Most **common ways** to hack companies under **4h**

→ default killchain for many companies

Florian Hansemann

Over **10 years** of experience in security analyses of all industries and company sizes (from small tax firms, medium-sized companies with 200 employees to banks, aerospace, **military** and nuclear power plants)

Several 0-Days disclosures (e.g. **Sophos**, Datev, **Intel**, Microsoft, **Fujitsu**)

Nationally and internationally known and awarded several times

Permanent consulting mandates as **trusted advisor** for international companies based in Germany

Comprehensive network of experts from all disciplines in the field of cybersecurity

Known from

Selection of titles

Top 21 Security Twitter Accounts Worldwide
(https://www.sentinelone.com/blog/21-cyber-security-twitter-accounts-you-should-be-following-in-2021/)

Keynote Speaker „Best of the World in Security"
(https://hansesecure.de/2021/05/best-of-the-world-in-security-keynote-speaker/)

Top 100 most influential cybersecurity brands worldwide
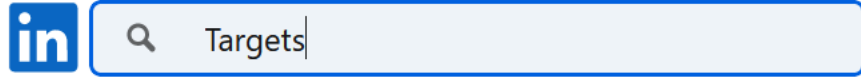(https://onalytica.com/blog/posts/whos-who-in-cybersecurity-2/)

Top 21 Sources for Security Teams Worldwide
(https://techbeacon.com/security/modern-red-teaming-21-resources-your-security-team)

- ✅ 00:00 – 00:30 OSINT
- ✅ 00:30 – 01:30 DROPPER
- ✅ 01:30 – 02:00 PHISH
- ✅ 02:00 – 02:30 PRIVESC
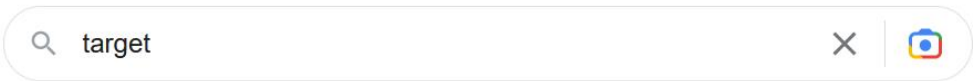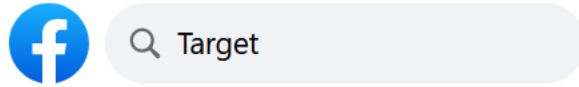- ✅ 02:30 – 03:30 RECON
- ✅ 03:30 – 04:00 SPRAY

agenda

OSINT
00:00 – 00:30

HanseSecure
CHOOSE THE INTRUDER!

cobaltstrike
by HelpSystems

Mythic

00:30 – 01:30 DROPPER
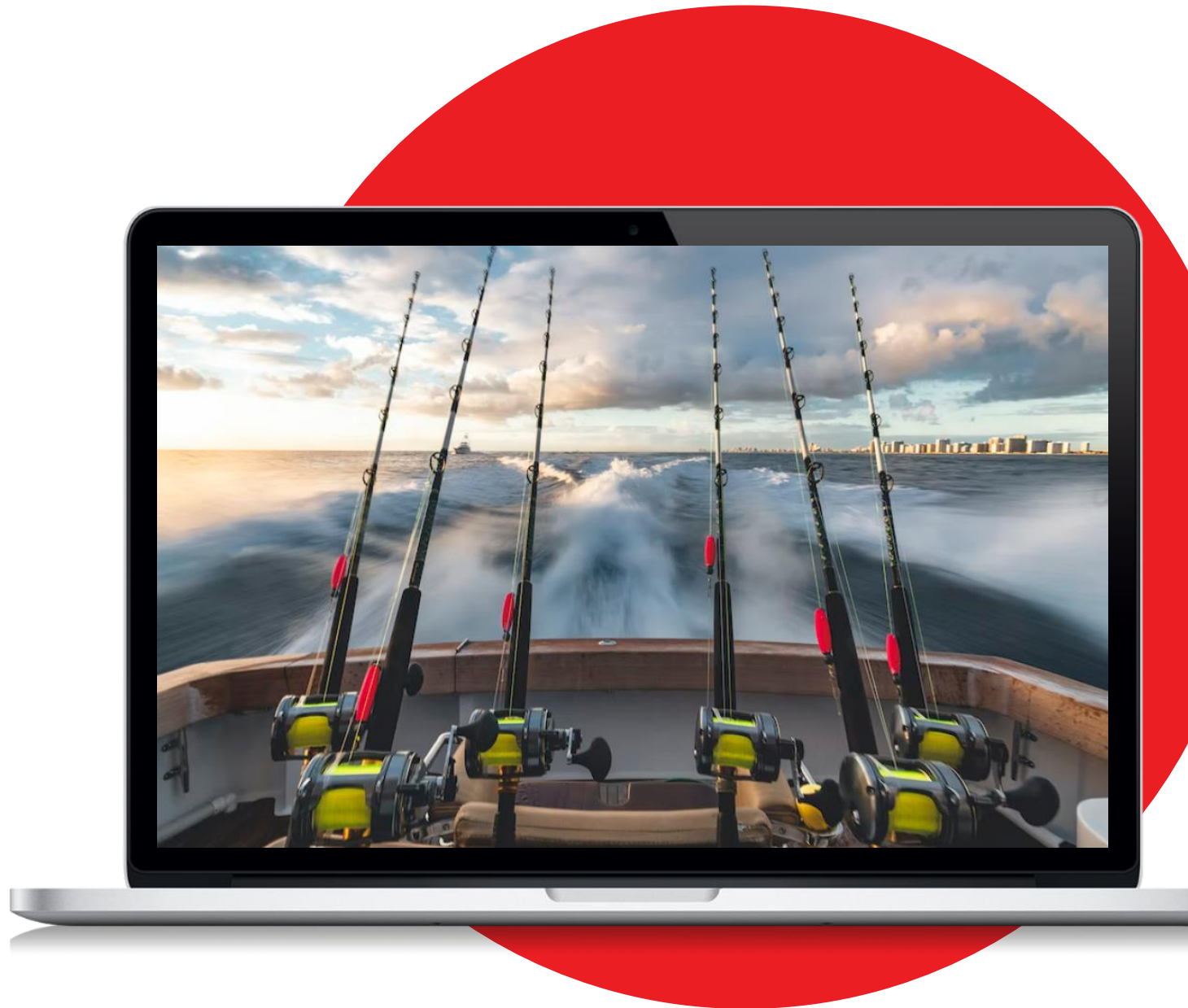
NIMPACKT

Shellter
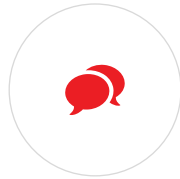AV Evasion Artware

babelfor.NET

01:30 – 02:00 PHISH

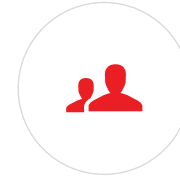itm4n / **PrivescCheck** Public

PowerShellMafia / **PowerSploit** Public archive

02:00 – 02:30
PRIVESC
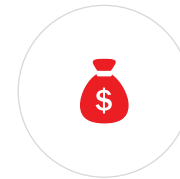
rasta-mouse / **Watson** Public archive

Service Permissions

Old Software

Environment Path

Privileged File Access

02:30 – 03:30 RECON

Privileged SPNs, aka Kerberoasting

Unconstrained Delegation

ACLs/DACLs

BLOODHOUND

PowerShellMafia / PowerSploit (Public archive)
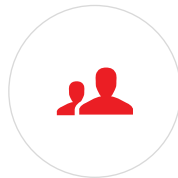
03:30 – 04:00 SPRAY

Username = Password

There are many variations of passages of Lorem Ipsum available.

Weak Password

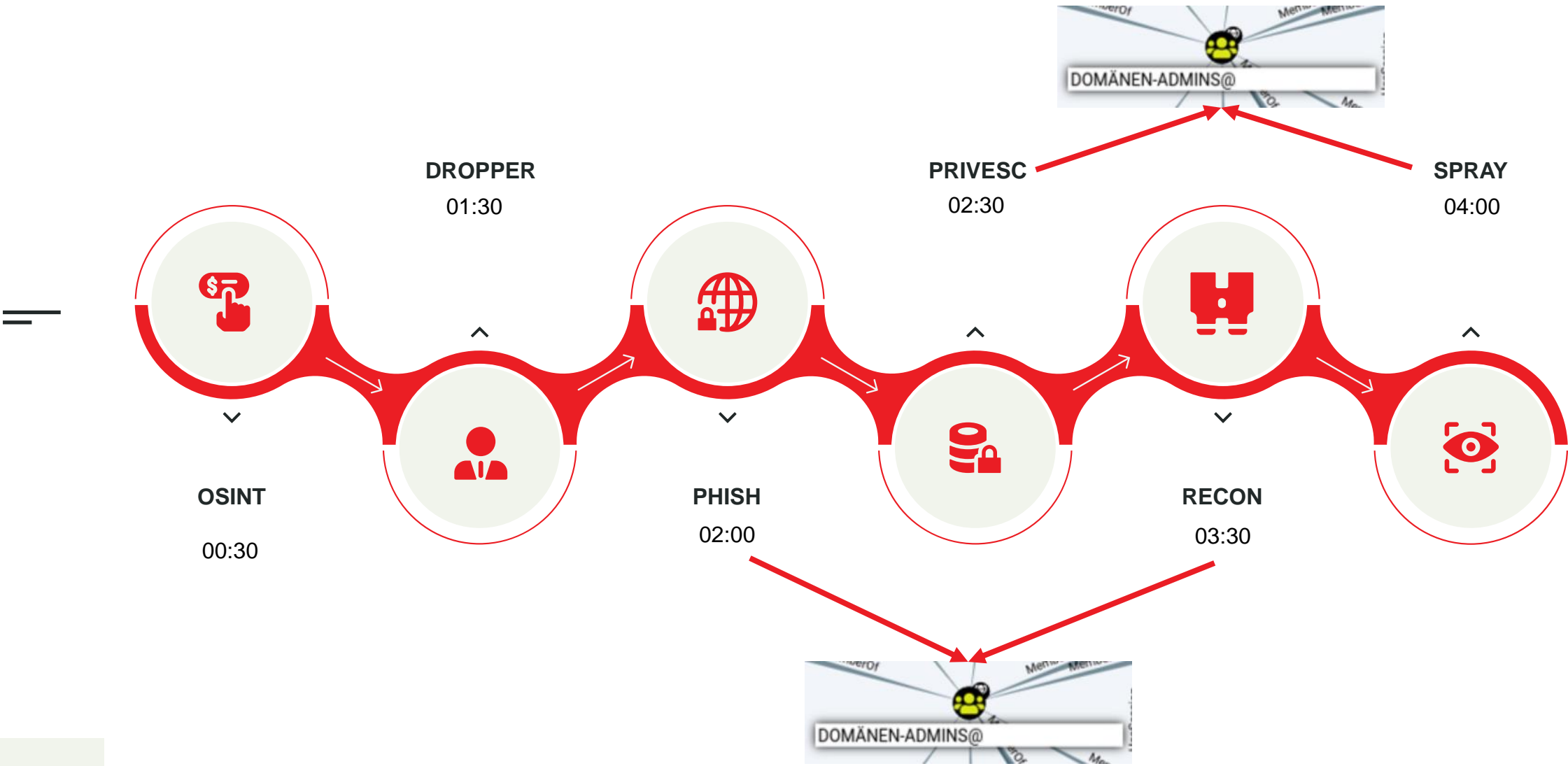There are many variations of passages of Lorem Ipsum available.
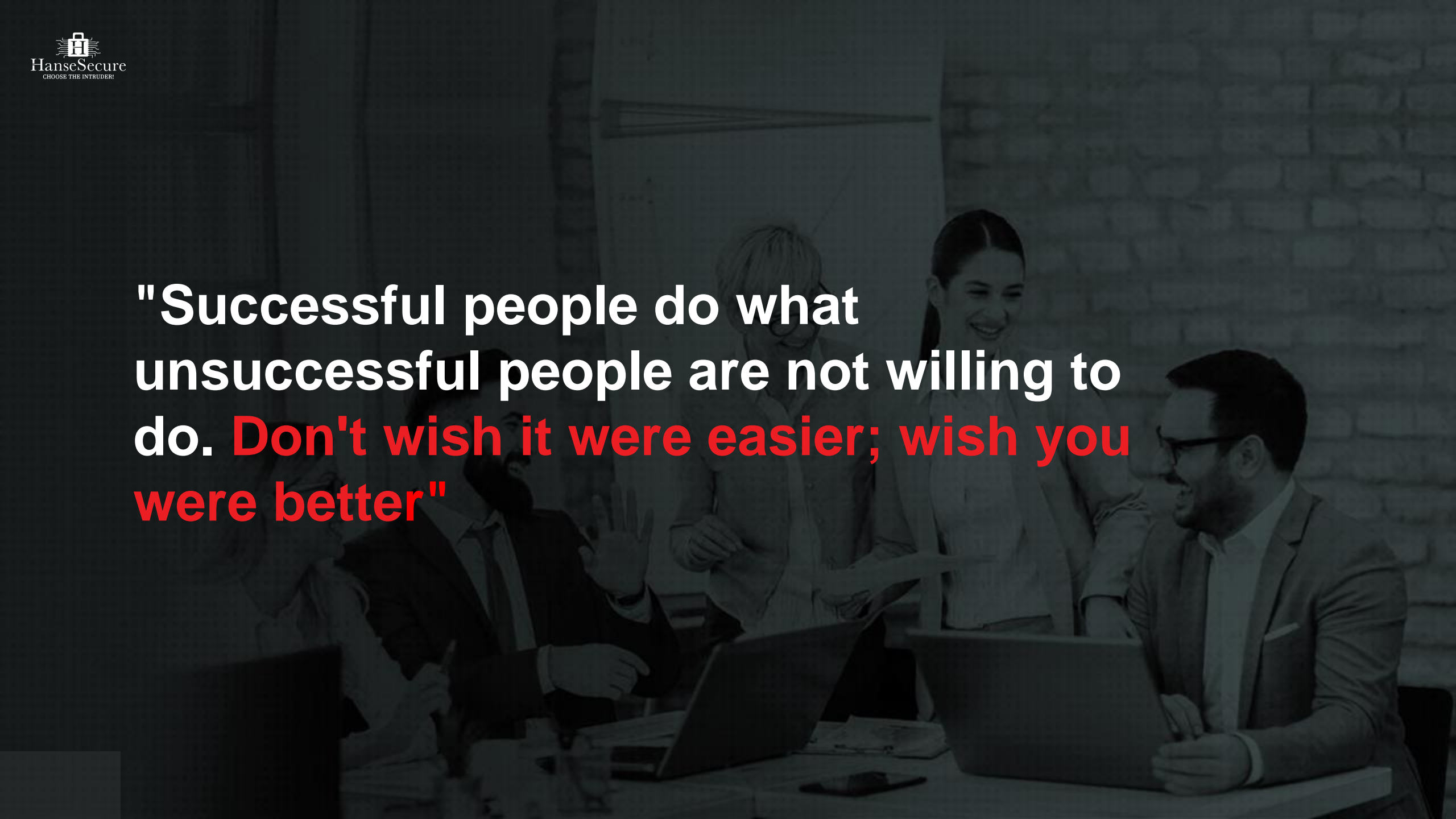
Default Password

There are many variations of passages of Lorem Ipsum available.

dafthack / DomainPasswordSpray Public

SUMMARY

DROPPER
01:30

PRIVESC
02:30

SPRAY
04:00

OSINT
00:30

PHISH
02:00

RECON
03:30

DOMÄNEN-ADMINS@

DOMÄNEN-ADMINS@

"Successful people do what unsuccessful people are not willing to do. Don't wish it were easier; wish you were better"

HanseSecure
CHOOSE THE INTRUDER!

GET IN TOUCH

📍 **Neuhauser Str. 15, 80331 München**

📞 **https://hansesecure.de/kalender/**

✉️ **info@hansesecure.de**

🌐 **https://hansesecure.de/**