



# Share experience. Build resilience

Welcome to SECCON NL 2022

digital trust  
center.



HSD  
securitydelta.nl

CYBERVEILIG  
NEDERLAND



Nationaal Cyber Security Centrum  
Ministerie van Veiligheid en Justitie

telindus  
a Proximus company

avit

CISCO  
SECURE

“This is why you’ll fail”

– Yoda –

Tijme Gommers  
Product Lead Adversary Simulation  
Northwave Security













Melissa van Loenen

Aan: Tijme



Ma 29-8-2022 16:45

Dear Tijme,

The board of Cisco would like to gain more insight into your productivity at work. That is why the management asked Survi Research to perform an Employee Productivity Survey (EPS).

Our recent research shows that management does not always know how productive certain employees are, and that this only moderately translates into a reward at the end of the year. Survi Research helps us measure productivity within Cisco, and will be a tool for you to show your performance to your manager.

Besides the fact that this performance indicator can help you at the end of the year, as a token of appreciation we will also raffle a Macbook Pro among the first 25 participants of the survey.

Click [here](#) to start the survey.

When logging in, make sure that the link starts with https and has a green lock next to it. Although the survey is anonymous, we ask you to authenticate using your Cisco account, to prevent multiple registrations and other fraud.

Yours sincerely,

**Melissa van Loenen**

Manager Customer Success

Survi Research, Inc.







Melissa van Loenen

Aan: Tijme



Ma 29-8-2022 16:45

Dear Tijme,

The board of Cisco would like to gain more insight into your productivity at work. That is why the management asked Survi Research to perform an Employee Productivity Survey (EPS).

Our recent research shows that management does not always know how productive certain employees are, and that this only moderately translates into a reward at the end of the year. Survi Research helps us measure productivity within Cisco, and will be a tool for you to show your performance to your manager.

**As a token of appreciation we will also raffle a Macbook Pro among the first 25 participants of the survey.**

Click [here](#) to start the survey.

When logging in, make sure that the link starts with https and has a green lock next to it. Although the survey is anonymous, we ask you to authenticate using your Cisco account, to prevent multiple registrations and other fraud.

Yours sincerely,

**Melissa van Loenen**

Manager Customer Success

Survi Research, Inc.





Melissa van Loenen

Aan: Tijme



Ma 29-8-2022 16:45

Dear Tijme,

The board of Cisco would like to gain more insight into your productivity at work. That is why the management asked Survi Research to perform an Employee Productivity Survey (EPS).

Our recent research shows that management does not always know how productive certain employees are, and that this only moderately translates into a reward at the end of the year. Survi Research helps us measure productivity within Cisco, and will be a tool for you to show your performance to your manager.

Besides the fact that this performance indicator can help you at the end of the year, as a token of appreciation we will also raffle a Macbook Pro among the first 25 participants of the survey.

Click [here](#) to start the survey.

When logging in, make sure that the link starts with https and has a green lock next to it. Although the survey is anonymous, we ask you to authenticate using your Cisco account, to prevent multiple registrations and other fraud.

Yours sincerely,

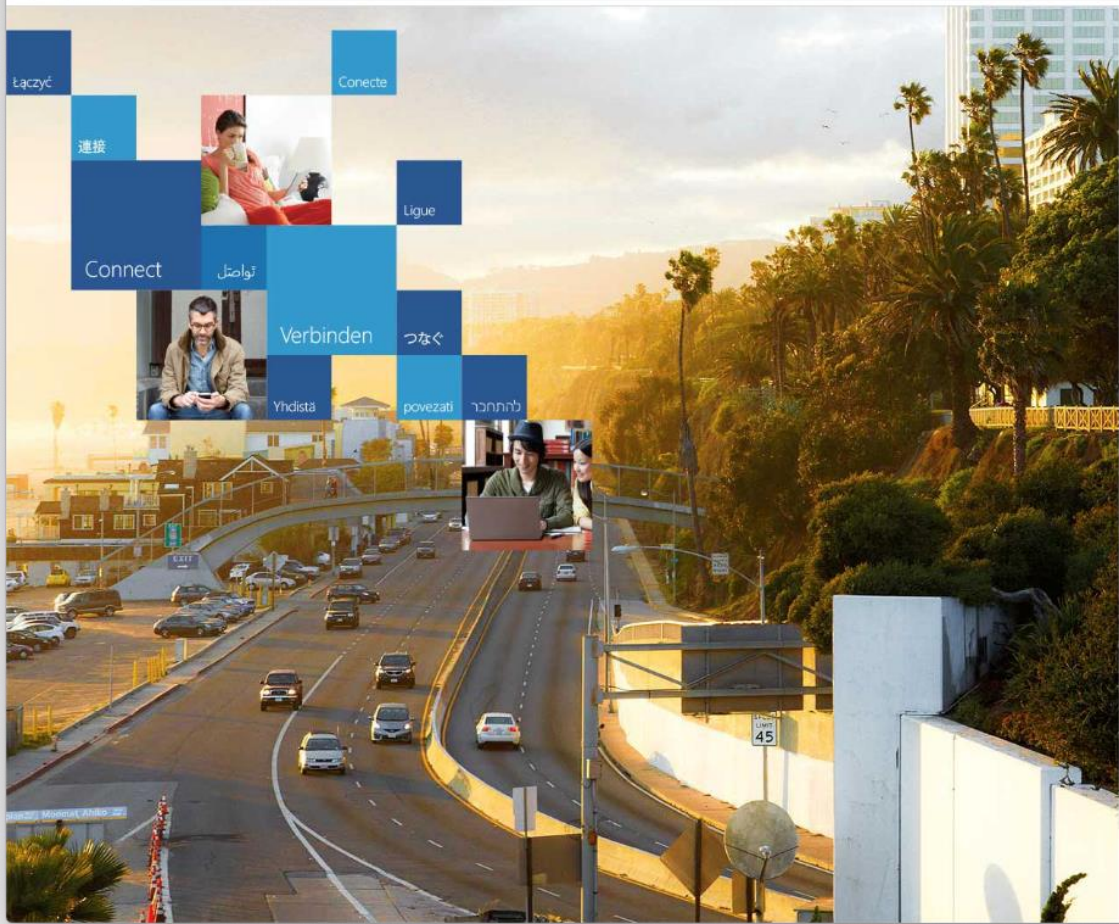
**Melissa van Loenen**

Manager Customer Success

Survi Research, Inc.







# Office 365

Sign in with your organizational account

**Sign In**

Keep me signed in

## Approve sign-in?

Northwave  
tijme.gommers@northwave.nl

Deny

Approve

Mail - Outlook

outlook.office.com/mail/inbox/id/AAQkADg2Mjg3Yt1LWFjYWQ1NDcxY111ZDg4LT10MThmMjQwNzBmMQAQABo%2FKqFhUTZBl03a4jpn05E%3D

Outlook Search

New message Delete Archive Junk Sweep Move to Categorize Snooze Undo

1/2 Tomorrow 9:30 AM

Favorites

- Inbox 2039
- Sent Items 47
- Drafts
- Add favorite

Folders

- Inbox 2039
- Drafts
- Sent Items 47
- Deleted Items 1430
- Junk Email 50
- Archive

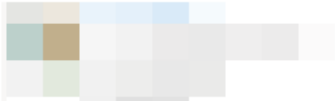
Focused Other Filter

1/2

Tomorrow 9:30 AM



## Mail during my holiday break



Hi Karl,

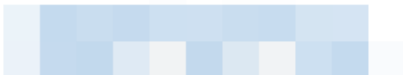
I am just finishing up my todo list for today. I will be at the beach for the next two weeks ☀️!

Could you keep an eye on my inbox while I am enjoying my holiday? My password is Danielle1983!

Talk to you at lunch!

Thanks!

Kind regards,





# 73%

of the e-mail inboxes contain (sensitive) data about crown jewels



# 100%

success rate of phishing attacks



An aerial photograph of a small boat on a vast, deep blue ocean. The boat is positioned on the left side of the frame, leaving a white wake behind it. The water's color transitions from a lighter turquoise on the left to a darker, deeper blue on the right. The overall scene is serene and expansive.

# 95%

persistence access after 3 weeks



## HAVE A PHISHING ACTION PLAN

### BUSINESS

- Have an out of band channel to alert phishing victims.
- Make sure employees are familiar with your phishing procedures.

### BYTES

- Block access to the phishing website.
- Pro-actively perform password resets of affected accounts.
- Use passwordless authentication.

### BEHAVIOUR

- Teach users how to recognize phishing.
- Instruct users on how and where to report suspicious e-mails.







Please log on

User name

Password

Log On

=67E F?DFAA@CE =6>FCD :? 3@E9 D:K6 2?5 2AA62C2?46[ E96J 2=D@ 7:==65 64@=@8:42= ?:496D E92E  
E6 4@>>F?:E:6D @44FA:65],b`. {2C86 A2CED @7 |25282D42C[ H9:49 2C6 ?@H 56G@:5 @7 7@C6DED 2?  
?:496D D:??46H6E92E :?4=F565 >@C6 E92? a\_ =6>FC DA64:6D 4@G6C:??8 E96 7F== C2?86 @7 =6>FC  
?4C62D65 @FC DE23:==:EJ 2?5 EFC>@:= @? |25282D42C 5FC:??8 E96 >:5\`hf\_D[ 7:6=5 DEF5:6D C@  
:E:6D F?56C@?DF?56CDE2?5:??8 @7 E96D6 AC:>2E6D] #6D62C49 724:==:E:6D ==:<6 E96 sF<6 {6>FC:  
C256DECF4E:@?>@C6 4@?EC@==65 D6EE:??8D] {6>FCD 2C6 :>A@CE2?E 7@C C6D62C49 3642FD6 E96:C  
:6D 2C6 pC492:ED D92C65 H:E9 2?E9C@A@:5 AC:>2E6D 42? J:6=5 :?D:89ED @? AC:>2E6 2?5 9?  
D <?@H? 2D D42C],`e. p== >@56C? DEC6AD:CC9:??6 :?4=F5:??8 =6>FCD 2C6 EC25:E:@?2==J E  
A64:2=:K65 252A:7@C>?8 E96 t@46?6 Wde E@ bc >J2X @C !2=6@46?6 Wee E@ de >J2X  
?6?E56DECF4E2CC2?86>6?E @7 E66E9[ <?@H? 2D 2 E@@E94@>3[ H9:49 ?62C=J 2== =:G:??8 DEC  
D @7 E96 9JA@E96D:D :D E92E =6>FCD 56D46?565 7C@> =@C:D:7@C> W=@C:D\`=:<6X AC:>2E  
54E 2? 366?4.TE@49C@>6 3 86?6 2?5 E96 AC6D6?46 @7 E96 DEC6AD:CC9:??6 E@@E94@>3 :? 3



He%an@!1

This password is very easy to remember!



## Password

The password does not meet the password complexity requirements. Passwords must:

- Have at least 8 characters
- Have at least one capital letter
- Have at least one number
- Have at least one special character
- Have not been used in past year
- Not be the same as your account name



An aerial photograph of turquoise water with a small boat visible in the distance. The water transitions from a lighter teal on the left to a darker teal on the right. A white horizontal band is overlaid across the center of the image.

November 2020!





```
~ > ./bruteforce.sh
```

Terminal window showing a command execution. The window title is "~ (-zsh)". The command `./bruteforce.sh` has been entered. The time `at 16:32:02` is displayed in the top right corner.



```
~ > ./passwordspray.sh
```

~ (-zsh) at 16:35:20



## MAKE LIFE EASY FOR YOUR USERS

### BUSINESS

- Check your password requirements.
- Length is more important than complexity and rotation.

### BYTES

- Get your users a password manager
- Consider passwordless authentication.
- Detect password spray attacks.

### BEHAVIOUR

- Make life easy for your users.
- Educate users on creating secure passwords.





ubridae  
mentovarius  
ula Cañas Gte C.R.  
o Luconi  
F 1968



Familia Colubridae  
Especie Elaphe  
Localidad Valle Central C.R.  
Venosa



Familia Colubridae  
Especie Mastigodryas melanocephala  
Localidad Sarapiquí C.R.  
Colector HEFB # 173 F 1968



Familia Colubridae  
Especie Leptodeira annulata  
Localidad San José Costa Rica  
Colector Jimmy Lott L  
# 187 F 2013



Familia Colubridae  
Especie Imantodes cenchoa  
Localidad Palmichal de Acosta C.R.  
Colector Bartolo Castro # 1990



Familia Colubridae  
Especie Oxybelis aeneus  
Localidad San José C.R.  
F 1968 "Bejuquilla parda"








Familia Colubridae  
Especie Drymobius margaritiferus  
Localidad Hda Sta Paula C.R.  
Colector Lorenzo Luconi  
# 18 F 1968

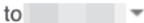


Internship Application - Gmail

mail.google.com/mail/u/0/?ui=2&view=bt&ver=1cid59g061n3t&search=sent&th=%23thread-a%3Ar-5832153877631247883%7Cmsg-a%3Ar-5830501394414563755&c...

Internship Application 

 **Jochem Willemsen** <jba.willemsen@gmail.com> 3:14 PM (9 minutes ago)   

to 

Dear Sir / Madam,

I am currently finalizing the last semester of the HBO study commercial economics and am now looking for a suitable internship. The vacancy for the marketing employee internship fits perfectly with my profile.

Because my application letter and CV were a bit too large to send as an attachment, I put them on Wetransfer as a ZIP file. You should already have received an email about this as well. If you cannot open the files properly, please let me know.

The Wetransfer link:  
<https://we.tl/N8OLzq9QBT>


I hope to hear from you soon!





Kind regards,  
Jochem Willemsen

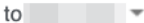


Internship Application - Gmail

mail.google.com/mail/u/0/?ui=2&view=bt&ver=1cid59g061n3t&search=sent&th=%23thread-a%3Ar-5832153877631247883%7Cmsg-a%3Ar-5830501394414563755&c...

Internship Application 

 **Jochem Willemsen** <jba.willemsen@gmail.com> 3:14 PM (9 minutes ago)   

to 

Dear Sir / Madam,

I am currently finalizing the last semester of the HBO study commercial economics and am now looking for a suitable internship. The vacancy for the marketing employee internship fits perfectly with my profile.

Because my application letter and CV were a bit too large to send as an attachment, I put them on Wetransfer as a ZIP file

The Wetransfer link:  
<https://we.tl/N8OLzq9QBT>


I hope to hear from you soon!





Kind regards,  
Jochem Willemsen



Internship Application - Gmail

mail.google.com/mail/u/0/?ui=2&view=bt&ver=1cid59g061n3t&search=sent&th=%23thread-a%3Ar-5832153877631247883%7Cmsg-a%3Ar-5830501394414563755&c...

Internship Application 

 **Jochem Willemsen** <jba.willemsen@gmail.com> 3:14 PM (9 minutes ago)   

to [redacted]

Dear Sir / Madam,

I am currently finalizing the last semester of the HBO study commercial economics and am now looking for a suitable internship. The vacancy for the marketing employee internship fits perfectly with my profile.

Because my application letter and CV were a bit too large to send as an attachment, I put them on Wetransfer as a ZIP file. You should already have received an email about this as well. If you cannot open the files properly, please let me know.

The Wetransfer link:  
<https://we.tl/N8OLzq9QBT>

I hope to hear from you soon!

Kind regards,  
Jochem Willemsen





■■■ %

anti-virus detection



# 91%

anti-virus detection









**NORTHWAVE**  
Intelligent Security Operations



## Bots

Show  entries Search:

Last communication	Host	User	Domain	Logon server
47 seconds ago	WINDOWS-C77810			
48 seconds ago	WINDOWS-RD5428			
1 minute ago	WINDOWS-RD5391			
2 minutes ago	WINDOWS-RD5109			

Showing 1 to 4 of 4 entries Previous **1** Next



■ ■ ■ %

C&C channel detection



# 2%

C&C channel detection









## ASSUME YOUR NETWORK BREACHED

### BUSINESS

- Does your security policy consider that you've been hacked?
- Check your incident response plans.

### BYTES

- Implement a layered defense strategy.
- Detect malicious behavior instead of using signatures.

### BEHAVIOUR

- Is someone actually looking at your log files and AV-alerts?
- Educate end-users on how to recognize malicious files.





# Ask me anything

Share experience. Build resilience.



# SECCON-NL 2022

Share experience. Build resilience

Time

09:00 – 10:00

Opening Keynote Sadie Creese (Professor Cybersecurity @ Oxford University)

Main stage (Zilversmederij 300 seats)

Breakout room 1 (Penningzaal 80 seats)

Breakout room 2 (Depot 80 seats)

Breakout room 3 (Stempelkamer 60 seats)

Breakout room 4 (Schatkamer 30 seats)

10:00 – 10:15

Break - switch to main stream

Threat Intel

Threat Intel

Post Quantum Security

Threat Intel

AI

10:15 – 10:45

Threat Intel update from Talos - Martin Lee (Talos Threat intelligence organization)

No More Leaks Project - Felix Nijpels (Dutch Police)

The Impact of Quantum on security - a general outlook - Sam Samuel (Cisco)

Threat management at the Dutch Railway - Dimitri van Zantvliet Rozemeijer (Chief Cyber Dutch Railway)

Get ready for the AI attack bot - Richard de Vries (Tata Steel)

10:45 – 11:00

Break - switch to main stream

Detection and Response

SOAR

Post Quantum Security

Detection and Response

Detection and Response / AI

11:00 – 11:30

Day in life at the Dutch Tax Office SOC - Karl Lovink (Belastingdienst)

Stay Ahead of the Game: Automate your Threat Hunting Workflows - Christopher van der Made (Cisco)

Quantum hurdles: an optimistic view of post-quantum security - Sander Dorigo (Fox Crypto)

What Cyber can learn from Biology? - Koen Hokke (KPN)

Unsupervised Anomaly-Based Network Intrusion Detection Using Auto Encoders for Practical Use - Julik Keijer (Northwave)

11:30 – 11:45

Break - switch to main stream

Detection and Response

Detection and Response

DevSecOps/ Detection and Response

DevSecOps

11:45 – 12:15

Compliancy vs security. Pentesting is dead - Edwin van Anel (ZeroCopter)

Incident Response without compromise. How to prepare for the worst day of your career with dice! - Wouter Hindriks (Avit)

Threat Modelling: it's not just for developers - Timothy Wadhwa-Brown (Cisco)

Changed responsibilities in modern software development environments - Martin Knobloch (Microfocus)

How to break a data center? Fred Streefland (Secior)

12:15 – 13:00

LUNCH

13:00 – 13:45

Panel Discussion with Liesbeth Holterman (host CVNL) Koen Sandbrink (NCSC), Jochem Smit (Northwave), Oscar Koeroo (Min Ezk), Jan Heijdra (Cisco)

13:45 – 14:00

Break - switch to main stream

Threat intel / Detection and Response

Threat Intel

Detection and Response

DevSecOps

14:00 – 14:30

CERT in Ukraine experience sharing by Andrii Bezverkhyi (SOCPrime)

This is why you will fail: Most successful attack scenarios and their defenses - Tijme Gommers (Northwave)

Risk-based Auth & ZTA - Frank Michaud (Cisco)

Creating clarity and unity in security standards and guidelines - OpenCRE.org - Rob van der Veer (Software Improvement Group)

(Placeholder) WICCA Breakout (with Wendy joining)

14:30 – 14:45

Break - switch to main stream

Detection and Response

Detection and Response

Detection and Response

Threat Intel

Detection and Response / AI

14:45 – 15:15

Advanced Attacker Automation: Botnet capabilities and techniques used to evade your defences - David Warburton (F5)

Security Maturity: from XDR to SIEM - Gilles van Heijst (Orange Cyber Defense)

Improving Business Security by implementing Security.txt - Julius Offers (Digital Trust Center)

Tackling the challenge of translating threat intelligence into actual action - Raymond Bierens (Connect2Trust)

Fostering emerging technologies in cybersecurity, to reinforce our strategic autonomy. - Christian van der Woude (Dcypher)

15:15 – 16:00

Closing Keynote - Wendy Nather