CROWDSTRIKE

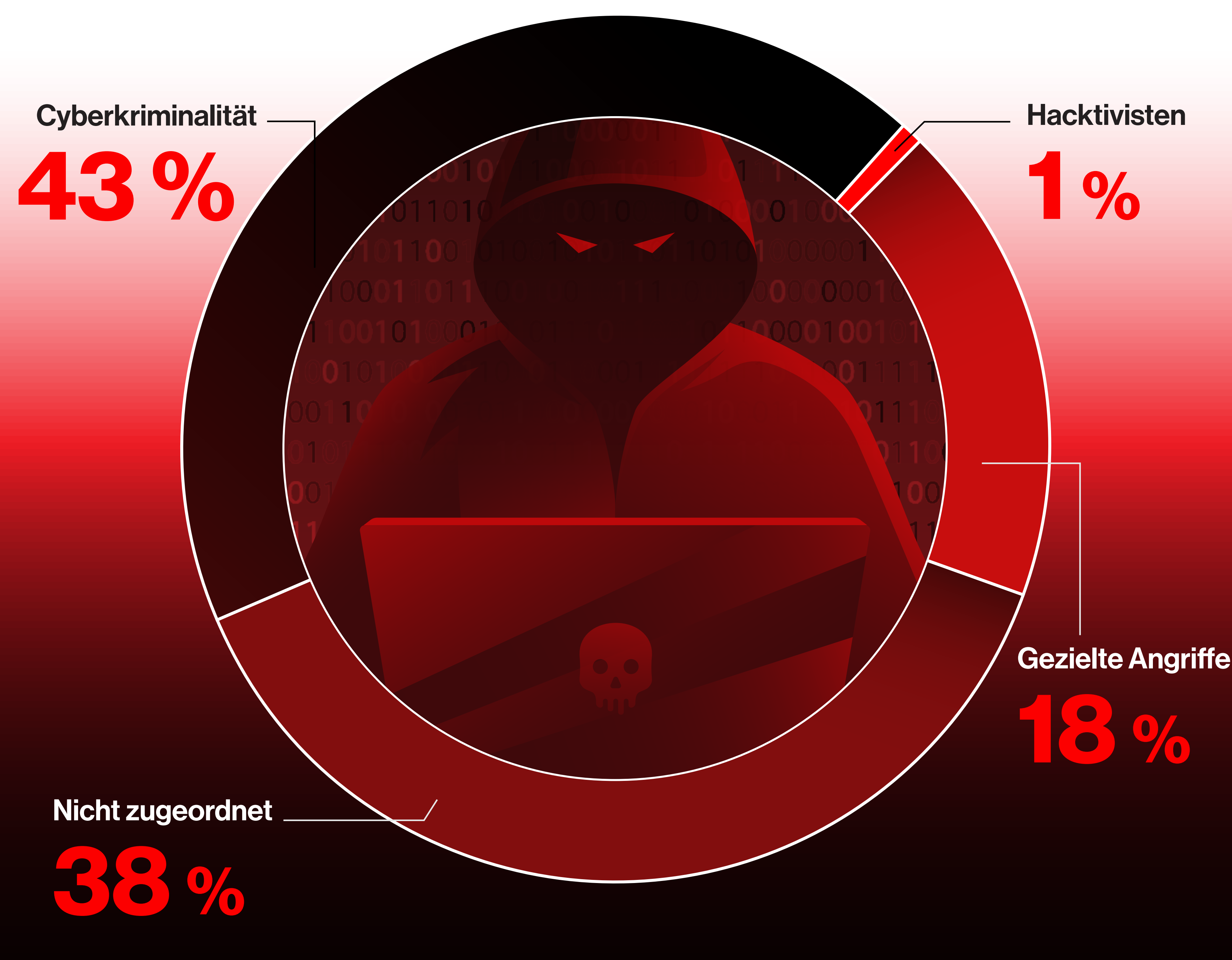
NOWHERE TO HIDE

Threat Hunting Report des Falcon OverWatch-Teams 2022

Das CrowdStrike Falcon OverWatch™-Team, das täglich rund um die Uhr nach Bedrohungen sucht, veröffentlicht jedes Jahr die aktuellsten Ergebnisse seiner technischen Analysen. Schwerpunkt sind dabei neue und beliebte Vorgehensweisen von Bedrohungsakteuren sowie aktuelle Trends bei Kompromittierungen, die in den vorherigen zwölf Monaten vom 1. Juli 2021 bis 30. Juni 2022 beobachtet wurden. Im vergangenen Jahr hat das OverWatch-Team besonders starke Veränderungen bei der Ausgestaltung und Umsetzung der Angriffe beobachtet.

Mehr Angriffe, mehr Komplexität

2022



71 %
der vom OverWatch-Team erkannten Bedrohungen enthielten keine Malware-Komponente

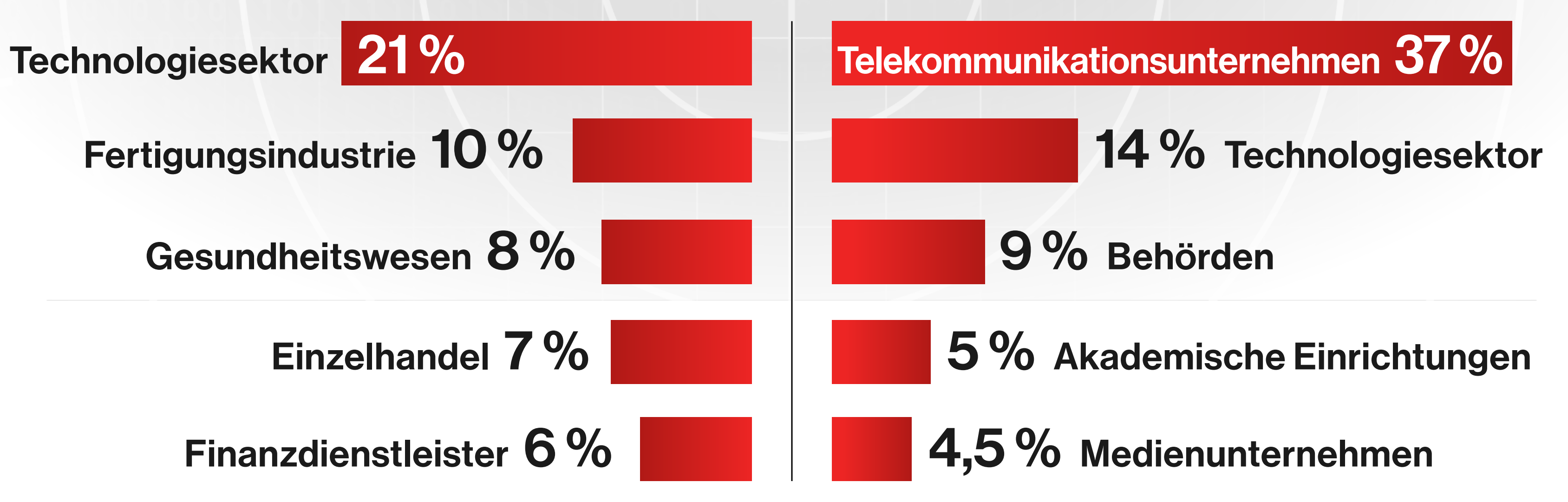
50 %
Zunahme interaktiver Hands-on-Keyboard-Aktivitäten im Jahresvergleich

1:24 Std.
durchschnittliche Breakout-Time

Die Motive der Bedrohungsakteure bestimmen die Angriffsstrategie

Top 5 der Branchen nach Angriffstyp

Cyberkriminalität vs gezielte Angriffe



Cyberkriminalität = Finanziell motivierte Angriffe
Gezielte Angriffe = Staatlich unterstützte Angriffsaktivitäten

Neue und erwähnenswerte Taktiken

IceApple

Taktiken
Umgehung der Schutzmaßnahmen, Anmeldedatenzugriff, Exfiltration

Ziele
IIS-Server

Beschreibung
- Hochentwickeltes .NET-basiertes Post-Exploitation-Framework
- Nutzt reflektiv geladene .NET-Assemblys aus
- Geringer forensischer Footprint, speicherbasiert

fscan

Taktiken
Erkennung

Ziele
Interner Host, Kartografierung der Umgebung

Beschreibung
- Seit Ende 2021/Anfang 2022 gängiges Angreifertool
- Schwachstellenscanner, der jetzt für erweitertes Fingerprinting verwendet wird
- Ausnutzung erfolgt per modifiziertem öffentlichem Schlüssel, SSH-Befehle

Sweet Potato

Taktiken
Erweiterung der Zugriffsrechte

Ziele
Windows-Anmeldedaten, Sicherheitstoken

Beschreibung
- Erzwingt Systemauthentifizierung zur Erfassung übertragener Anmeldedaten
- Erste Variante („Hot Potato") bereits 2016 entdeckt
- Automatisches Skript probiert mehrere Varianten aus (z. B. Juicy Potato, Lonely Potato)

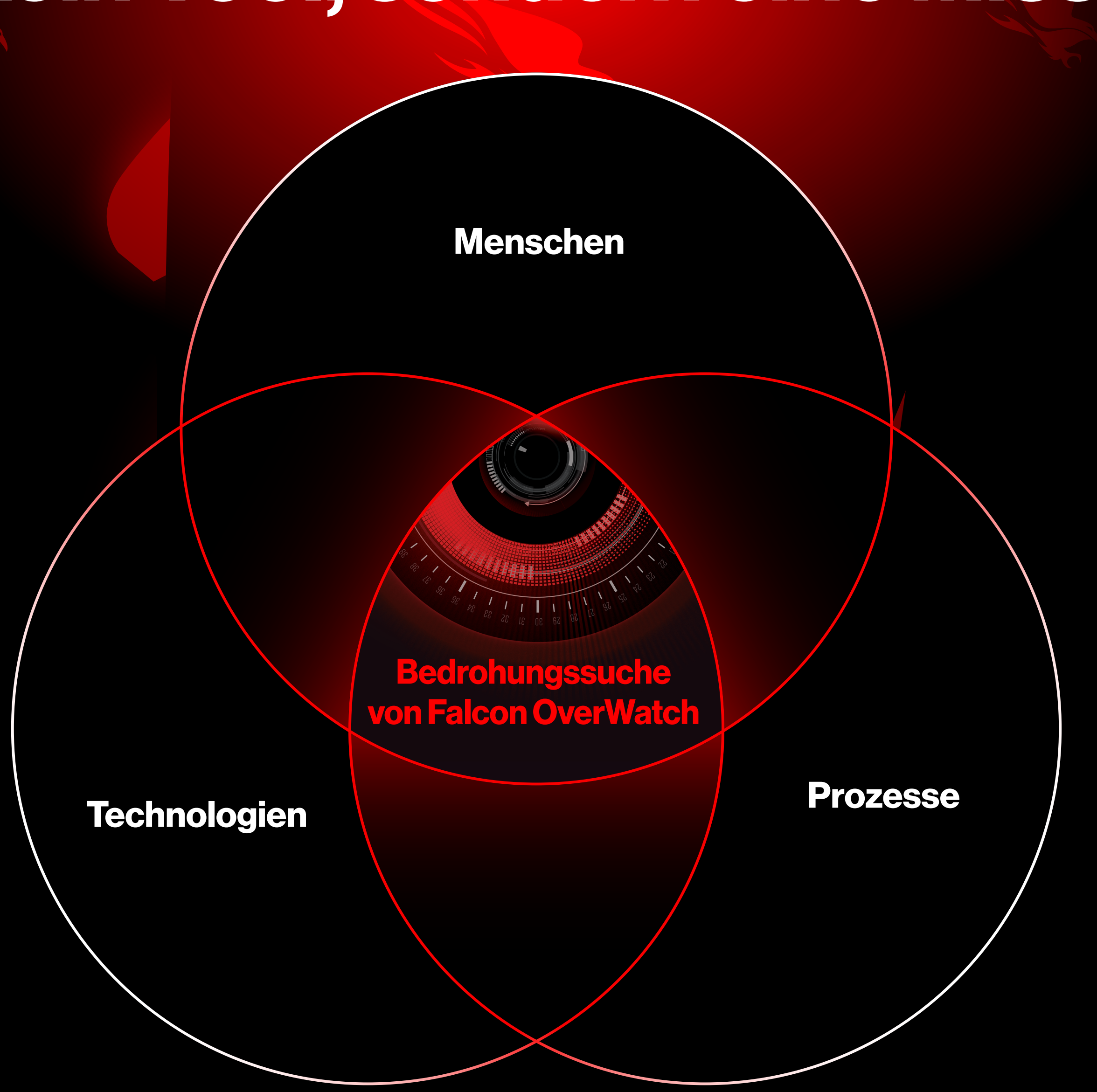
Web Server Zero-Day

Taktiken
Persistenz (per WebShell), interaktive Reconnaissance, Erfassung von Anmeldedaten, Exfiltration

Ziele
Instanzen von Confluence-Servern und -Rechenzentren

Beschreibung
- Schwachstelle ermöglicht Ausführung von nicht authentifiziertem Remote-Code
- Bei Cybercrime- und gezielten Angriffen beobachtet
- Testangriff umfasste WebShell-Bereitstellung, interaktive Reconnaissance, Erfassung von Anmeldedaten, Abruf von Remote-Tools

Proaktive Bedrohungssuche ist kein Tool, sondern eine Mission



Die Taktiken kennenlernen.
Die Bedrohungsakteure kennenlernen.
Rund um die Uhr Angriffe abwehren.

Threat Hunting Report des Falcon OverWatch-Teams 2022

Vollständigen Bericht herunterladen →

Weitere Informationen finden Sie unter: https://www.crowdstrike.de/services/

Folgen Sie uns:

CROWDSTRIKE

We Stop Breaches