illusive

Assume Breach

Senior Sales Engineer EMEA, Wolfgang Halbartschlager

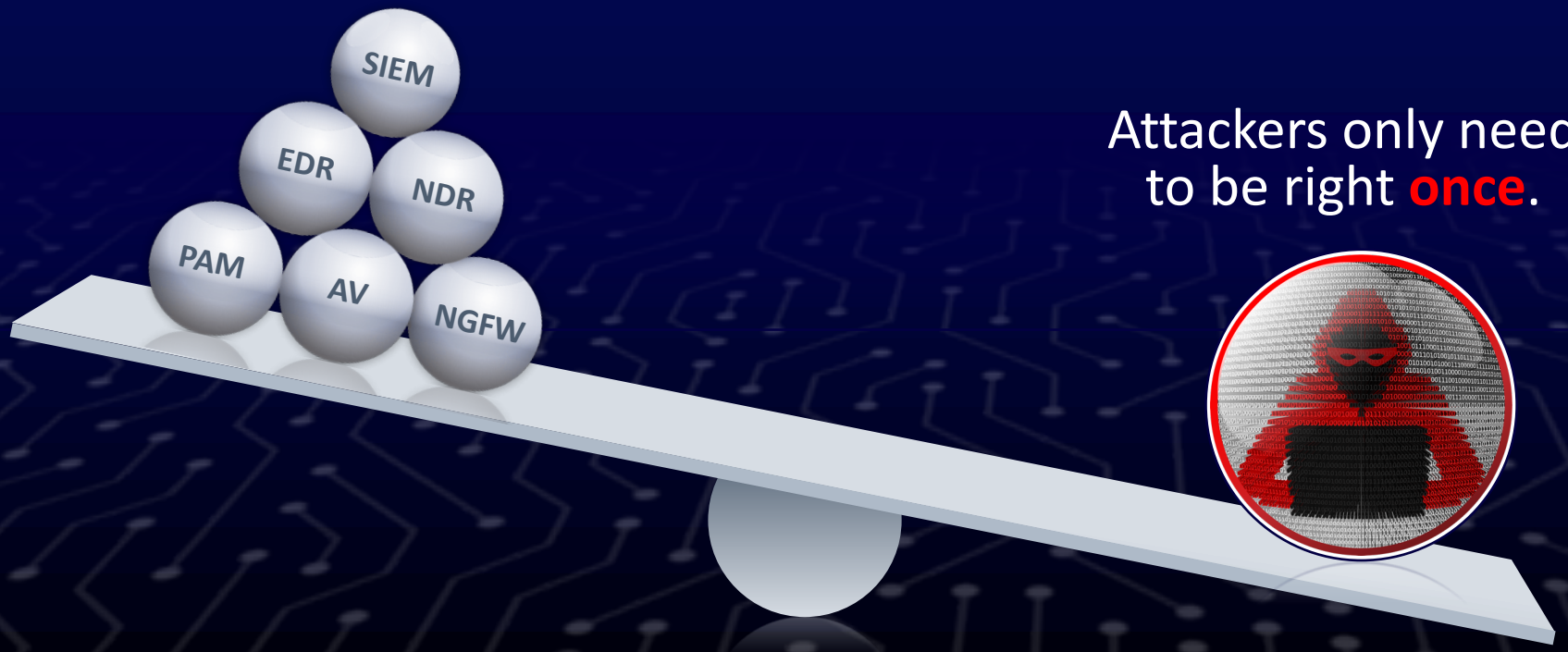
Built by Attackers to Beat Attackers

Agenda

- Aktuelle Lage
- Vorgehensweise moderner Angreifer
- Solarwinds Angriff
- Moderne Verteidigungsstrategien
- 6 Tipps zur Risikominimierung
- Q & A

Aktuelle Lage

Defenders need to be right **every time**.



Attackers only need to be right **once**.

solarwinds

18,000
potentially impacted

RANSOMWARE

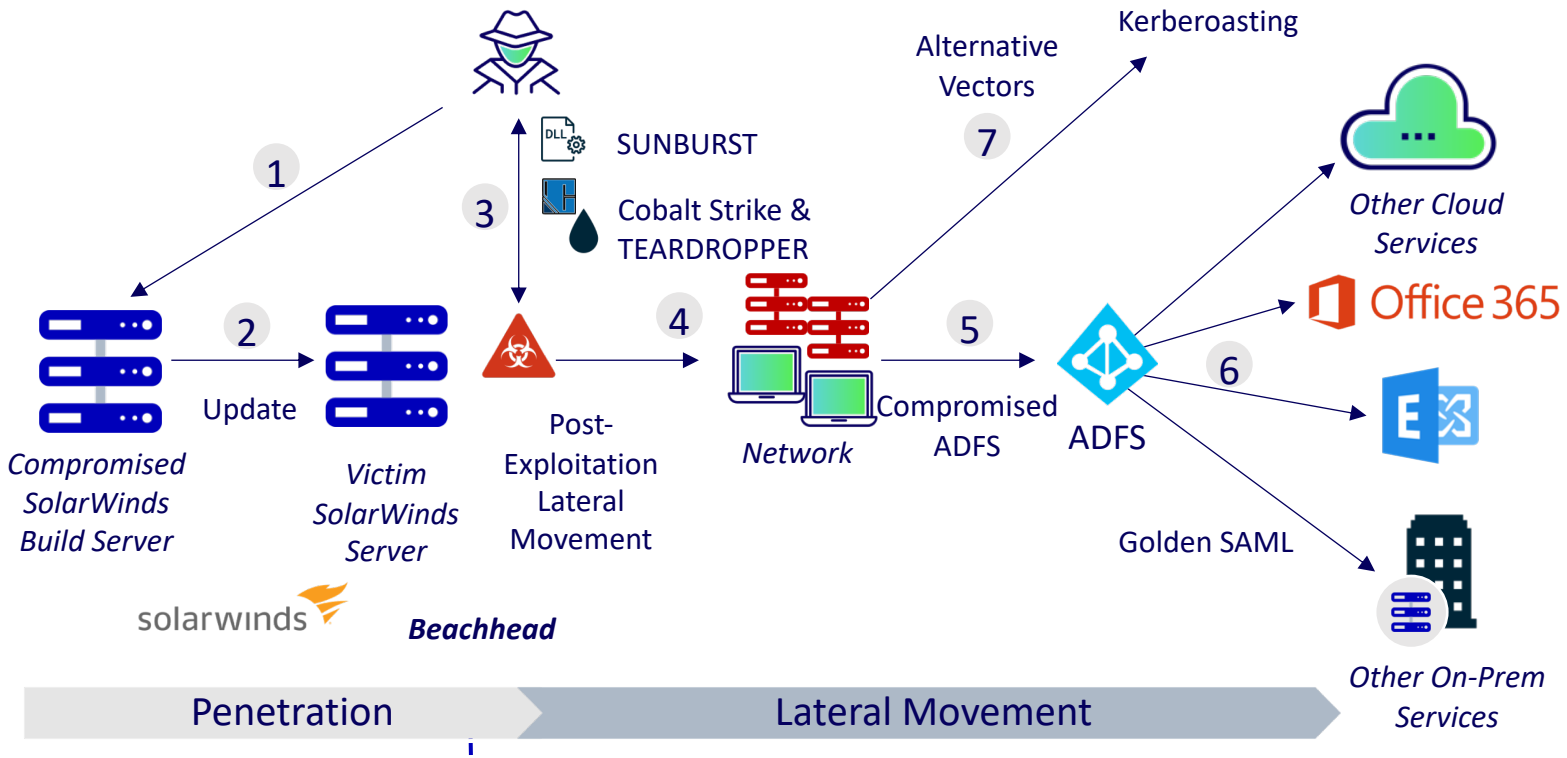
700%
rakes in
$1B annually

ILLUSIVE
ACTIVE DEFENSE

stopped
100+
ransomware
nation-state and insider

illusive

SolarWinds Angriff



Penetration | Lateral Movement

Assume Compromise

- Credential & Session Harvesting
- Privilege Escalation
- Impact

Moderne Verteidigungsstrategien

6 Tipps zur Risikominimierung

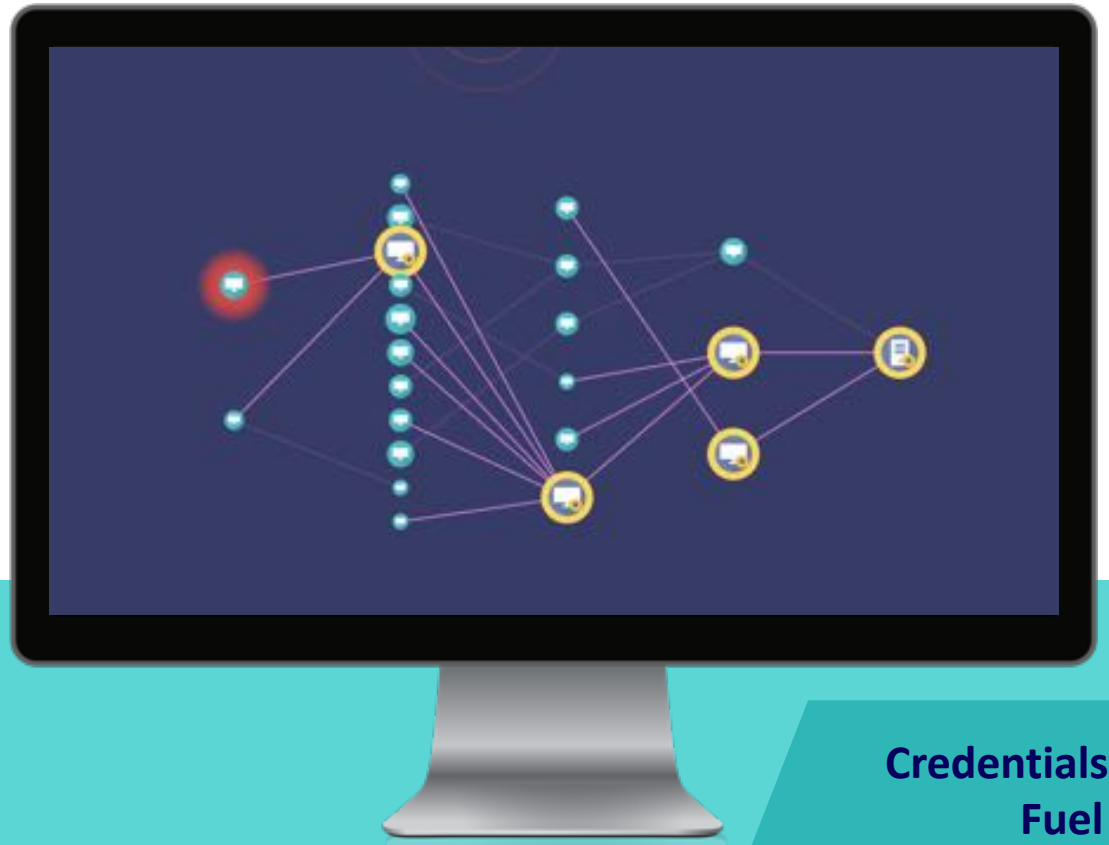
Security Awareness	Alle Mitarbeiter inclusive Mangement & IT schulen lassen. Verpflichtend für ALLE. Natürlich gilt das auch für Mitarbeiter aus der IT selbst.
NextGen AV EDR	Signaturbasierte Erkennung reicht nicht mehr aus. Alle namhaften Hersteller sind eine gute Wahl. Der Microsoft Defender hat ebenfalls eine EDR Variante namens Defender ATP bzw. Defender Endpoint. Teilweise ist dieser bereits in der Office 365 Lizenz (zB E5) mit dabei.
Sicherheit von Priviligierte Accounts	Nicht nur Domain Admins sind priviligierte Benutzer. Regelmäßige Passwortänderungen, MFA verwenden wo möglich, LAPS ist kostenlos für Lokale Admin User, Failed Logons überwachen (Event IDs 4768,4625,4771,4776 – Audit)

6 Tipps zur Risikominimierung

Sicherheitsrichtlinien umsetzen	Klare Richtlinien die für ALLE gültig sind. Ordnungsgemäß abmelden, keine Sessions offen lassen. Richtlinien müssen eingehalten warden.
Servicebenutzer	Servicebenutzer sind Servicebenutzer und keine normalen Benutzer. Least Privileges einhalten, Nicht für alles einen Domain Admin verwenden, Service Benutzer nicht für interactive Logons verwenden, RDP Login für Servicebenutzer disablen
Angreifer-früherkennung	Angreifer bleiben oft über Monate, sogar Jahre im Netzwerk. Über zusätzliche Technologien nachdenken. Zusätzlich zu Behaviour Analysen kann Deception Technologie helfen um Insider oder zielgerichtete Angriffe inkl. Ransomware frühzeitig zu erkennen.

Risiko identifizeren & minimieren

Before → After



Credentials and Pathways
Fuel Attacks

illusive

Tarnen & Täuschen (Deceptions)

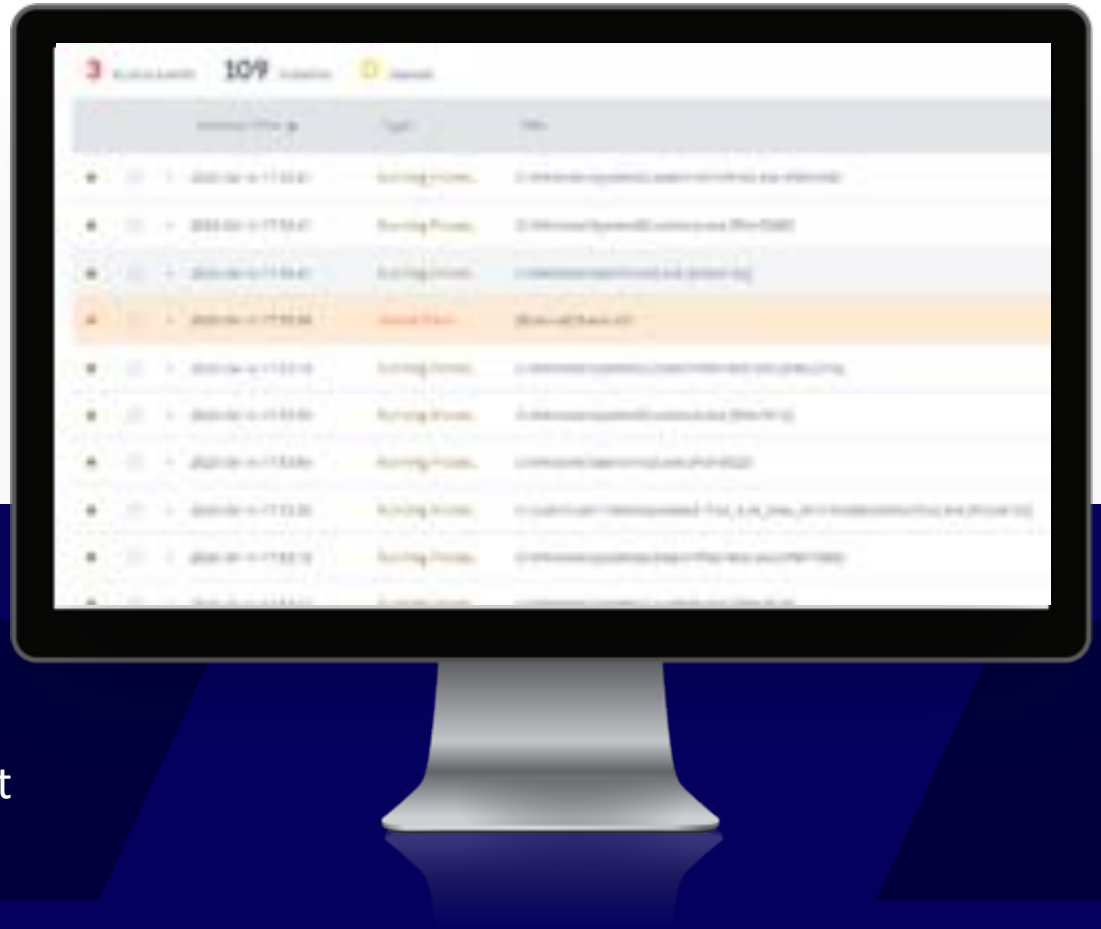
Before → After

UNDEFEATED versus 100+ Red Teams

Microsoft MANDIANT cisco

illusive

Forensische Analysen



60-90%

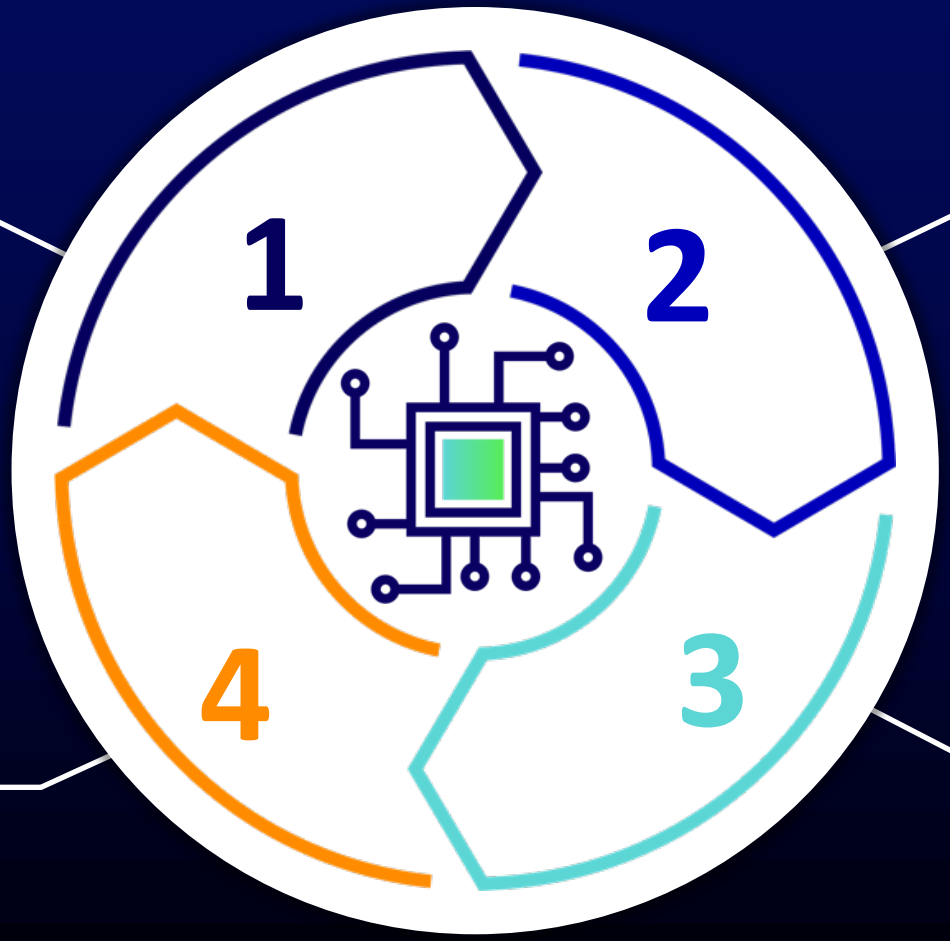
reduction in SOC analyst investigation time

SOURCE-BASED
FORENSICS

illusive

Shake the Tree

Assume Compromise
Force attackers to move in order to surface their existence



Eliminate accessible credentials & pathways

Surface privileged credentials and pathways on SolarWinds Orion and ADFS servers and general environment

Bolster lateral movement detection strategy

Ensure strategy and technologies are in place and fully implemented

Monitor for lateral movement

Monitor for attackers' movement in their pursuit to regain access

Reset administrator passwords

Reset password for privileged accounts that attacker may have access to

illusive

Danke

wolfgang@illusive.com

Assume Breach, Stop attackers from moving laterally

Built by Attackers to Beat Attackers