One does not simply rely solely on a managed SOC!

IT-SecX 2022: Daniel Kroiß & Stefan Prinz

—

Oktober 2022

[~]$ whoami

Stefan Prinz

In the past: Penetration Tester, Senior Security Consultant, Teamlead in DFIR
Now: Senior Manager for DFIR @ **KPMG** in Vienna, Austria

Offensive Security, DFIR,
Cyber Resilience Consulting, War Game Simulations, PurpleTeaming

Mountainbiking, Hiking, Snowboarding, Gutiar, Metal Music, Good food & wine

Daniel Kroiß

In the past: Developer @ Web start-up, InfoSec Officer at Bank
Now: Director for Cyber Security @ **KPMG** in Vienna, Austria

Security Architecture, Security Strategy, Technical Security Assessments, Incident Response, OT-Security, Red/Blue Teaming

Baseball, Alpine Skiing, Rock Music, Cyber Security, Biking

Intro

“If you spend more on coffee than on IT security, you will be hacked. What’s more, you deserve to be hacked.”

Richard Clarke – Special Advisor for the US Gov.

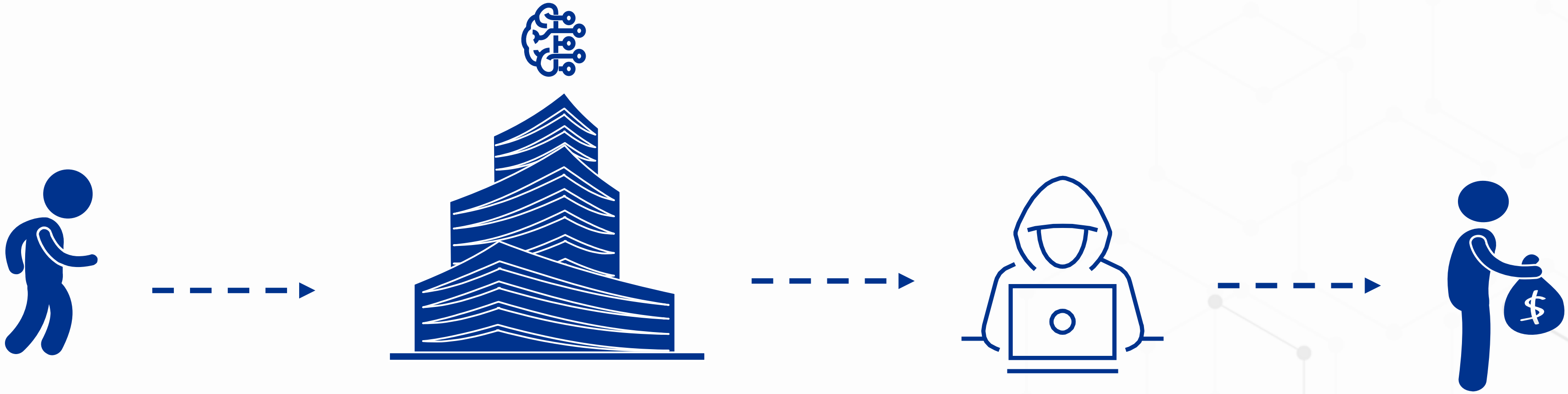
Editors Note: Coffee *is important* though!

More and more **organizations** are now turning to **externally (co-)managed** Security operation centers (**SOCs**). These professional Security service providers **promise up to 24/7 monitoring** of their customers' IT infrastructure at a relatively **low price** in order to detect and prevent attacks as early as possible. But the **important question** remains: is this really the **solution** to all **of our problems**?

Prevention vs Detection

A motivated attacker will always breach your network.

It‘s a cost-benefit-thingy.



Prevention only has failed! Assume Breach!

By getting full-coverage visibility in your network, you‘ll be able to detect attacks, once they were successful.

Fun with fla… Facts.

Ransomware costs and Payment

$228k

Average payment amount

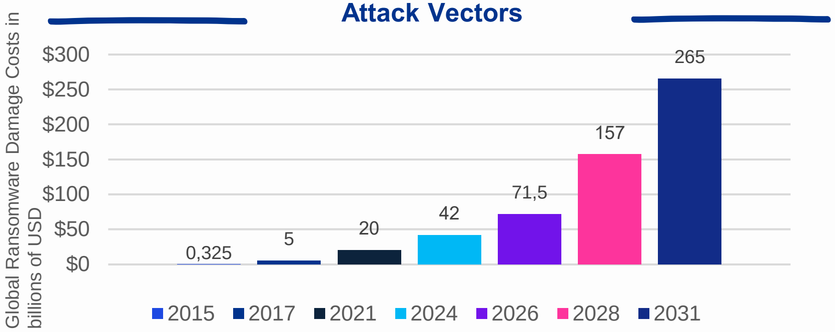
+8% % from Q1 2022

24 days

Average Downtime

-8% % from Q1 2022

Attack Vectors



Targeted Industries

Professional Services	~21,9%
Public Sector	~14,4%
Health Care	~10,0%
Software Services	~9,4%

30% Of Ransomware Attacks were performed by BlackCat and Lockbit 2.0

Annual budget in AT for cyber security	2020	2021
Over 10% of the IT budget	7%	10%
6 - 10% of the IT budget	6%	18%
3 – 5% of the IT budget	11%	20%
1 – 2% of the IT budget	6%	11%
Under 1% of the IT budget	6%	4%
"We don't have a dedicated budget for cyber security."	26%	26%
„I don‘t know“	37%	11%
Companies:	382	201

Source: KPMG Cyberstudie 2021

Source: Coveware: https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022
https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

What my SOC typically can, and can’t do

Individual service levels are dependent on the respective contract, service provider and may differ from this list!

What they typically do:

- Threat Detection & Prevention
- Incident Escalation
- Vulnerability & Asset Mgmt
- Reporting KPIs to Mgmt
- .....

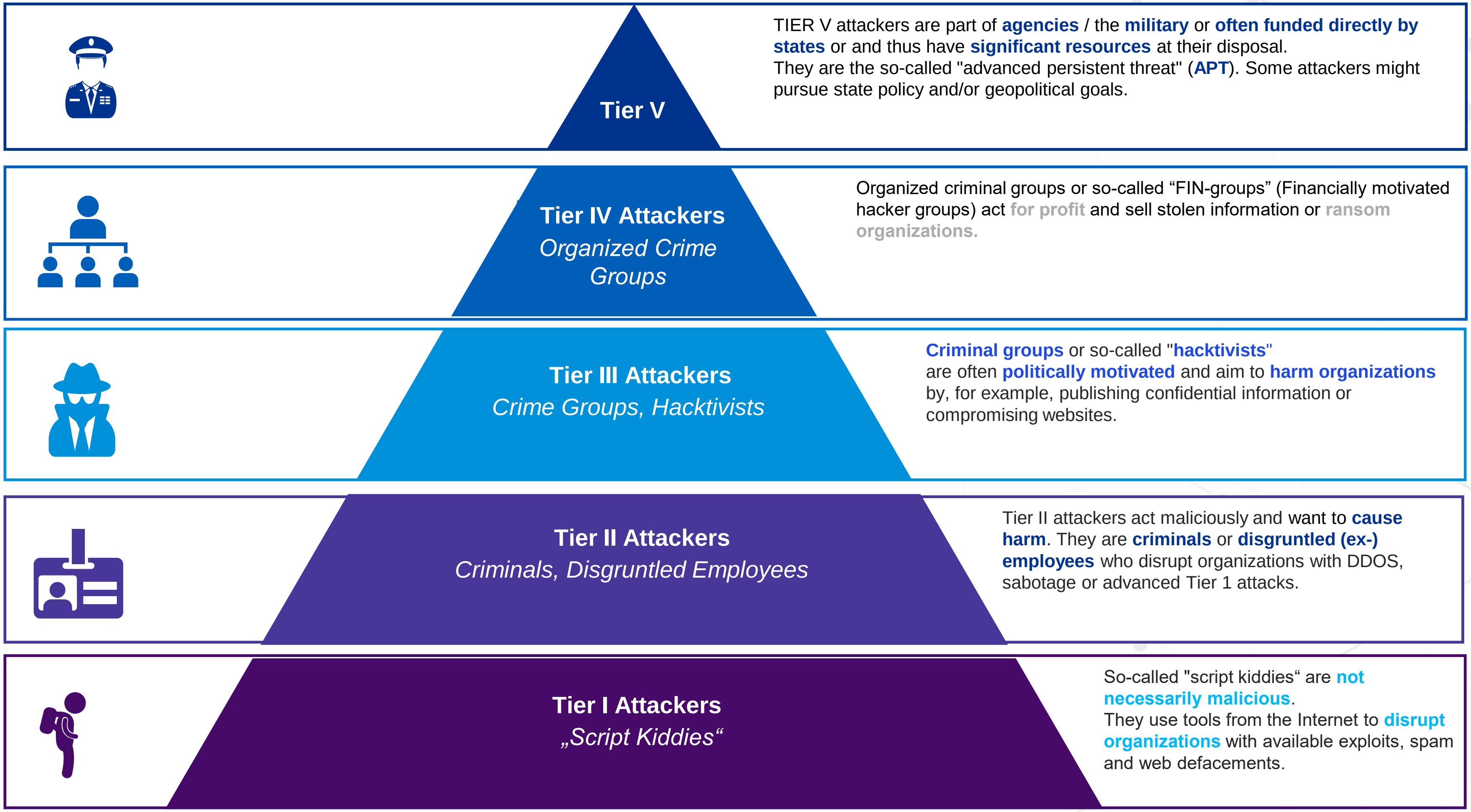
What they typically cannot do:

- Incident and Crisis Management
- Making Business Decisions
- Invasive containment measures
- Backups and disaster recovery
- .....

This can only lead us to one conclusion:

One does not simply rely solely on a managed SOC

Threat Actors – Mapped and Categorized



Tier V

TIER V attackers are part of **agencies** / the **military** or **often funded directly by states** or and thus have **significant resources** at their disposal.
They are the so-called "advanced persistent threat" (**APT**). Some attackers might pursue state policy and/or geopolitical goals.

Tier IV Attackers
Organized Crime Groups

Organized criminal groups or so-called "FIN-groups" (Financially motivated hacker groups) act **for profit** and sell stolen information or **ransom organizations.**

Tier III Attackers
Crime Groups, Hacktivists

Criminal groups or so-called "**hacktivists**"
are often **politically motivated** and aim to **harm organizations** by, for example, publishing confidential information or compromising websites.

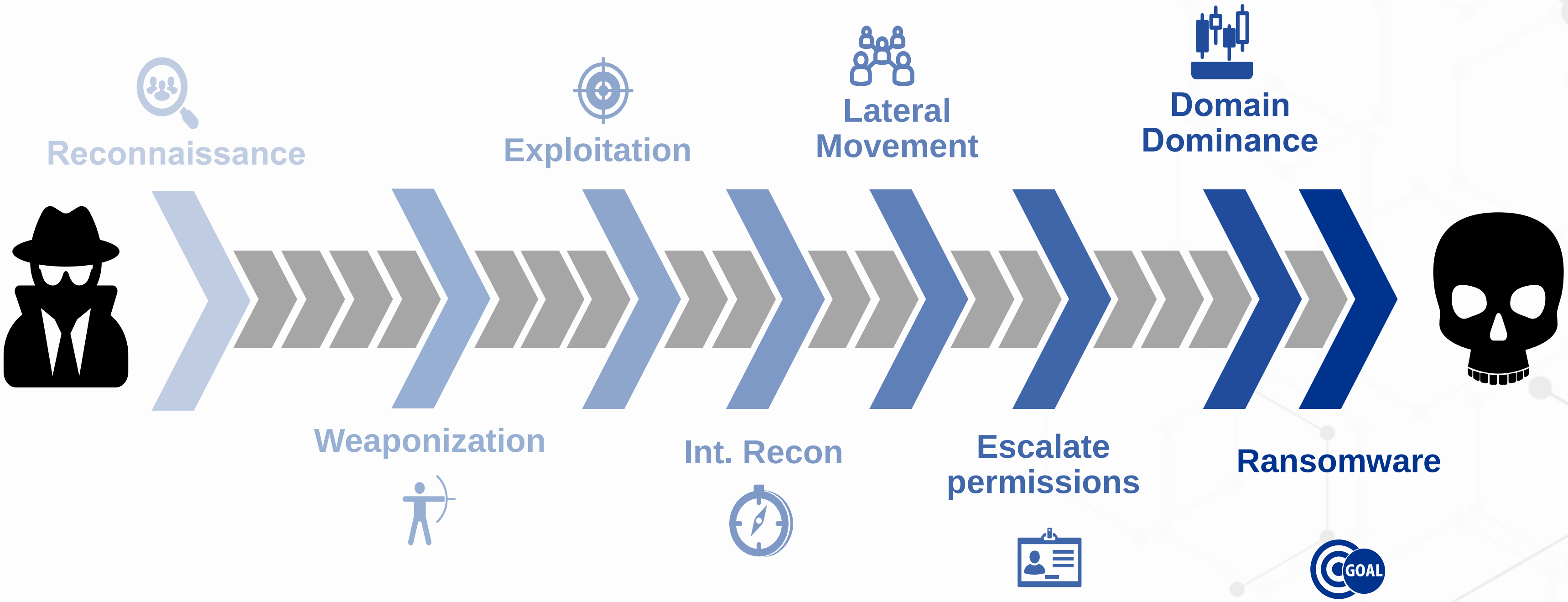
Tier II Attackers
Criminals, Disgruntled Employees

Tier II attackers act maliciously and want to **cause harm**. They are **criminals** or **disgruntled (ex-) employees** who disrupt organizations with DDOS, sabotage or advanced Tier 1 attacks.

Tier I Attackers
„Script Kiddies"

So-called "script kiddies" are **not necessarily malicious**.
They use tools from the Internet to **disrupt organizations** with available exploits, spam and web defacements.

The Cyber Kill Chain



So what could that mean irl?

Meet our Contenders

FIN1337 - Tier IV Threat Actor

- Professionally organized group of offensive hackers
- Expertise in all phases of the cyber killchain
- Proficient in monetizing hacks via Ransomware
- Kids want nice Christmas presents

Munder Difflin

- Medium to large organization.
- Heavily reliant on IT systems for daily work.
- Co-Managed SOC model.
- Leverages SIEM, EDR and other typical IDS/IPS systems
- Loves to click on shiny links and attachments

Round 1 – Recon to Exploit

FIN1337

Munder Difflin… Quaterly report looks nice, +15%. I wonder what their Security looks like

Managed SOC, SIEM, EDR… Thanks LinkedIn OSINT. Looks tough but could be worth my while.

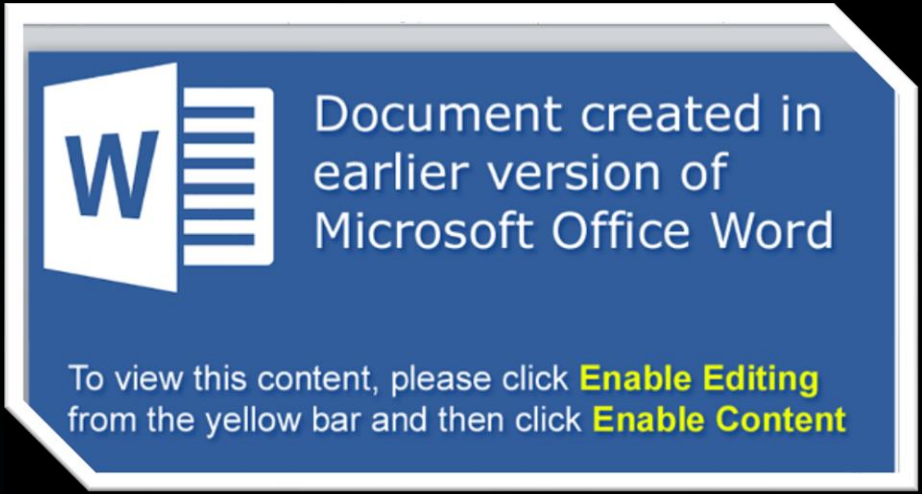
Let‘s craft a nice payload for this *letter of application* to bypass their EDR, upload to their application website and then…

Round 1 – One click to pwn them all

HR
Kam

What a refreshing application from this candidate. Let’s see the CV next. Huh? What‘s that?

Okay let‘s do that… Wow, very good candidate. Better forward it to the Teamlead to get an interview with him!



Document created in earlier version of Microsoft Office Word

To view this content, please click **Enable Editing** from the yellow bar and then click **Enable Content**

Round 2 – Hello? Who's there? Must have been nothing

FIN1337

… And there's the shell!
Process migration & dropper persisting in user space done. Time for some priv-esc…

….

What in tarnation! My file got pwned… I'll stay low for a while and keep my foothold.

SOC
John

SIEM Alert **Ticket#58008**

TrojGenMalBlah-1337xyzwhatdoesthismean **was identified, quarantined and removed by EDR**

Nice. Good job EDR. Ticket - closed!

A few days later...

Round 3 – Stairway to Heaven or Highway to Hell?

FIN1337

Slow and steady wins the race.
Admin creds in that PowerShell script.
Let‘s cruise through the domain with it, shall we?
Since all their administrators use psexec, let’s do that as well.

SOC
John

SIEM Alert **Ticket#58009**

Unusual SMB traffic detected.

SIEM Alert **Ticket#58010**

Unusual administrative account usage detected.

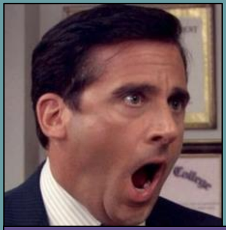
This requires invasive containment measures to control. I’ll escalate to the client immediately!

Round 4 – We have to talk…

SOC
Munder Difflin

You network has been compromised. Here's what we suggest:

- Isolate all affected machines, potential negative business SLA impact
- Reset all passwords & AD golden ticket
- Identify the root cause of the problem
- Activate your crisis team and prepare for the wurst.



CISO
Mark

How could this even happen?
Shouldn't the SOC protect us from attacks?
How are your suggestions affecting my business?

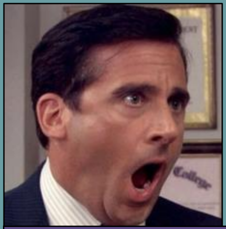
Round 4 – I didn't sign up for this

SOC
Munder Difflin

We did what we are here fore:

- Detecting threats
- Escalating critical alerts
- Recommending measures

We are not authorized to isolate large parts of your network/business services. We don't even have access to all your tools!



CISO
Mark

We are not organized for a crisis like this!
Who can tell me what effects an isolation like this has?
Who do we have to inform?

…

And why can't I open my files anymore? How should I check my crisis plan now?

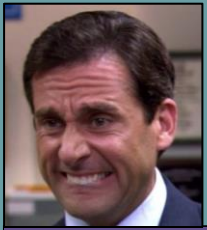
Maybe this is a good time to update my CV and LinkedIn profile?!

Round 5 – Game Over

FIN1337

Hey Munder Diflin – how about paying?

Need us to help you to get the Monero?



CISO
Mark

Hold on.. We’re not paying.. Let’s find out:

What states are our backups in?

Are they also compromised or even encrypted?

What systems do I restore first?

How could this all even happen?!?!

Immediate technical lessons learned?

[1] **Configuring secure backups and restoring** after ransomware attacks are typically not part of a Managed SOC.

[2] A Managed SOC **needs extensive privileges and competences** in the monitored organization in order to be able to work effectively at all. Or it is scope and effectiveness is limited – be aware of a false sense of Security!

[3] It must be **clear to all parties**, what the managed SOC is **contracted** to do. The rest is left to do for the organization.

[4] **Procedures for emergencies** are **to be defined** and, above all, **practiced** in order to clarify who has which competencies and tasks in emergency situations.

Back to theory – think about the following: What can a SOC do? What should a SOC do?

1. Which Roles should your SOC play? Which can it play?

Level 1: SOC Analyst

- **Reviews** the initial SIEM/EDR/other detection tool **alerts**
- Evaluate false-/true-positive status, determine **relevancy** and **urgency**
- Manages and configures security monitoring tools
- Creates new **trouble tickets** for alerts that **signal an incident** and **require** Level 2 **review**

Level 2: First Responder & Incident Handler

- **Reviews trouble tickets** generated by Level 1 Analyst
- Performs **triage** and **deep analysis**
- Correlates with threat intelligence
- **Identifies** the **threat actor**, nature of the attack and systems or data affected
- **Decision: declare incident? Escalate?**

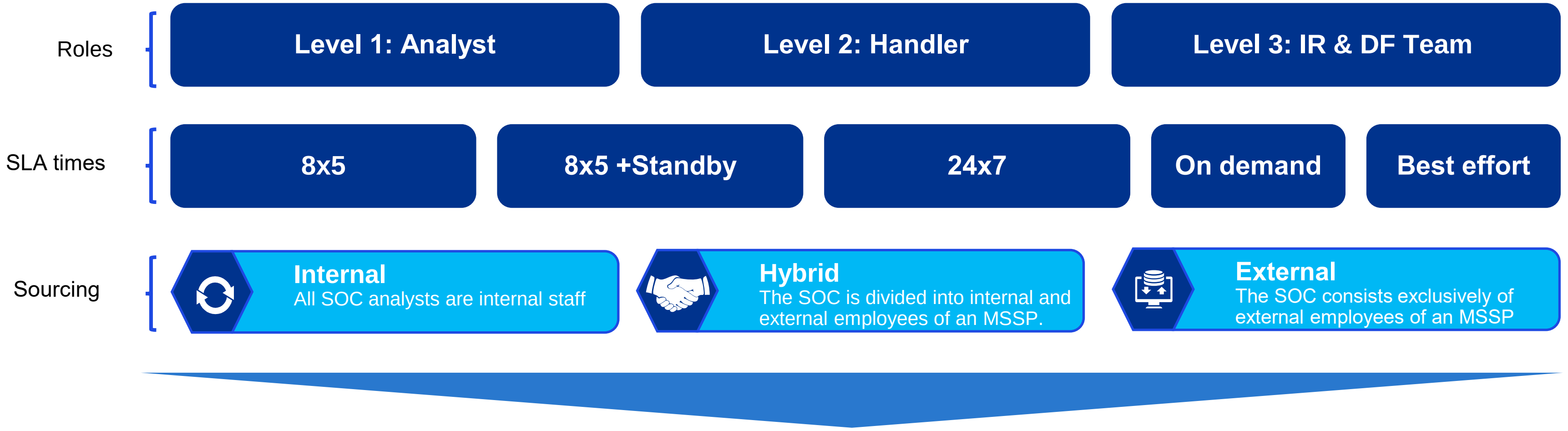
Level 3: IR Lead & Team

- Lead incident **identification, containment, eradication** and **recovery activities**.
- IR Team consists of members from **different departments** (including IT, Corporate Communication, Legal) that supports the IR Lead in incident handling.
- Recommends how to **optimize security monitoring tools** based on threat hunting discoveries.
- **Shutdown** business services.
- **Digital Forensics**

2. What SLA times do you expect for each level?

8x5	The analysts work Monday till Friday from 9 to 5. An attack on Friday night will not be handled until Monday morning.
8x5 **+ Standby**	Additionally, to the analysts working during normal hours, there is always a person on standby in case an incident occurs.
24x7	Analysts are working 365 days a year around the clock.

Mix & Match – Your SOC TOM



Roles

- Level 1: Analyst
- Level 2: Handler
- Level 3: IR & DF Team

SLA times

- 8x5
- 8x5 +Standby
- 24x7
- On demand
- Best effort

Sourcing

- **Internal** All SOC analysts are internal staff
- **Hybrid** The SOC is divided into internal and external employees of an MSSP.
- **External** The SOC consists exclusively of external employees of an MSSP

Any combination is possible to build a complete SOC Operating Model. It could well could look like:

Level 1 – 24x7 – External MSSP 1 (SIEM, Firewall, EDR) / Best-effort – Internal (Proxy, Ops Logs, Cloud Alerts, CASB, CSPM Vuln. Mgmt,…)

Level 2 – Best effort – Internal SOC Team (Human-intelligence based correlation)

Level 3 – On-demand – External MSSP 2/3 (Cyber Insurance, DFIR support contracts, etc.) / best-effort – internal (IT)

Choose your weapons: Which SOC Target Operating Model is the right for you?