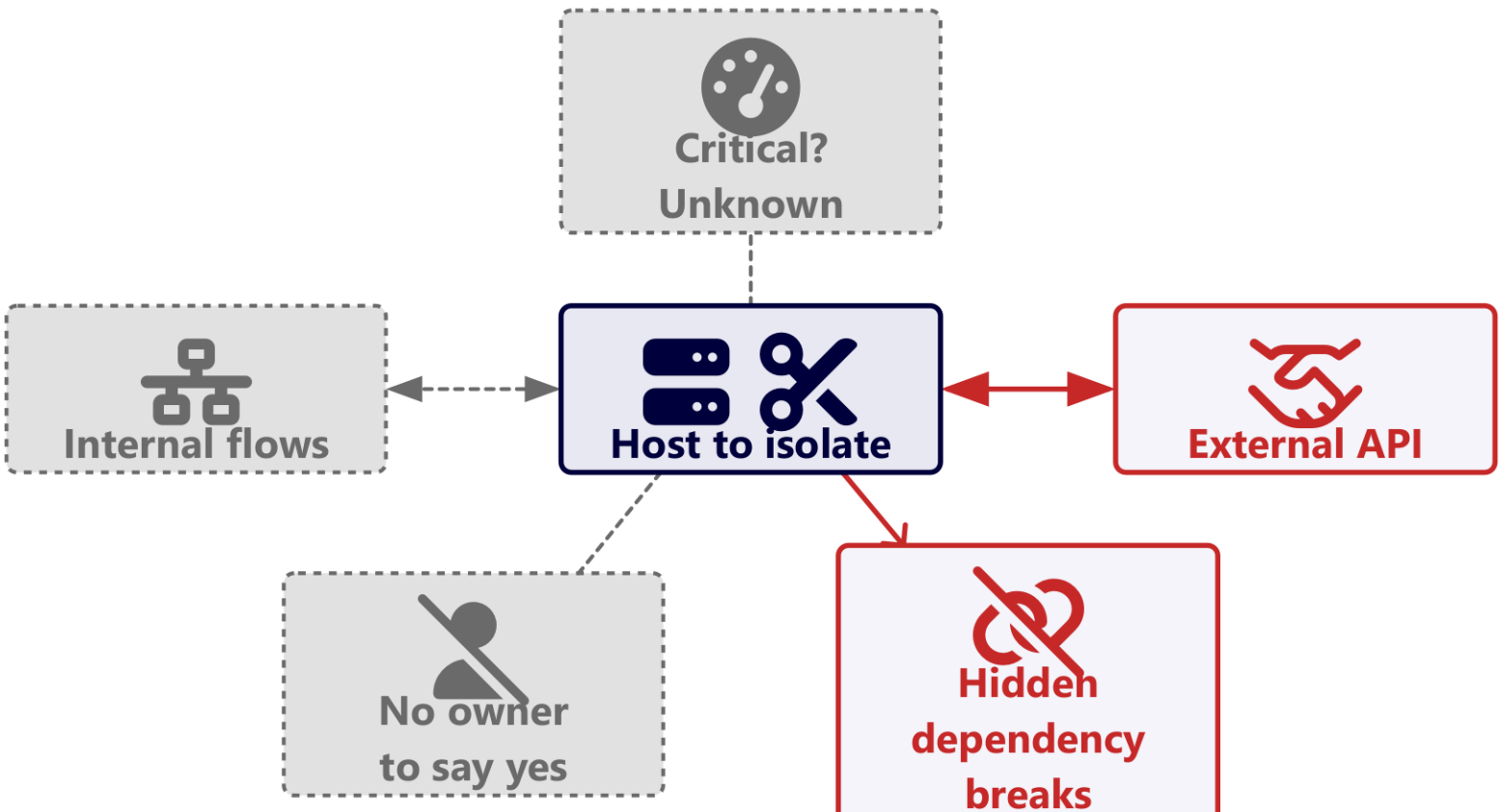
- ✕ No asset inventory
- ✕ ~5 years old, by former staff
- ✕ Admins to be found

- ✕ No config tool, deploy by hand
- ✕ Kernels too old

- ✕ Sized for the old scope
- ✕ Scaled up on the fly

Red wire or blue wire ...

TLP:CLEAR



Red wire or blue wire ...

TLP:CLEAR

Internal fl

ernal API

to say yes

breaks

Thanks for the notes

TLP:CLEAR

~1000 hosts… Which ones were hit?

Thanks for the notes

TLP:CLEAR

Staging dir, left behind — 42 entries

```
$ ls .md/
banner
banner.log
brute
...
ip-s*****
ip.txt
res.txt
scan.log
userpass.txt
```

Thanks for the notes

TLP:CLEAR

Staging dir, left behind — 42 entries

```
$ ls .md/
ba
ba
bi
.
ip-s*****
ip.txt
res.txt
scan.log
userpass.txt
```

Banner grabber — banner

```
$ strings banner | grep -A1 grabber
banner grabber by PRG
usage: %s <infile> <port> <threads>
```

Thanks for the notes

TLP:CLEAR

Staging dir, left behind — 42 entries

```
$ ls .md/
ba
ba
bi
.
ip-s
ip.t
res.txt
scan.log
userpass.txt
```

Banner grabber — banner

```
$ strings banner | grep -A1 grabber
ba
us
```

masscan results — 1605 SSH hosts

```
#masscan
banner tcp 22 10.x.x.x ssh SSH-2.0-OpenSSH_8.7
banner tcp 22 10.x.x.x ssh SSH-2.0-OpenSSH_7.4
banner tcp 22 10.x.x.x ssh SSH-2.0-OpenSSH_5.2
```

Thanks for the notes

TLP:CLEAR

Staging dir, left behind — 42 entries

```
$ ls .md/
```

Banner grabber — banner

```
$ strings banner | grep -A1 grabber
```

masscan results — 1605 SSH hosts

```
#masscan
```

Brute force, then CPU check — 80 hosts cracked

```
echo "Made in Moldova"
./haiduc 300 -b $1 pass 22 \
  "nproc;uptime;uname -m"
[+] 10.x.x.x 22 root ********
[+] 10.x.x.x 22 postgres ********
```

Thanks for the notes

TLP:CLEAR

Staging dir, left behind — 42 entries

banner

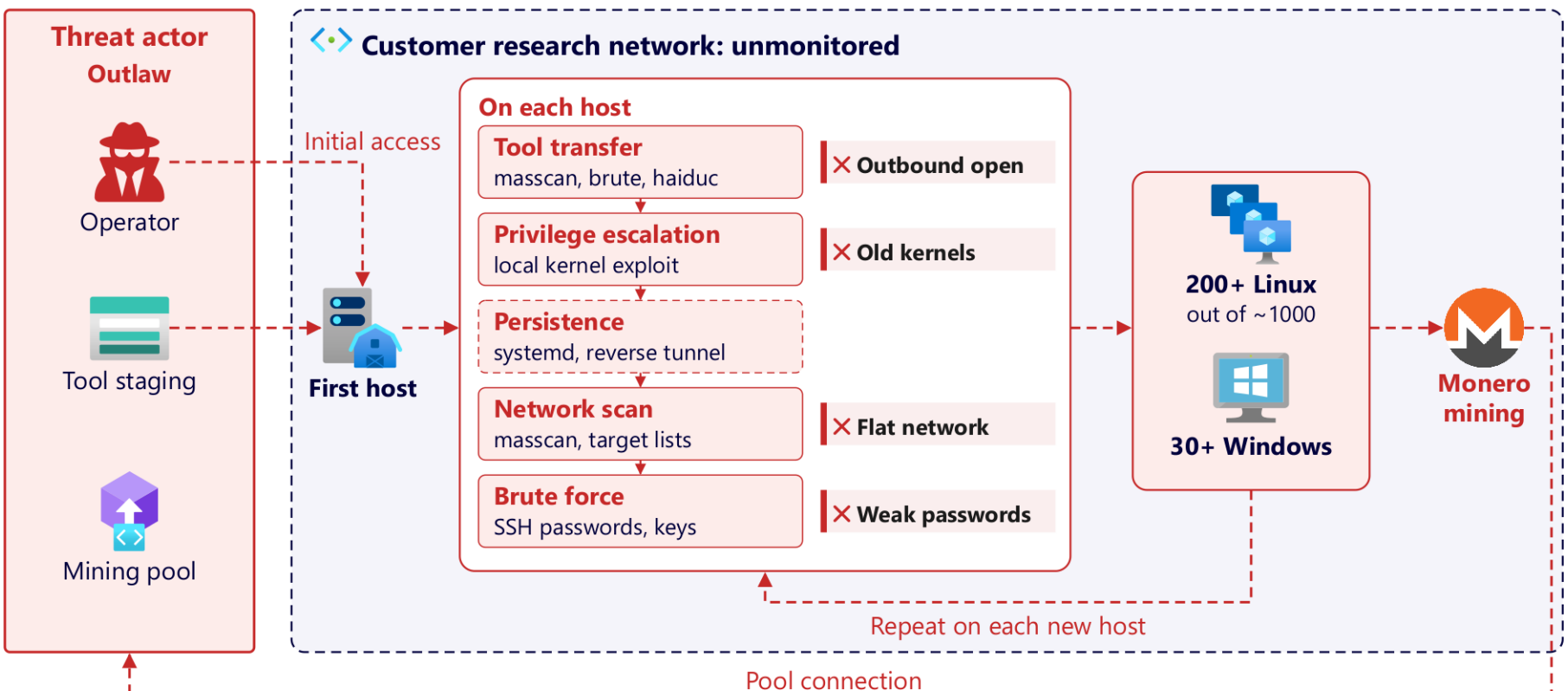
05 SSH hosts

80 hosts cracked

[+] 10.x.x.x 22 postgres ********

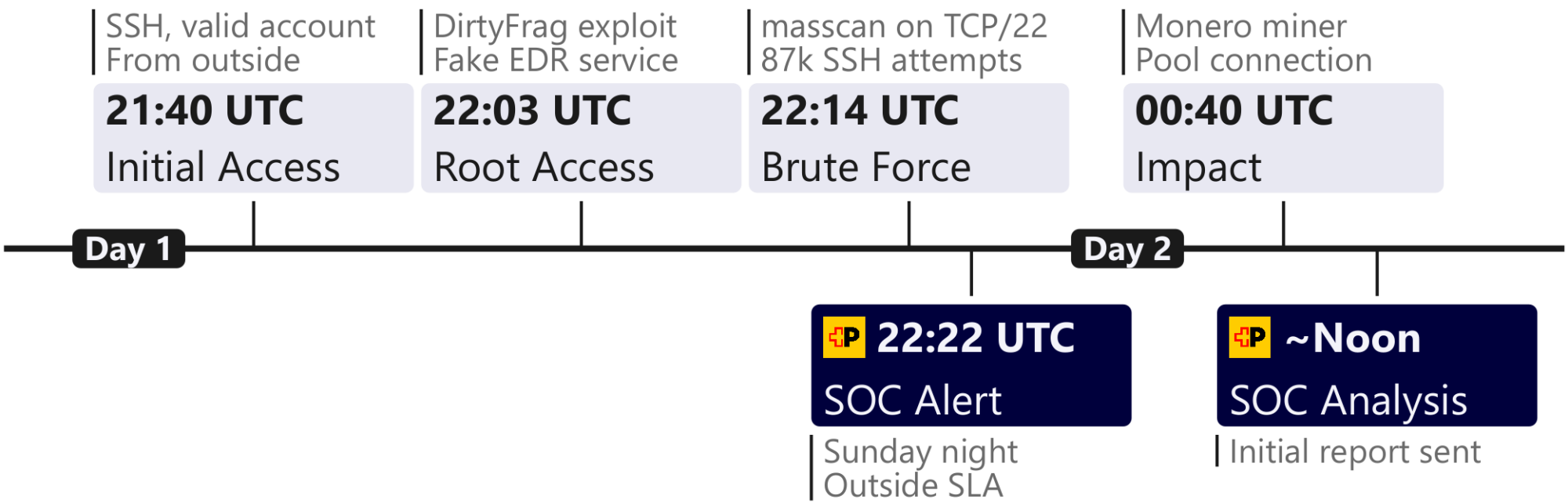
How it spread

TLP:CLEAR



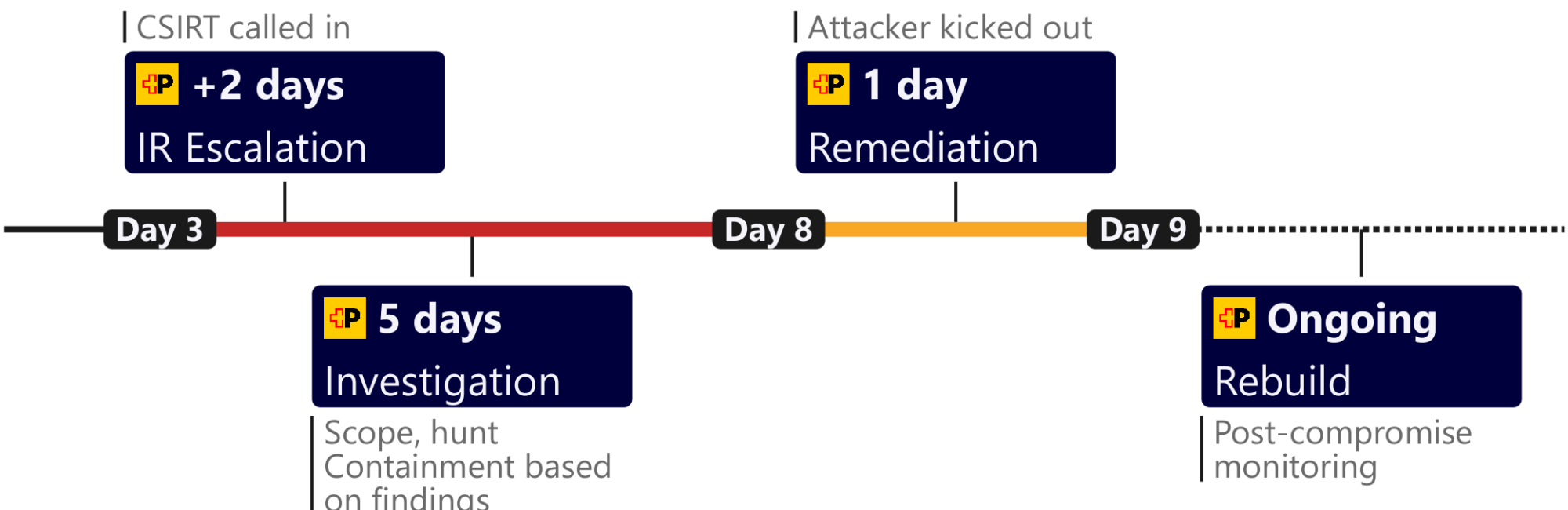
How fast it went

TLP:CLEAR



The response

TLP:CLEAR



The bigger picture

Not only a big company issue

TLP:CLEAR

10%

Of our incident response cases involve some form of shadow IT.

Other forms we see

TLP:CLEAR

Assumed contract

provider drops by,
no real contract

Merged company

its IT came along,
nobody reviewed it

Ninja project

built around security,
shipped to production

Other forms we see

TLP:CLEAR

Assumed contract
provider drops by,
no real contract

Merged company
its IT came along,
nobody reviewed it

Ninja project
built around security,
shipped to production

Ex-staff server
still running,
no owner

Exposed test/dev
open to the internet,
never patched

Why it happens

TLP:CLEAR

- [x] Deadline beats the security rules
- [x] Set up in minutes: a card, a cloud account
- [x] Asking IT feels slow, or ends in “no”
- [x] Rules unclear, or nobody checks
- [x] It works, so nobody turns it off

What it costs IR

TLP:CLEAR

Longer dwell time
attacker stays while we search

Failed recovery
no backups, rebuild from scratch

Forensic blind spots
no logs, short retention

What it costs IR

TLP:CLEAR

Longer dwell time
attacker stays while we search

False containment
unmapped system, attacker still in

Failed recovery
no backups, rebuild from scratch

Team fatigue
long days, no room for a 2nd case

Forensic blind spots
no logs, short retention

Rushed actions
a reboot or block warns the attacker

Before it happens

TLP:CLEAR

Technical

Discovery
asset inventory, scans, pentest

Alert on new assets
new subnets, unknown hosts

Baseline in place
logs, segmentation, outbound filter

IR readiness
tools ready, credentials rotated, hunt

Before it happens

TLP:CLEAR

Technical

Discovery
asset inventory, scans, pentest

Alert on new assets
new subnets, unknown hosts

Baseline in place
logs, segmentation, outbound filter

IR readiness
tools ready, credentials rotated, hunt

Governance

Define policies
what is allowed, who approves

Named owner
plus a backup

Tabletop exercise
with an unknown network in it

Written agreements
IT providers, acquired companies

Simple request process
no blame when reported

Before it happens

TLP:CLEAR

Technical

Discovery
asset inventory, scans, pentest

Alert on new assets
new subnets, unknown hosts

Baseline in place
logs, segmentation, outbound filter

IR readiness
tools ready, credentials rotated, hunt

Governance

Define policies
what is allowed, who approves

Named owner
plus a backup

Tabletop exercise
with an unknown network in it

Written agreements
IT providers, acquired companies

Simple request process
no blame when reported

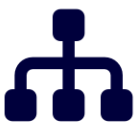
Owner refuses changes: treat it as untrusted, isolate it, monitor the border

If it happens anyway

TLP:CLEAR

Task driven

tasks and priorities,
not emotions



Work streams

divide and conquer,
no more one big call

One rep per stream

speaks and decides

Regular follow-ups

findings, actions,
blocking points

IR basics

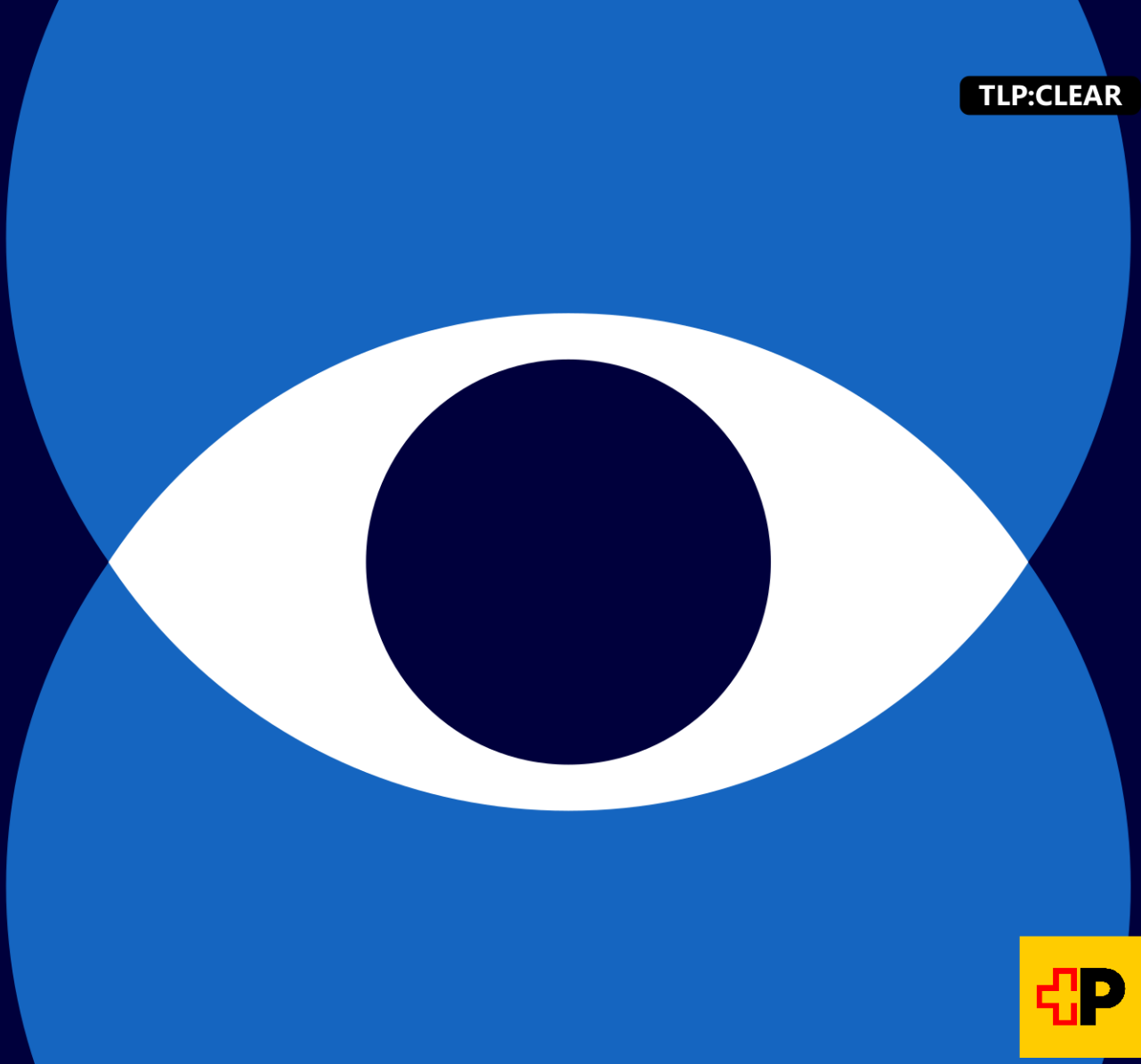
no reboot or wipe,
planned containment

So what is shadow IT?

TLP:CLEAR

One of the best backdoors an attacker can get

Swiss Post Cybersecurity

TLP:CLEAR

Danke,
Merci,
Grazie,
Thank you