Cyber Security in de industrie: 'Vriend' of 'Vijand'?

Fred Streefland
Chief Security Officer (CSO) NEUR & EEUR
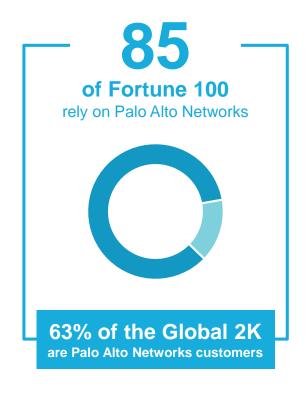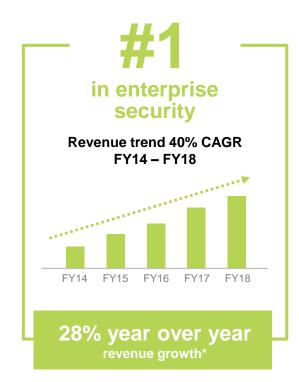
INTRODUCTIE
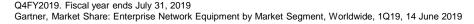
INTRODUCTIE (SPREKER)

Introductie (Palo Alto Networks)

85
of Fortune 100
rely on Palo Alto Networks

63% of the Global 2K
are Palo Alto Networks customers

#1
in enterprise security

Revenue trend 40% CAGR FY14 – FY18

FY14 FY15 FY16 FY17 FY18

28% year over year
revenue growth*

65,000+
customers
in 150+ countries

J.D. POWER
2018
CERTIFIED ASSISTED
TECHNICAL SUPPORT

tsia
RATED OUTSTANDING
2018
ASSISTED SUPPORT
GLOBAL | PALO ALTO NETWORKS

9.1/10
average CSAT score

Q4FY2019. Fiscal year ends July 31, 2019
Gartner, Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 1Q19, 14 June 2019

paloalto
NETWORKS

INFORMATION TECHNOLOGY (IT)

"*We screwed it up !*"

(The Cyber Security industry didn't do a good job…)

Nir Zuk, Founder & CTO Palo Alto Networks

Cybercrime will generate at least $1.5 trillion this year—and that's conservative

Cybercrime Annual Revenues

Crime	Annual Revenues
Illegal online markets	$860 Billion
Trade secret, IP theft	$500 Billion
Data Trading	$160 Billion
Crime-ware/CaaS	$1.6 Billion
Ransomware	$1 Billion
Total Cybercrime Revenues	$1.5 Trillion
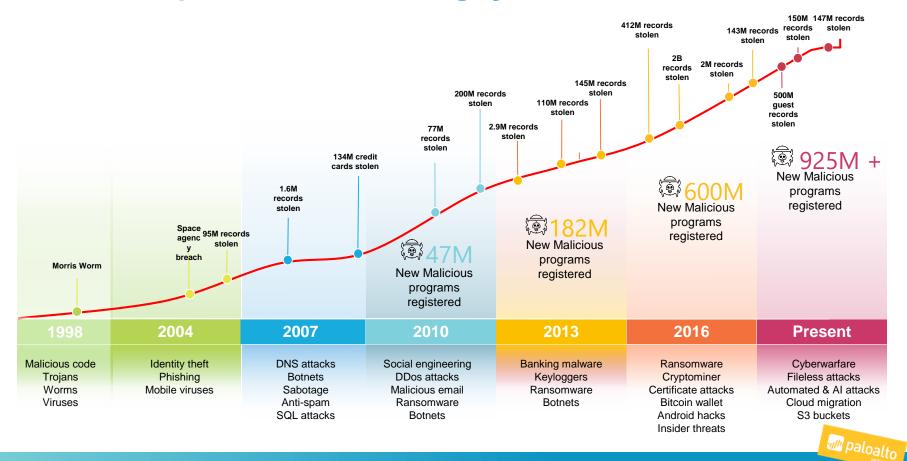
Source: Imperva Cyber Threat report 2019

The development of the 'bad guys'

1998	2004	2007	2010	2013	2016	Present
Malicious code Trojans Worms Viruses	Identity theft Phishing Mobile viruses	DNS attacks Botnets Sabotage Anti-spam SQL attacks	Social engineering DDos attacks Malicious email Ransomware Botnets	Banking malware Keyloggers Ransomware Botnets	Ransomware Cryptominer Certificate attacks Bitcoin wallet Android hacks Insider threats	Cyberwarfare Fileless attacks Automated & AI attacks Cloud migration S3 buckets

Network Security

Network Firewall

Network Monitoring/Forensics

Intrusion Prevention Systems

Unified Threat Management

Endpoint Security

Endpoint Prevention

Endpoint Detection & Response

Application Security

WAF & Application Security

Vulnerability Assessment

Managed Security Service Provider

Messaging Security

Risk & Compliance

Security Operations & Incident

Mobile Security

Industrial / IoT Security

Security Incident Response

Specialized Threat Analysis & Protection

Identity & Access Management

Cloud Security

Fraud Prevention / Transaction Security

SOCs are overloaded with alerts and not effective (anymore)!

174k
alerts per week

30 +
Point products

4+ Days
To complete an investigation

A NEW APPROACH IS NEEDED

"
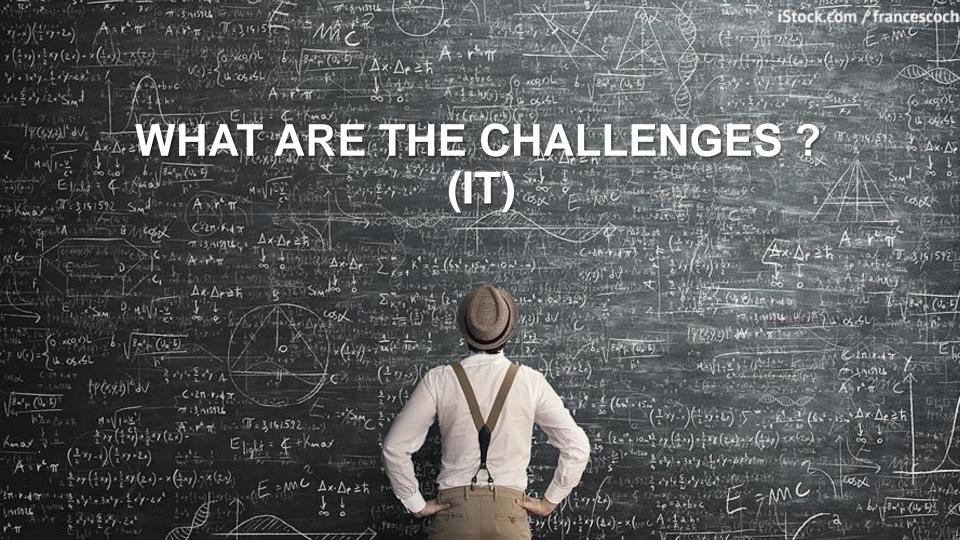
What I need is
more visibility and less complexity !

CISO of Swedish company

"

WHAT ARE THE CHALLENGES ?
(IT)

INSTRUMENTED & INTERCONNECTED WORLD

DEMANDING PEOPLE

COMPLEX ORGANIZATIONS
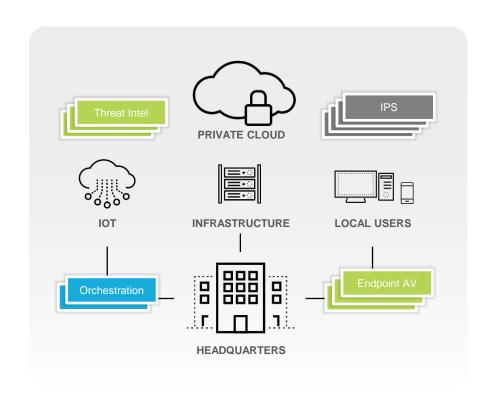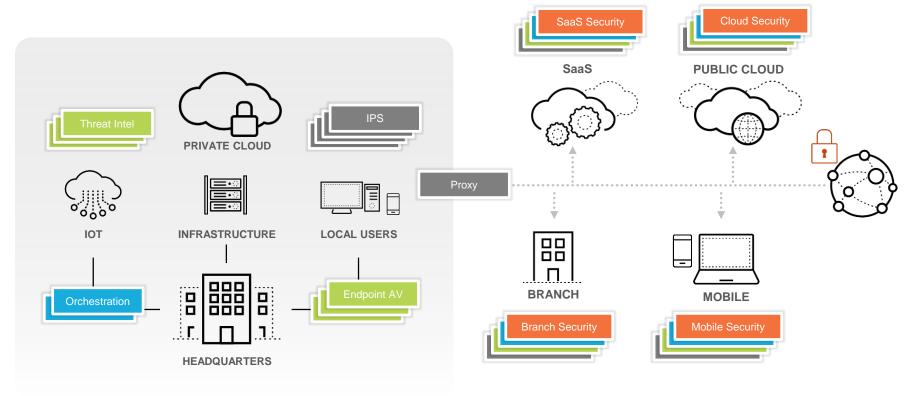
In the old days, cyber security was 'relatively' easy…

..but today's world makes security challenging!

INTERNET OF THINGS

'MOVE TO THE CLOUD'

COMPLIANCE & REGULATIONS

HIGHLY AUTOMATED ADVERSARIES

THE NEW 'ATTACKERS'

BUSINESS GROWTH

SO, WHAT'S THE ISSUE ?

INSTRUMENTED & INTERCONNECTED WORLD

DEMANDING PEOPLE

INTERNET OF THINGS

5G

COMPLEX ORGANIZATIONS

'MOVE TO THE CLOUD'

COMPLIANCE & REGULATIONS

HIGHLY AUTOMATED ADVERSARIES

BUSINESS GROWTH

Today's CISO….

NO visibility and NOT in control !

OPERATIONAL TECHNOLOGY (OT)

WHAT ARE THE CHALLENGES ?
(OT)

INSTRUMENTED & INTERCONNECTED WORLD

DEMANDING PEOPLE

INTERNET OF THINGS

5G

COMPLEX ORGANIZATIONS

'MOVE TO THE CLOUD'

COMPLIANCE & REGULATIONS

HIGHLY AUTOMATED ADVERSARIES

BUSINESS GROWTH

+ additional OT challenges

Unpatchable Legacy systems

Roles & responsibilities
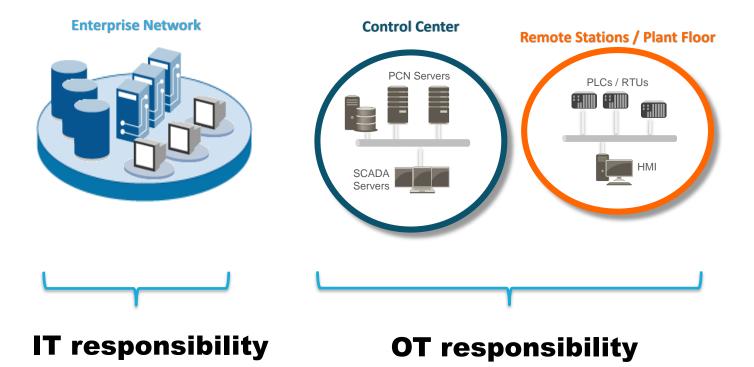
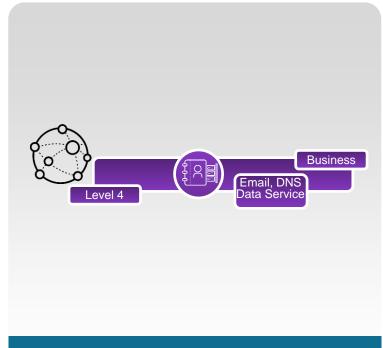Increasingly targeted

'always on' requirement

Board level awareness

…and the 'move' of IT into the OT domain!

Enterprise Network

Control Center
- PCN Servers
- SCADA Servers

Remote Stations / Plant Floor
- PLCs / RTUs
- HMI

IT responsibility   **OT responsibility**

IT Security

OT Security

Traditional approach: Air Gap

INFORMATION TECHNOLOGY

Level 4
Business
Email, DNS
Data Service

OPERATIONAL TECHNOLOGY

Level 3.5
DMZ
Patch Srv
Jmp Srv

Level 3
Manufacturing Operations
Historian
Process sys

Level 2
Controls Systems
HMI
Eng. Sta

Level 1
Intelligent Device
PLC, RTU, IED

Level 0
Process
Actuator

paloalto
NETWORKS
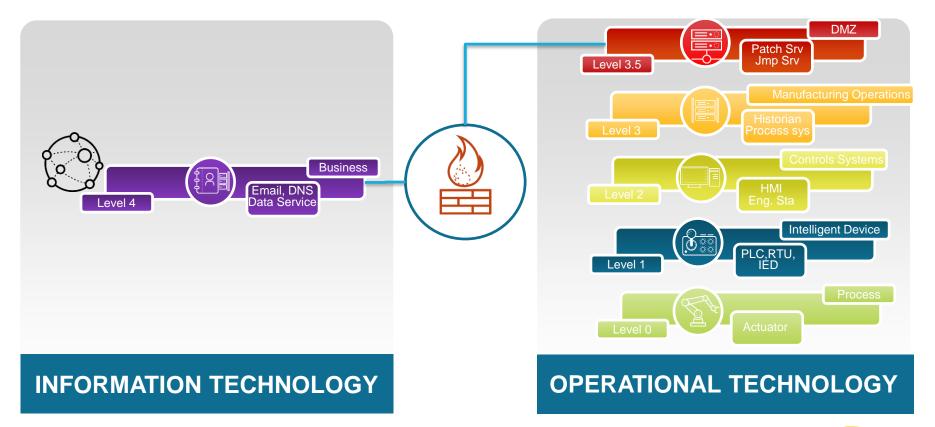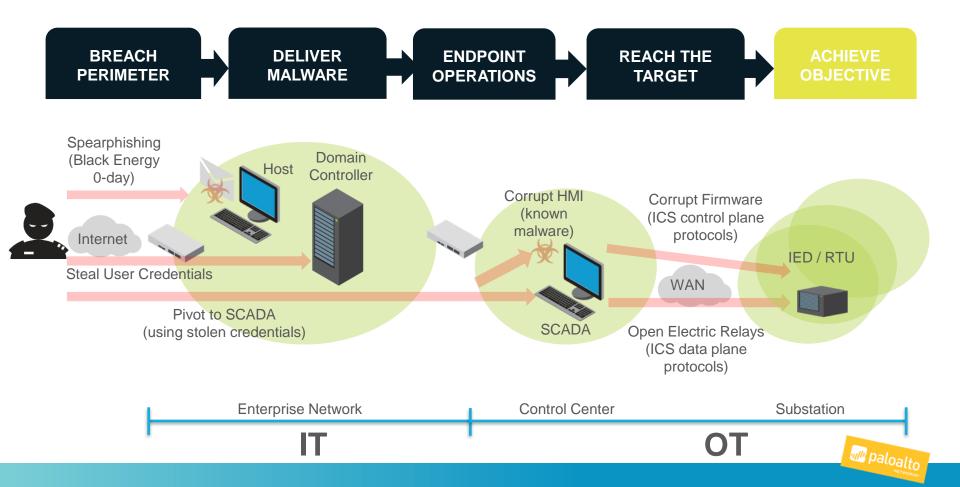
Traditional approach: Firewall

INFORMATION TECHNOLOGY

- Level 4
- Business
- Email, DNS Data Service

OPERATIONAL TECHNOLOGY

- Level 3.5 — DMZ, Patch Srv Jmp Srv
- Level 3 — Manufacturing Operations, Historian Process sys
- Level 2 — Controls Systems, HMI Eng. Sta
- Level 1 — Intelligent Device, PLC,RTU, IED
- Level 0 — Process, Actuator

paloalto
NETWORKS

Ukraine Power Grid attack

| BREACH PERIMETER | DELIVER MALWARE | ENDPOINT OPERATIONS | REACH THE TARGET | ACHIEVE OBJECTIVE |

Spearphishing (Black Energy 0-day)

Host

Domain Controller

Internet

Steal User Credentials

Pivot to SCADA (using stolen credentials)

Corrupt HMI (known malware)

Corrupt Firmware (ICS control plane protocols)

IED / RTU

WAN

SCADA

Open Electric Relays (ICS data plane protocols)

Enterprise Network | Control Center | Substation

IT | OT

paloalto NETWORKS

CHANGE CYBER SECURITY

Where to start?

Start with the business and the risks!

Cyber Security = <u>reducing risks</u> for the business, so that the business can do 'its business'*

(Within OT domain this means Availability ('Always on') !

* Fred Streefland, former CISO

'Think' ZERO TRUST

Ask yourself the following:
-   Which assets need the highest protection on availability, integrity and confidentiality?
    (What are my 'crown jewels'?)
-   What happens if these assets will be 'breached' (changed, stolen, leaked, deleted, etc.)? Can I still run my business or is my credibility/trust gone?
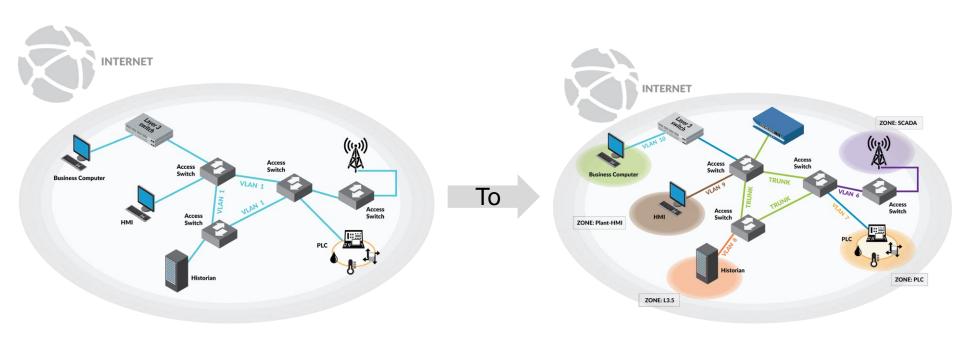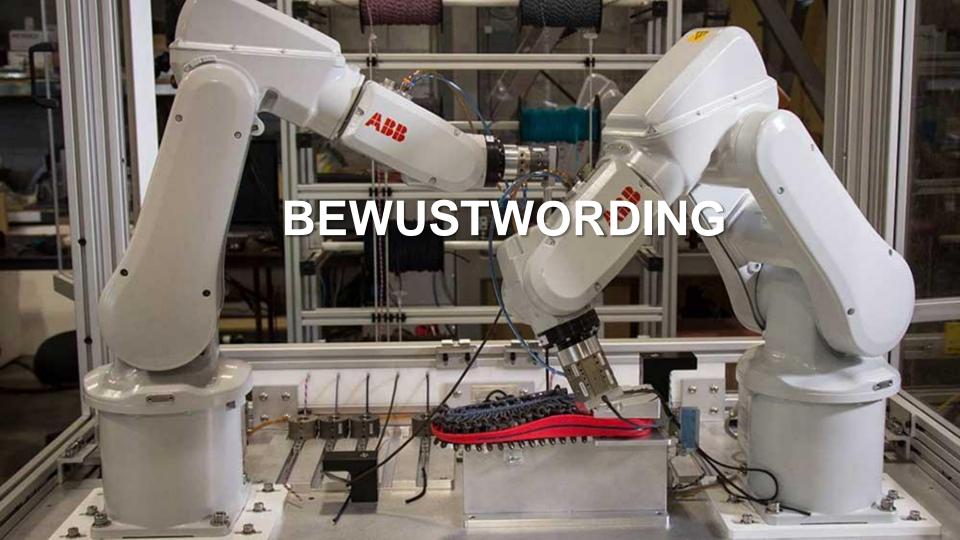-   Who has access to these assets and who is not allowed?

paloalto
NETWORKS®

ZERO TRUST

What are the Crown jewels?

Where are the Crown jewels?

Who has access to the Crown jewels?

ZERO TRUST principles:

1) Design Security Inside-Out

2) Nothing is 'trusted'

3) Inspect & log _all_ traffic

VISIBILITY! VISIBILITY! VISIBILITY!

From zero segmentation

To

Zero Trust Segmentation

BEWUSTWORDING

VERANTWOORDELIJKHEID

ERVARING
&
'LEREND VERMOGEN'
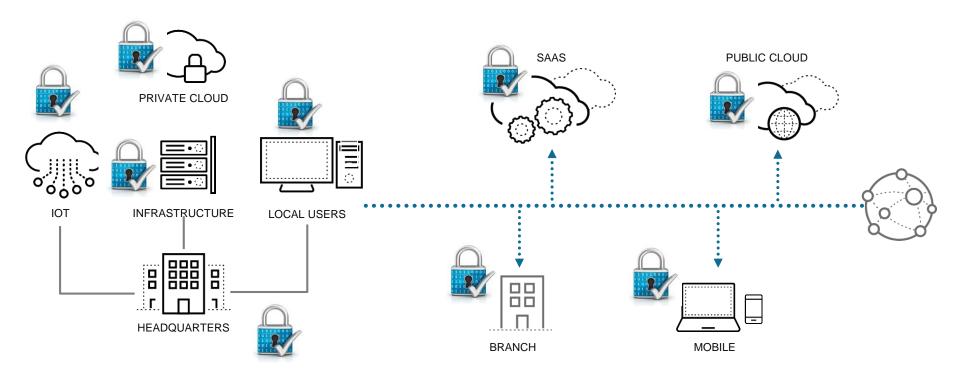
CONCLUSIE
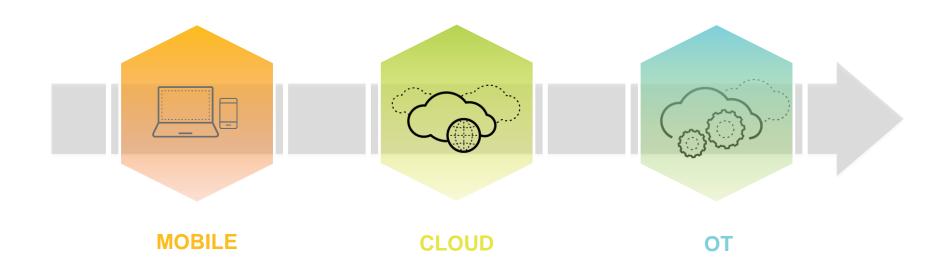
In today's world, where data is everywhere....

PRIVATE CLOUD

SAAS

PUBLIC CLOUD

IOT

INFRASTRUCTURE

LOCAL USERS

HEADQUARTERS

BRANCH

MOBILE

...visibility should be everywhere. Consistent !

So, your (new) security approach needs to be broad…

MOBILE   **CLOUD**   **OT**

..and security teams need to adapt !

ENFORCE

Consistent protection across
ALL architectures
(including OT)

SIMPLIFY

Improve operational efficiency
with **AUTOMATION**

EXTEND

Add new security capabilities
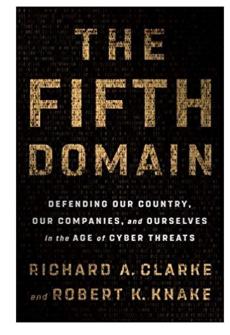that **WORK TOGETHER** fast

paloalto
NETWORKS®

Some 'Take Aways'

- **The world is moving fast and cyber security isn't easy - Be Aware;**

- **Start with the business & risks - Zero Trust is THE foundation;**

- **Embrace new technology as an <u>opportunity</u> - 'Do it good'– from the beginning!**

- **Don't invent the wheel yourself - Learn from your 'peers', the IT organization and the OT security people**

- **IT & OT must become 'partners' - Work together !**

A final 'Take Away'……

"We have the strategy, we have the resources, we have the tools, but what's needed is a <u>change in mindset</u> and JUST EXECUTE IT!"*

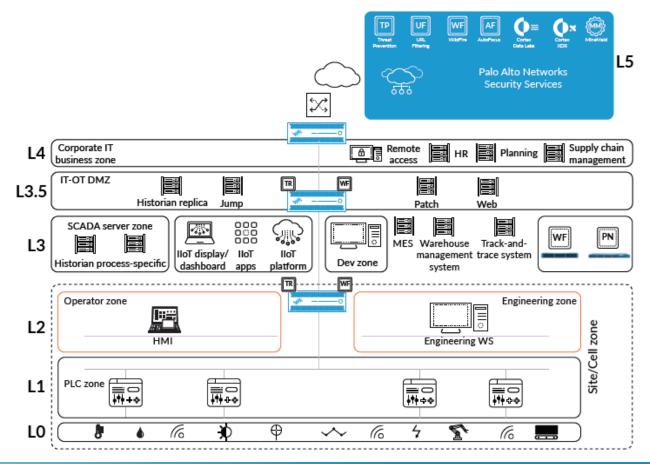*Source: Richard Clarke & Robert Knake

Bedankt voor uw aandacht!

✉ fstreefland@paloaltonetworks.com

paloalto
NETWORKS®

BACK-UP SLIDES

High level architecture for OT

How does this all come together?