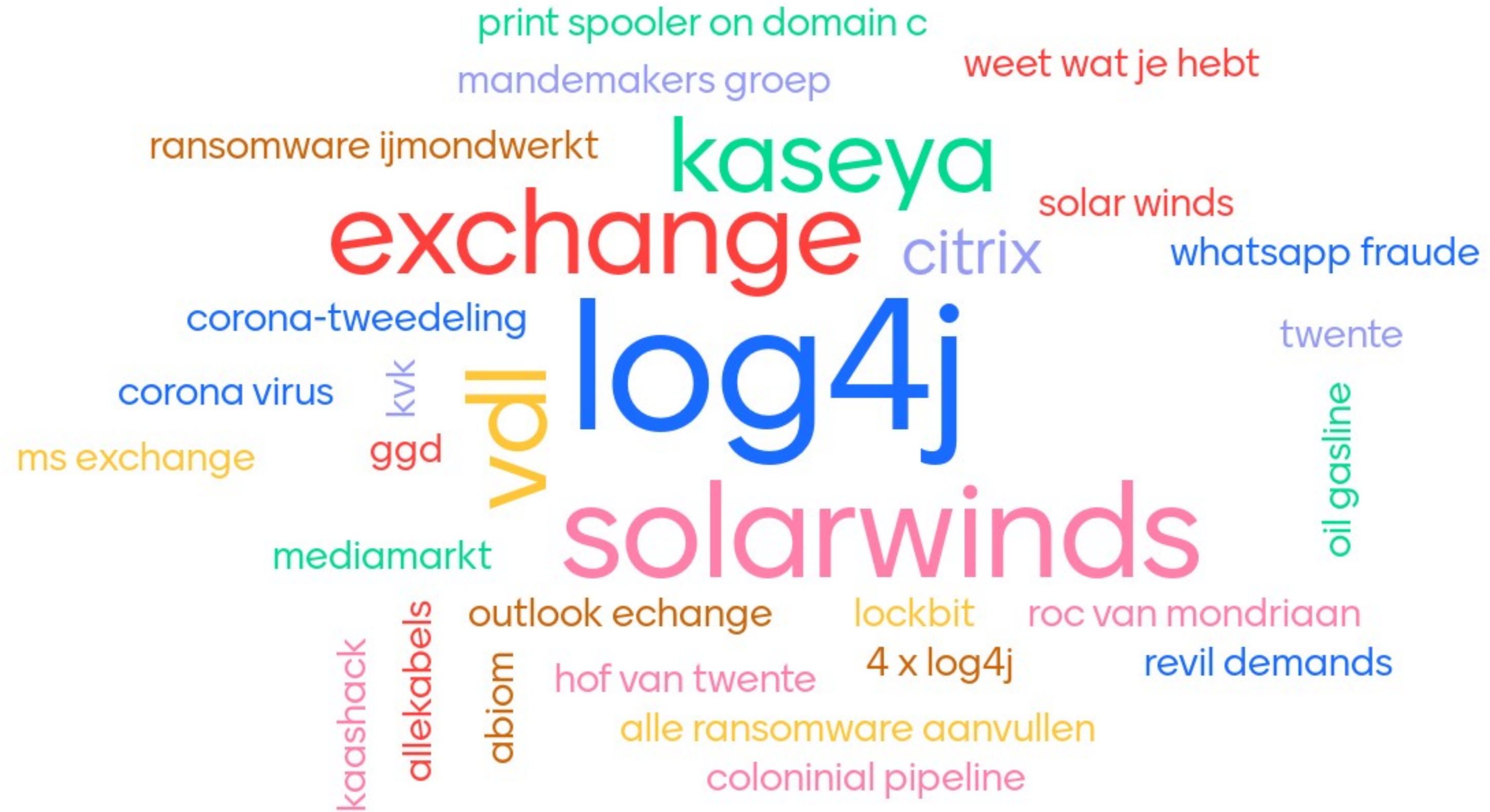


# Wat is voor jou het grootste Security incident van 2021?



# Welke les heb je het afgelopen jaar geleerd van Security incidenten ?

Oefenen

Be prepared

Patch management

Patchen

Zo min mogelijk openzetten naar binnen

a job in security is a job for life :)

Neemt toe

Patchen, patchen en monitoren

Never waiste a good crisis for getting thing done :-)



# Welke les heb je het afgelopen jaar geleerd van Security incidenten ?

De basis op orde

Stay calm

Weten wat je hebt en wie ervoor verantwoordelijk is.

Patchen en blijven patchen

Patchmanagement

Overzicht in assets is key om snel te handelen

Libraries goed blijven updaten en op de hoogte blijven door de goede kanalen te volgen.

Patchen, MFA

AWARENESS



# Welke les heb je het afgelopen jaar geleerd van Security incidenten ?

Cultuur en BasisHygiene

We kunnen uren blijven maken

Patchen

Werelden verbinden!

patchen!!!!

Testen loont!

Patchen

Asset management

Oefenen



# Welke les heb je het afgelopen jaar geleerd van Security incidenten ?

Vulnerability management

vergroot biodiversiteit aan systemen

Verkeersanalyse

Patchen en monitoren / prevention

Asset management

Backup

mfa

patchen en monitoren

Crisismanagement

# Welke les heb je het afgelopen jaar geleerd van Security incidenten ?

Patchmanagement en Vulnerability scanning zijn key

Integraal security oppakken met de business

Integrale security aanpak (prevent, detect, response + governance)

Dat tools als Teams erg helpen om snel te communiceren en we elkaar snel kunnen vinden

Patch, monitor en beperk toegang

Voor veel bedrijven is information security nog een onvolwassen discipline

TIBER

patchen

Backup restore oefenen

# Welke les heb je het afgelopen jaar geleerd van Security incidenten ?

Verbeteren van detectie, response en recovery

Prepare, prepare, prepare

Offline backup

soc en netwerkmonitoring

Niet onderschatten, voorbereid zijn op response

Feitelijke weerbaarheid is belangrijker dan compliancy aan normen

Awarenes

Patch Management / Incident Response

Supply chain in kaart brengen



# Welke les heb je het afgelopen jaar geleerd van Security incidenten ?

Offline Backups

Don't trust, verify

Zero Trust

Have a well-organized SIEM/SOC in operation!

Snelheid en bewustzijn dat je slachtoffer kunt worden

ingress en egress detection (monitoring)

CERT en SOC up & running

De basis op orde.

Open communicatie over Lessons learned. Oefenen, zero days niet achterhouden, maar zo snel mogelijk melden

# Welke les heb je het afgelopen jaar geleerd van Security incidenten ?

Identities management

Patchen en testen

MFA

Blijf de actualiteit op de voet volgen en patch patch patch

Asset maintenance

BC:DR

recoverability: offline of echte immutable backups

SBOM

Inzicht Cloud afhankelijkheid

# Welke les heb je het afgelopen jaar geleerd van Security incidenten ?

Sbom

Cyber security is zorg van hele organisatie, en niet alleen it.

Werkende restore van backups en weten hoe Lang dit duurt.

Bcm



**Bedankt!**

