

How to migrate a massive environment to **Check Point** and automate your activities to succeed

Federico Meiners, CCSM, CRISC, PMP



About me



Cybersecurity architect & Level 3 support

> Certifications: CCSM, PMP, CRISC, ITIL, GRCP

First Check Point version -> R77.30

> More than 50 Check Point deployments (Banks, Oil & Gas, ISPs, Healthcare, among others)

SOC Deployments, advisory, F5, Arbor, RSA

> CheckMates (Contribution is key)

The customer

- > Big ISP & Datacenter company
- > Government
- > MSSP
- > Key player: Cybersecurity

The project

- # x2 23500 appliances
- # 60 VS (ASA to CHKP)
- # 6 months
- # Next stage: Maestro

Automation

It doesn't have to be complex

Don't automate the whole thing

Less errors, less time, more **predictability**

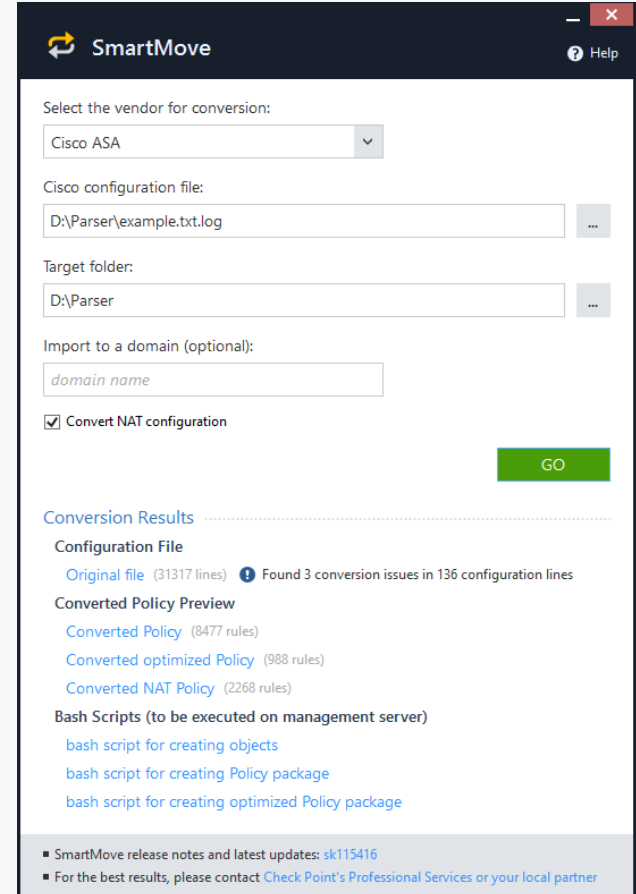
Automate whenever possible – SmartMove (sk115416)

From 59778 rules to 6027 (90%)

> Beware: Tool limitations

Optimized policy vs Normal policy

> Play safe!



The screenshot shows the SmartMove web interface. At the top, there's a header with the SmartMove logo and a help icon. Below that, a form for conversion settings is displayed. The 'Select the vendor for conversion:' dropdown is set to 'Cisco ASA'. The 'Cisco configuration file:' field contains 'D:\Parser\example.txt.log'. The 'Target folder:' field contains 'D:\Parser'. There is an optional field for 'Import to a domain (optional):' with the placeholder 'domain name'. A checkbox for 'Convert NAT configuration' is checked. A green 'GO' button is located at the bottom right of the form. Below the form, the 'Conversion Results' section is visible, showing a 'Configuration File' section with a link to the 'Original file' (31317 lines) and a note that 3 conversion issues were found in 136 configuration lines. The 'Converted Policy Preview' section lists three items: 'Converted Policy' (8477 rules), 'Converted optimized Policy' (988 rules), and 'Converted NAT Policy' (2268 rules). Underneath, there are three links for 'Bash Scripts (to be executed on management server)'. At the bottom, there are two footer items: 'SmartMove release notes and latest updates: sk115416' and 'For the best results, please contact Check Point's Professional Services or your local partner'.

Smart Move – Considerations for large MSSP deployments

> Avoid repeated names - Don't worry for repeated IP

Host_ / Network_ / Interface_Outside

> Make them unique – Avoid chain reactions

> Check the error logs

> If possible, script

```
sed -i 's/network_/network_FILENAME_/gI' FILENAME_objects.sh  
sed -i 's/network_/network_FILENAME_/gI' FILENAME_policy_opt.sh
```

Manual: **2 minutes**

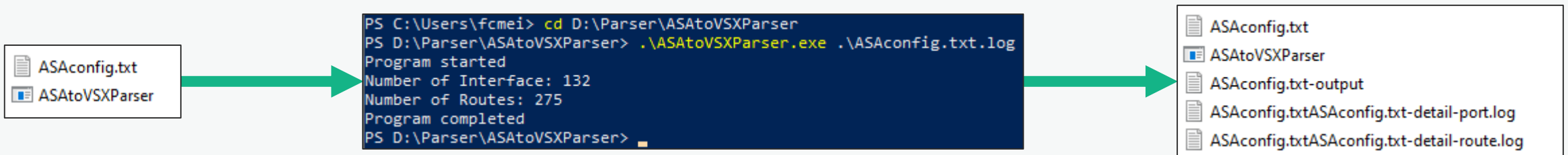
Automated: **1 second**

99% optimization

Rules are ok. Now what? - **ASAtoVSX** parser

> Created by Molten Minds (Daniel Azar)

Developed in Golang - Open source



CheckMates

ASAtoVSX - Translate your running config to vsx_util and more! [CheckMates post](#)

Outputs- ASAtoVSX parser

vsx_util output

```
1 transaction begin
2 add interface name bond1 ip 172.16.1.1 netmask 255.255.255.0
3 add interface name bond1 ip 10.10.10.1 netmask 255.255.255.0
4 add interface name bond1 ip 10.10.10.2 netmask 255.255.255.0
406 add route destination 192.168.1.0 netmask 255.255.255.255 next_hop 10.10.10.1
407 add route destination 192.168.1.0 netmask 255.255.255.0 next_hop 10.10.10.1
408 add route destination 192.168.1.0 netmask 255.255.254.0 next_hop 10.10.10.1
409 transaction end
```

Interfaces JSON

```
{
  "ID": "1",
  "Name": "IN",
  "Description": "",
  "Shutdown": false,
  "SecurityLevel": 30,
  "IPAdress": "172.16.1.1",
  "Netmask": "255.255.128.0"
},
```

Routes JSON

```
{
  "Name": "IN",
  "NextHop": "10.10.10.1",
  "IPAdress": "192.168.1.0",
  "Netmask": "255.255.224.0"
},
```


Key lessons from this project

Technical

Pre/Post checks

IPS Tuning

Max interfaces vs Max VS (sk99121)

#R. ASA	Interfaces
158	3
8477	132
184	10

Project management

Setbacks

Team mindset

Lack of knowledge

Technical decisions

Customer understanding

Predictable & Repeatable

Numbers

4 min

VS deployment

5-15 min

Objects and rules

10-30 min

Rulebase tuning

1:30 min

push policy duration

Automation 33 mins

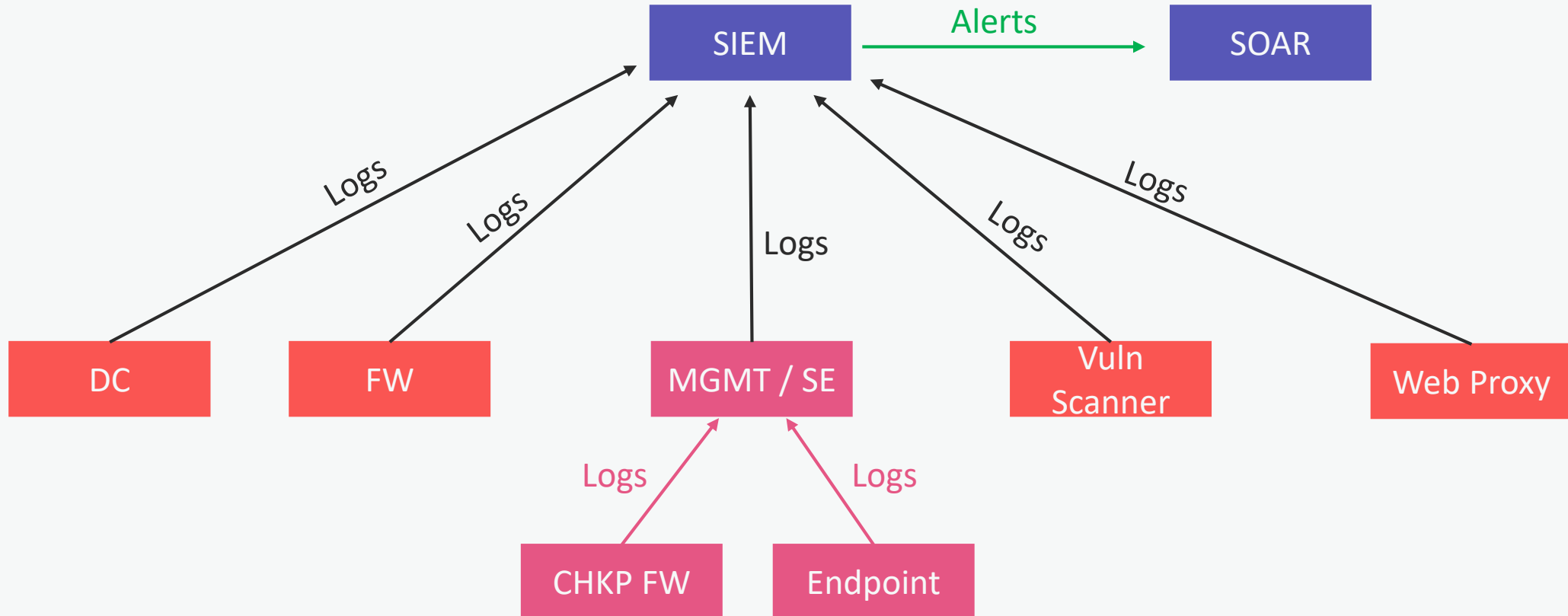
Manual 27 hours

98% less time

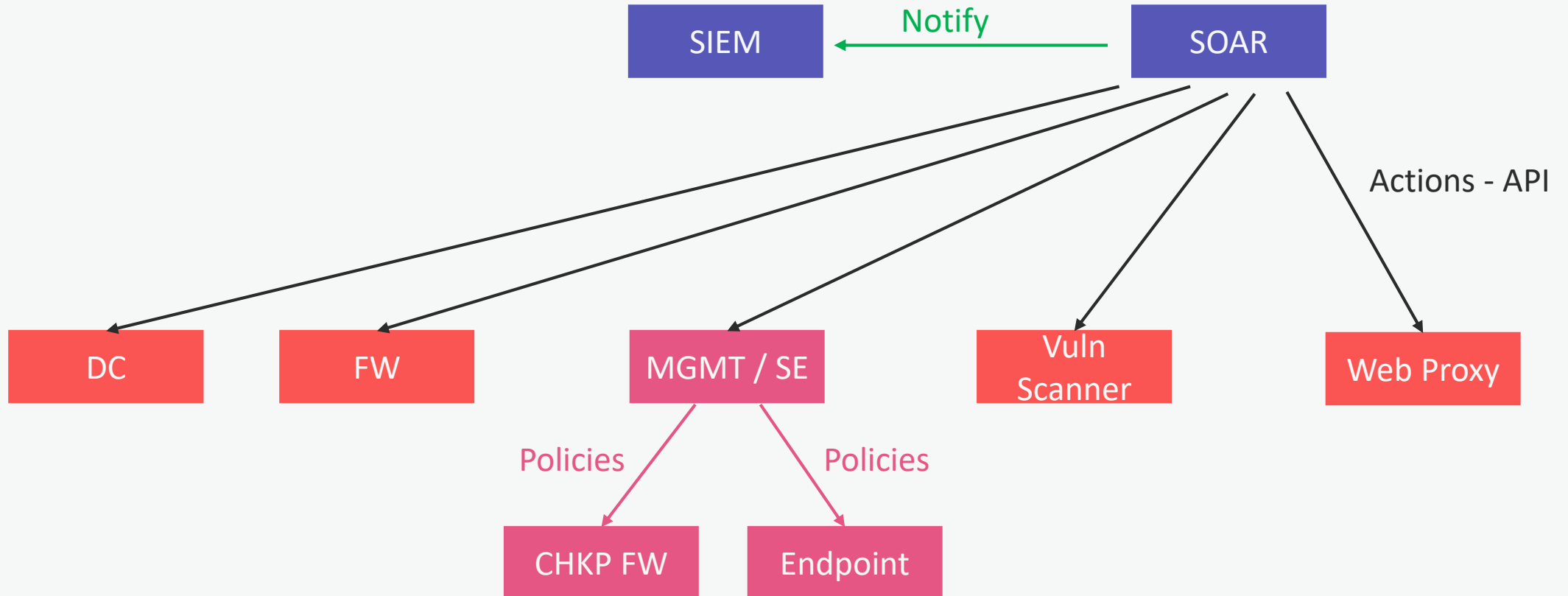
What about now?

SOAR

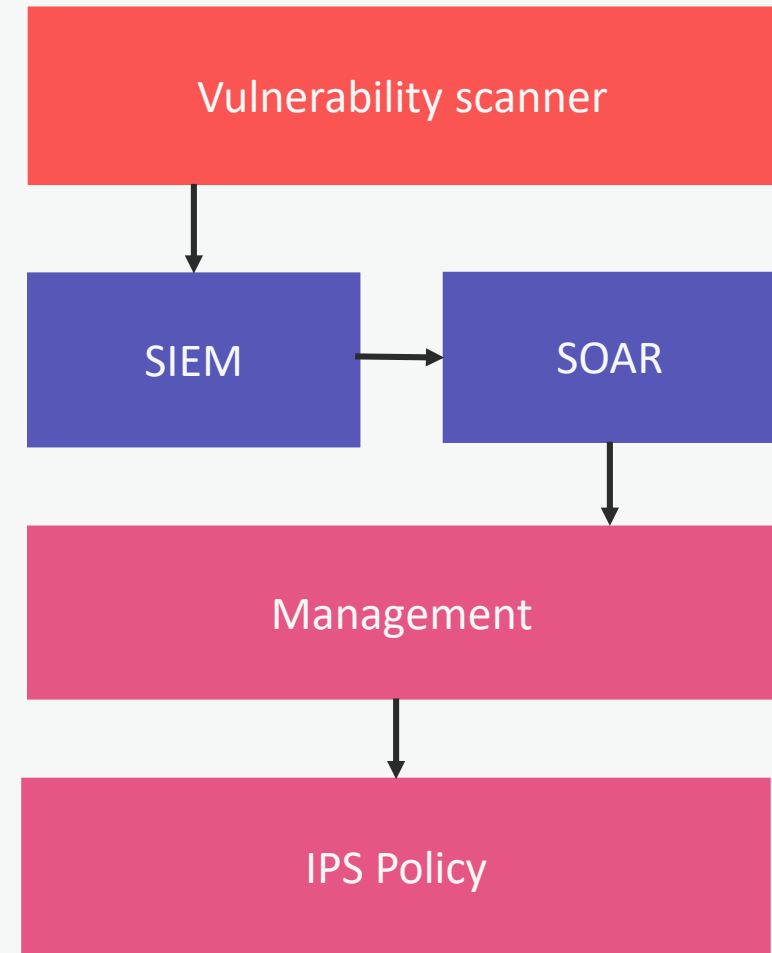
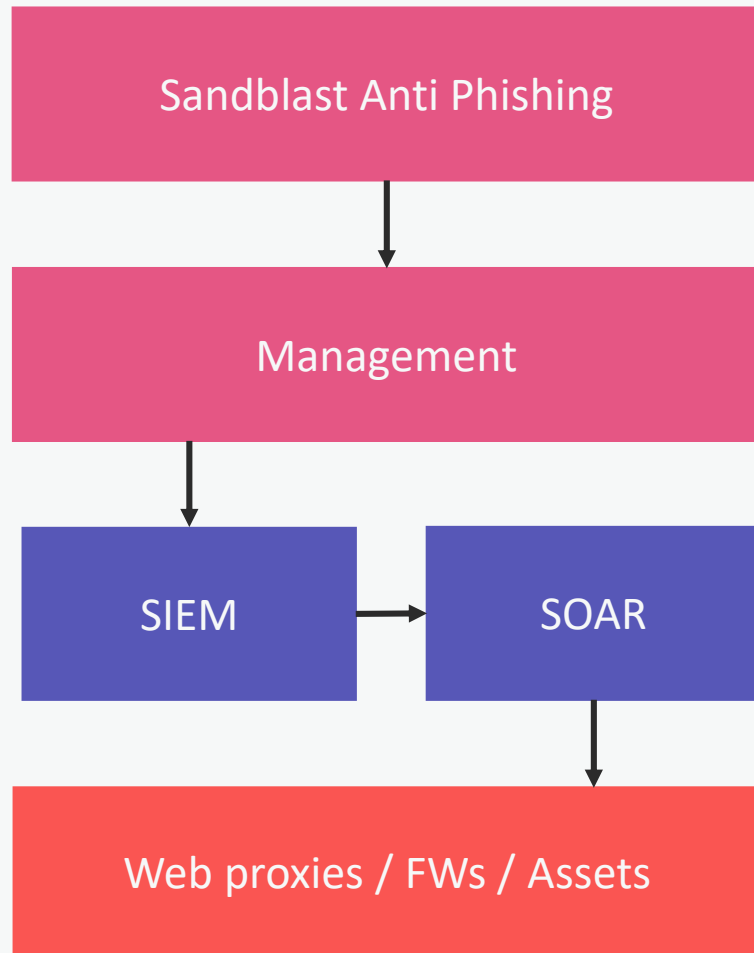
SOAR – How does it work? Part 1



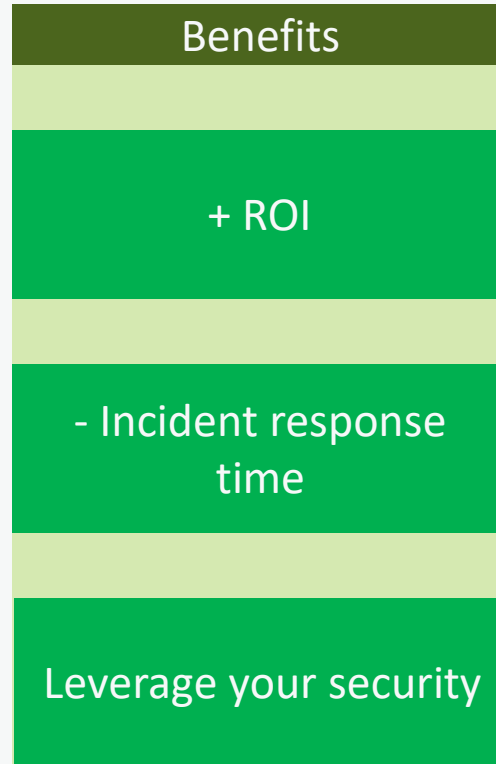
SOAR – How does it work? Part 2



SOAR – Check Point use cases



SOAR – Summary



The end – Special thanks

Check Point SE's

Lucas Garcia & Alejandro Botter

Check Mates

Tim Hall - Kaspars Zibarts - Michael Endrizzi

Customer and CPX Staff

For the given opportunity

#cpstop

(the end)

Mail fcmeiners@gmail.com

LinkedIn <https://www.linkedin.com/in/federicomeiners/>

CheckMates FedericoMeiners