Hey, Did You Hear About This New CVE?

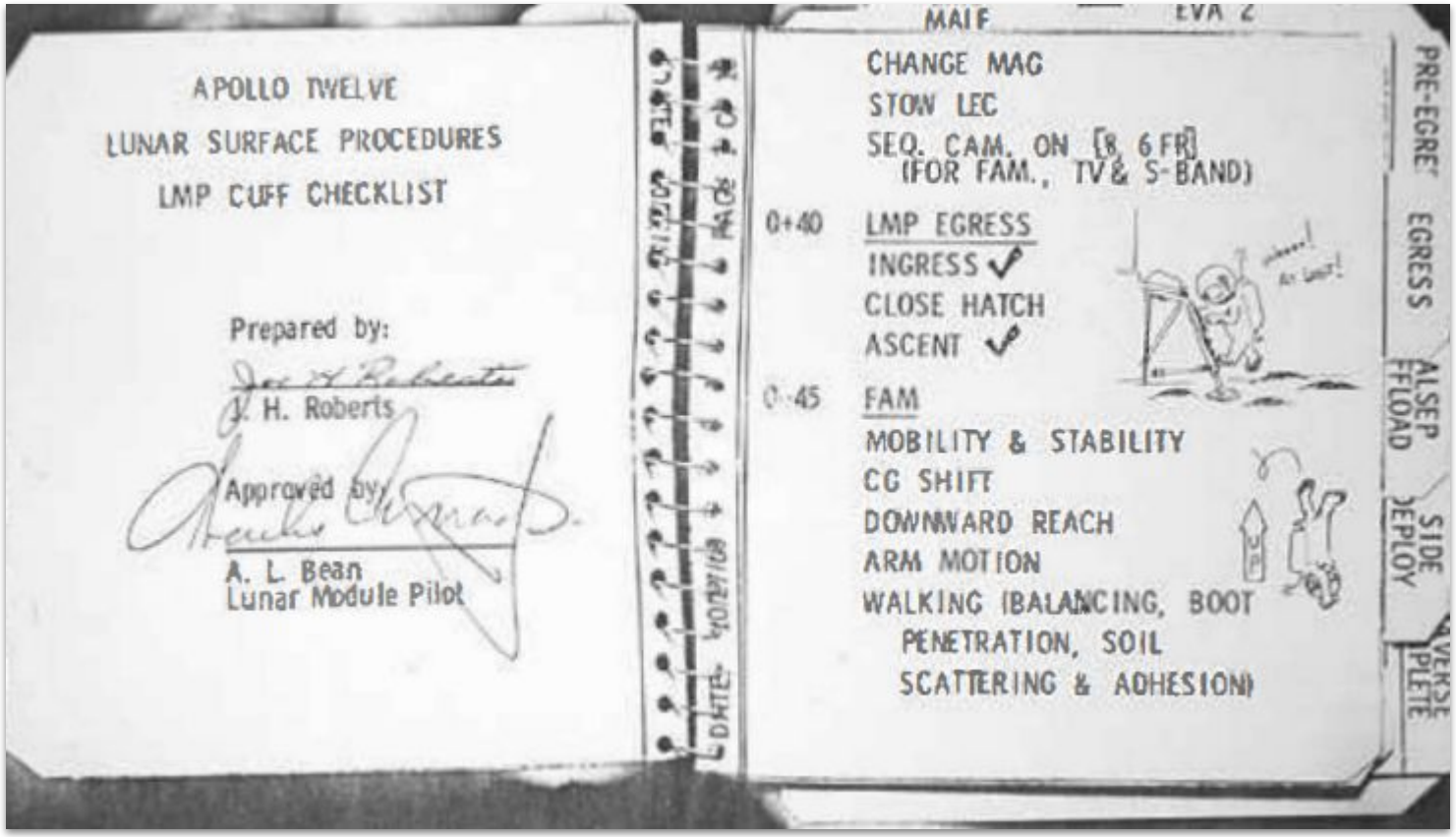
How to prepare for a security incident

Andrew Lytvynov, Gravitational & Alexandr Tcherniakhovski, Google

Agenda

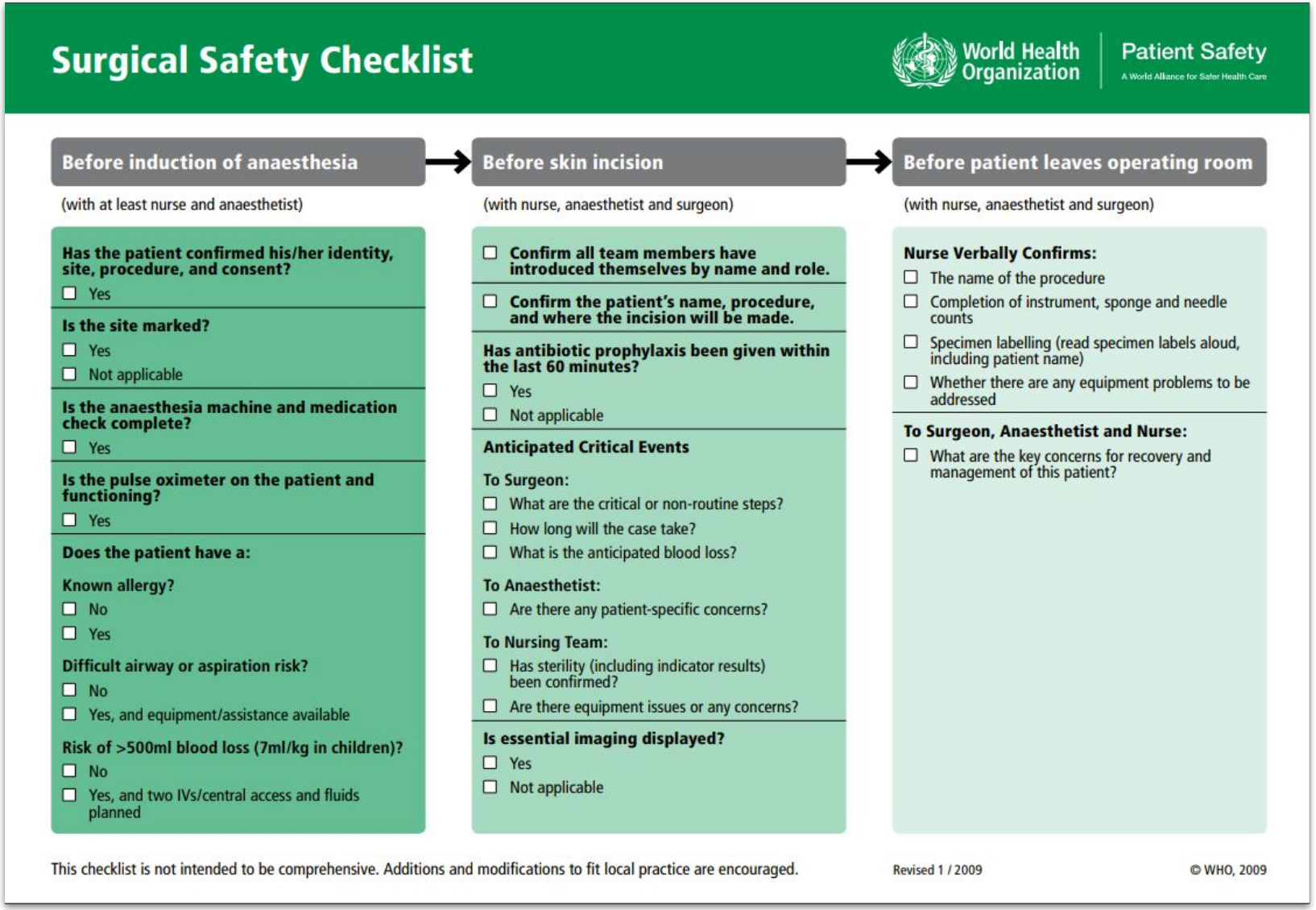
1. why checklists
2. pre-incident checklist
3. incident checklist

By Airwolfhound - commons file, CC BY-SA 2.0, https://commons.wikimedia.org/w/index.php?curid=70277974



[Apollo 12 Lunar Surface Journal : Cuff Checklists]

Photographed by Ulli Lotzmann on 15 March 2001.



Surgical Safety Checklist

World Health Organization | Patient Safety
A World Alliance for Safer Health Care

Before induction of anaesthesia

(with at least nurse and anaesthetist)

Has the patient confirmed his/her identity, site, procedure, and consent?
- ☐ Yes

Is the site marked?
- ☐ Yes
- ☐ Not applicable

Is the anaesthesia machine and medication check complete?
- ☐ Yes

Is the pulse oximeter on the patient and functioning?
- ☐ Yes

Does the patient have a:

Known allergy?
- ☐ No
- ☐ Yes

Difficult airway or aspiration risk?
- ☐ No
- ☐ Yes, and equipment/assistance available

Risk of >500ml blood loss (7ml/kg in children)?
- ☐ No
- ☐ Yes, and two IVs/central access and fluids planned

Before skin incision

(with nurse, anaesthetist and surgeon)

- ☐ **Confirm all team members have introduced themselves by name and role.**
- ☐ **Confirm the patient's name, procedure, and where the incision will be made.**

Has antibiotic prophylaxis been given within the last 60 minutes?
- ☐ Yes
- ☐ Not applicable

Anticipated Critical Events

To Surgeon:
- ☐ What are the critical or non-routine steps?
- ☐ How long will the case take?
- ☐ What is the anticipated blood loss?

To Anaesthetist:
- ☐ Are there any patient-specific concerns?

To Nursing Team:
- ☐ Has sterility (including indicator results) been confirmed?
- ☐ Are there equipment issues or any concerns?

Is essential imaging displayed?
- ☐ Yes
- ☐ Not applicable

Before patient leaves operating room

(with nurse, anaesthetist and surgeon)

Nurse Verbally Confirms:
- ☐ The name of the procedure
- ☐ Completion of instrument, sponge and needle counts
- ☐ Specimen labelling (read specimen labels aloud, including patient name)
- ☐ Whether there are any equipment problems to be addressed

To Surgeon, Anaesthetist and Nurse:
- ☐ What are the key concerns for recovery and management of this patient?

This checklist is not intended to be comprehensive. Additions and modifications to fit local practice are encouraged.

Revised 1 / 2009

Source: https://www.who.int/patientsafety/safesurgery/checklist/en/

Pre-Incident Checklists

"We need a different strategy for overcoming failures, one that builds on the experience and take advantage of the knowledge people have but somehow also makes up for our inevitable human inadequacies".

Gawande, A. (2014). The checklist manifesto: How to get things right.

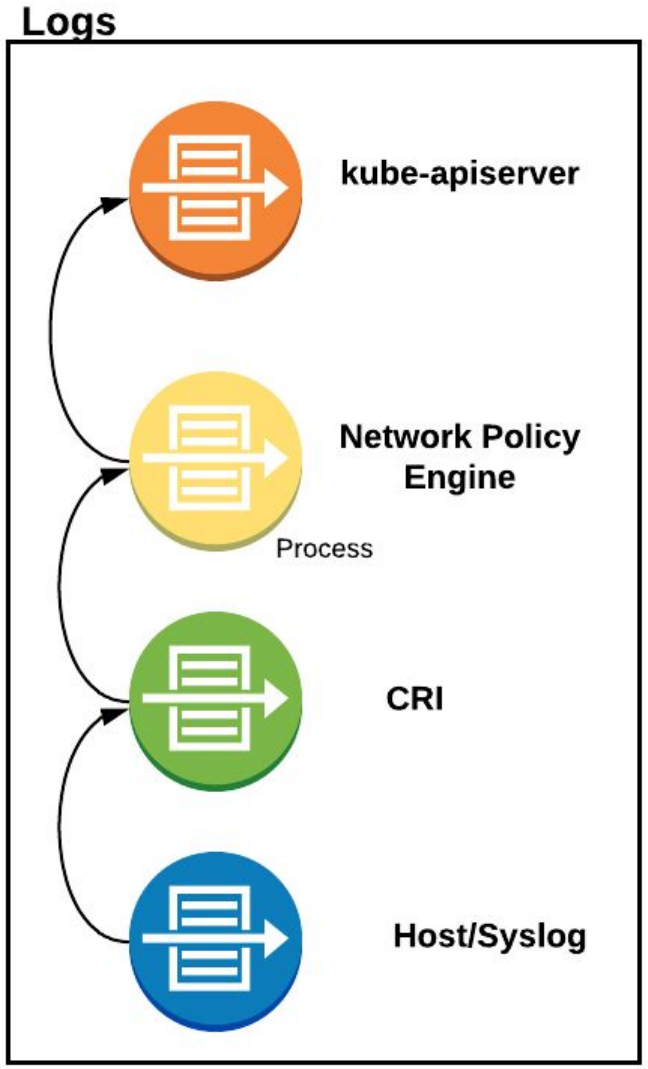
Dealing with incidents in K8S is hard

- Containers are ephemeral
- Internal IP Addresses change frequently
- OS Identities are often the same
- No direct link between the events in the Control Plane and containers

We consider a discovery of a vulnerability within GKE, Kubernetes or its ecosystem to be a Security Incident.

Services Owners' Pre-Incident

- RBAC
- Network
- Pod
- Image



https://www.cisecurity.org/benchmark/kubernetes/

Services Owners' Pre-Incident Checklist

RBAC

- ❑ Least Privileged RBAC Profile
- ❑ Kube-apiserver audit log enabled
- ❑ Alerts trigger on access deny

Services Owners' Pre-Incident Checklist

KubeCon CloudNativeCon Europe 2020 Virtual

```
apiVersion: audit.k8s.io/v1
kind: Policy
rules:
  - level: Metadata
    resources:
    - group: ""
      resources: [
        "secrets",
        "configmaps"
      ]
```

https://kubernetes.io/docs/tasks/debug-application-cluster/audit/

Services Owners' Pre-Incident Checklist

Network

- ❑ Expected Network flow diagrams
- ❑ NetworkPolicy (at least in audit mode)
- ❑ Alerts on access denied

Services Owners' Pre-Incident Checklist

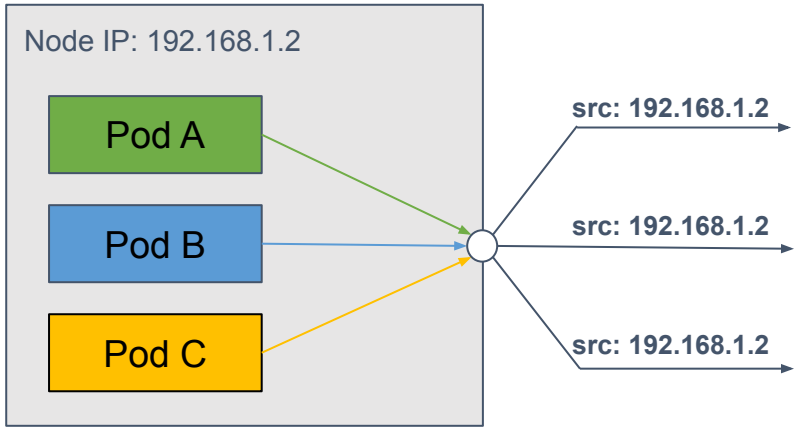

```
apiVersion: projectcalico.org/v3
kind: NetworkPolicy
Metadata:
  name: allow-tcp-6379
  namespace: production
Spec:
  selector: role == 'database'
  types:
  - Ingress
  - Egress
  ingress:
  - action: Log
    protocol: TCP
    source:
      selector: role == 'frontend'
```

https://docs.projectcalico.org/security/calico-network-policy

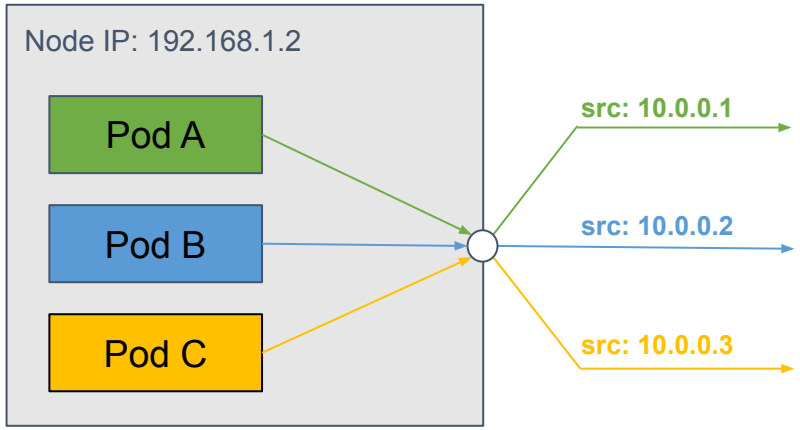
Services Owners' Pre-Incident Checklist

KubeCon CloudNativeCon Europe 2020 Virtual

- hostNetwork:true



- hostNetwork:false



https://kubernetes.io/docs/concepts/configuration/overview/#services

Services Owners' Pre-Incident Checklist

POD

- ❑ runAsNonRoot:true
- ❑ requiredDropCabilities:['ALL']
- ❑ allowPrivilegeEscalation: false

https://kubernetes.io/blog/2016/08/security-best-practices-kubernetes-deployment/

Services Owners' Pre-Incident Checklist

Image

- ❑ Distroless or Scratch
- ❑ Link between the binaries and Build Manifest

https://github.com/GoogleContainerTools/distroless

Services Owners' Pre-Incident Checklist


```
module github.com/GoogleCloudPlatform/k8s-cloudkms-plugin

go 1.13

require (
        cloud.google.com/go v0.47.0 // indirect
        github.com/gogo/protobuf v1.3.1
        github.com/golang/glog v0.0.0-20160126235308-23def4e6c14b
        github.com/golang/groupcache v0.0.0-20191027212112-611e8accdfc9 // indirect
        github.com/golang/protobuf v1.3.2
        github.com/google/go-cmp v0.3.1
        github.com/google/go-tpm v0.2.0
        github.com/phayes/freeport v0.0.0-20180830031419-95f893ade6f2
        github.com/prometheus/client_golang v1.2.1
        github.com/prometheus/client_model v0.0.0-20190812154241-14fe0d1b01d4
        go.opencensus.io v0.22.2 // indirect
        golang.org/x/net v0.0.0-20191109021931-daa7c04131f5
        golang.org/x/oauth2 v0.0.0-20190604053449-0f29369cfe45
        golang.org/x/sys v0.0.0-20191105231009-c1f44814a5cd // indirect
```

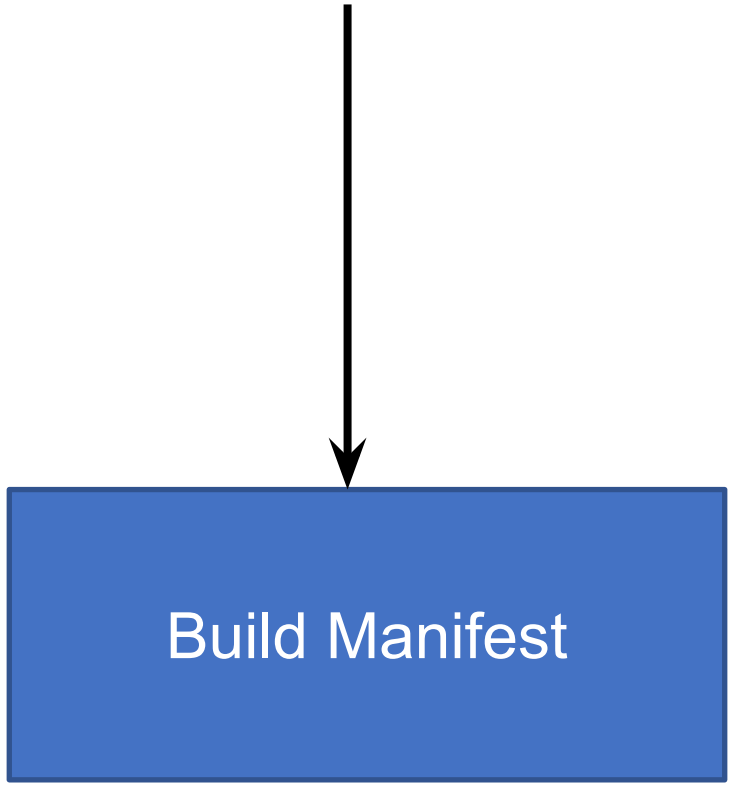
Image

https://blog.golang.org/using-go-modules

Services Owners' Pre-Incident Checklist

Image

http://gcr.io/my-project/my-image:tag1



Incident Checklist

Incident checklist

1. reproduce
2. create comms
3. establish ownership
4. mitigation
5. aftermath

1. Reproduce

- What can an attacker do?
  - what's the blast radius?
  - calculate the CVSS score
- Is the vulnerability real?
  - make sure it actually affects you
- Can you trigger it?
  - write down minimal repro
- What are the symptoms of exploit?

Image by Enrique Harris https://www.wallpaperflare.com/a-blurred-image-of-a-yellow-question-mark-box-from-mario-wallpaper-wallpaper-eqqpj

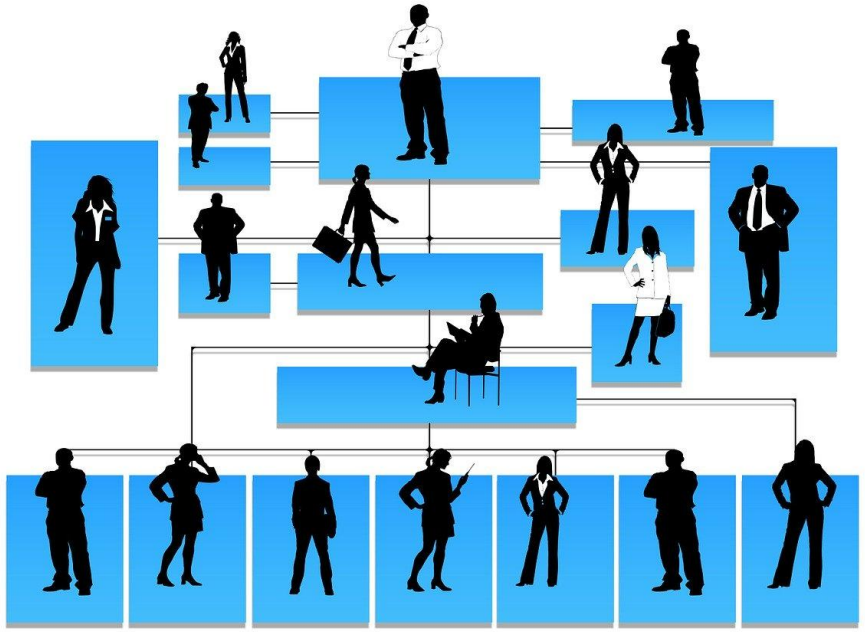
2. Create comms

- ❑ Create a (restricted) shared doc
  - ❑ copy from template
  - ❑ document all info and timeline
- ❑ Create a (restricted) chat room*
- ❑ (optional) Pick a CODEWORD
  - ❑ make sure it wasn't used before

*but record important info in doc

Image by The Library of Virginia https://commons.wikimedia.org/wiki/File:Radio_room_(2899347850).jpg

3. Establish ownership



- ❑ Incident Commander (IC)
  - coordinator and decision maker
- ❑ Comms lead
  - notifies affected users
- ❑ SMEs
  - advise and/or fix
- ❑ Ops lead (optional)
  - handles mitigation and rollout

Image by Gerd Altmann from Pixabay

4. Analyze and mitigate

- Mitigate
  - short-term fix
  - long-term ideas
- Rollout
  - pick regular or fast path
  - avoid outages
- Wait for rollout to complete
  - Declare all clear

Image by US Air Force https://www.afrc.af.mil/News/Art/igphoto/2000049526/

5. Aftermath

- Investigate actual compromises
  - collect relevant audit logs
  - number of users affected
  - if not zero, plan next steps
- Postmortem
  - root cause
  - timeline
  - affected users
  - action items

Image by US Air Force https://www.osi.af.mil/News/Article-Display/Article/861097/osi-agents-committed-to-the-challenge/

"We are all plagued by failures—by missed subtleties, overlooked knowledge, and outright errors. For the most part, we have imagined that little can be done beyond working harder... We are not in the habit of thinking the way the army pilots did as they looked upon their shiny new Model 299 bomber... They too could have decided just to "try harder"... Instead they chose to accept their fallibilities. They recognized the simplicity and power of using a checklist.".

Gawande, A. (2014). The checklist manifesto: How to get things right.

References

- Atul Gawande: The Checklist Manifesto
- Kubernetes audit logging
- Network logging via Calico NetworkPolicy
- gosystract - find all syscalls a Go binary can make
- Incident doc template
- CVSS calculator
- Guide for postmortems


KubeCon
CloudNativeCon
Europe 2020
Virtual
HELM
KEEP CLOUD NATIVE
CONNECTED