WithSecure Co-Monitoring Service

Thomas Tyroff, THOLD-IT
Daniel Knist, WithSecure

WITH secure

WithSecure Co-Monitoring service

- Monitoring (24/7 or out-of-hours) of severe-risk detections by WithSecure
- Validation and investigation of severe-risk detections by a human threat analyst
- Confirmed attacks are escalated directly to customers or partners on-call
- Threat Analyst provides containment advice for fast and effective remediation
- Possible to escalate to Incident Response services with or without IR Retainer

Outcome

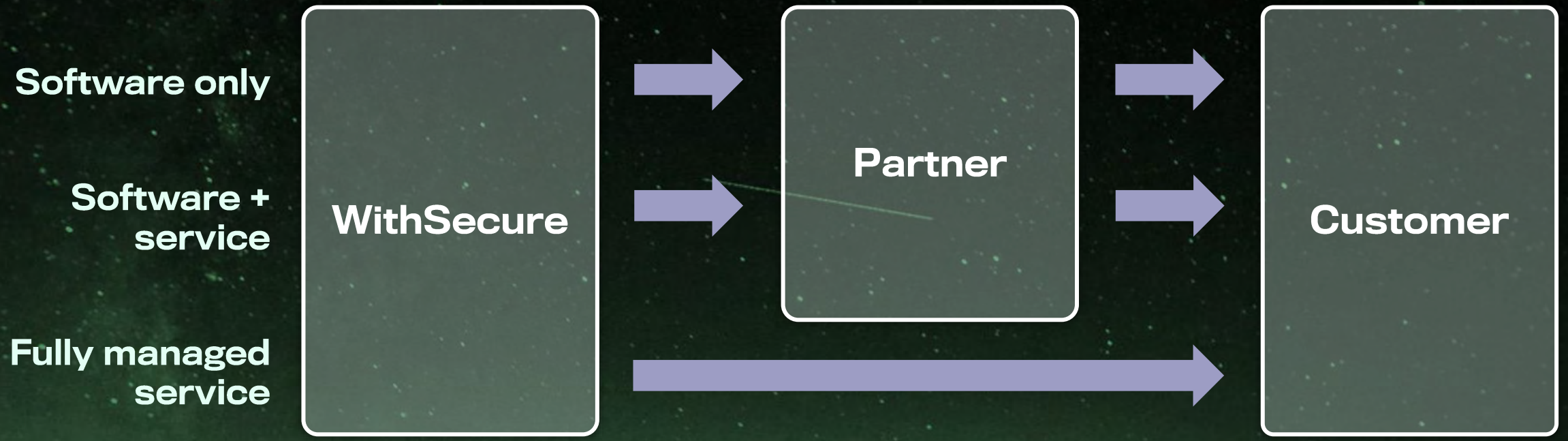
- **Improved resilience**
- **Minimized disruption and unplanned expense**
- **Customer trust**

How Co-Monitoring works

Detection & response portfolio

Feature	EDR	EDR + Elevate	EDR + Co-Monitoring
Detection	YES	YES	YES
Alerting	NO	NO	YES
Investigation	NO	YES	YES
Response guidance	NO	YES	YES
Response action	NO	NO	NO
IR Retainer (IRR)	OPTIONAL	OPTIONAL	OPTIONAL
IR days	NO	OPTIONAL for IRR customers	OPTIONAL for IRR customers
Threat hunting	NO	NO	NO
Security posture analysis	NO	NO	NO
Delivery	N/A	24/7	Out of office hours or 24/7
Offering	Software only	Software + service	Software + service

Commercial model




Erweiterte Services
To be continued.....


Cybersecurity
Resilienz schaffen, konsolidieren, entwickeln!
Thomas Tyroff &
Attila Tezsevin
THOLD-IT GmbH

THOLD-IT

- Corporate Development
- Outcome based Cybersecurity as a Service
- Auswahl, Betrieb und Umsetzung komplexer ICT-Projekte
- Interim CIO, CISO as a service
- Datenschutz Management
- Prozess- und Risikomanagement
- Incident Mangement & Desaster Recovery
- Notfall Rechenzentrum
- Umsetzung der normativer Anforderung, beispielsweise aus:
  DIN EN ISO 2700x,, BCM ISO 22301, NIS2 (Kritis), IT-Notfallplanung nach BSI 100-4

W / T H secure

24/7 Co-Monitoring von WithSecure "Schlafen Sie ruhig – wir passen auf!"

Warum 24/7 Co-Monitoring?

- Cyberkriminelle schlafen nicht
- Angriffe finden statt während wir uns ausruhen.
- Enorme Kosten: Cyberangriffe kosten Unternehmen Millionen.
- Rund-um-die-Uhr-Schutz
- Echtzeitüberwachung durch Experten
- proaktive Bedrohungserkennung und sofortige Reaktion
- Wie funktioniert es?
- Sicherheitsüberwachung: 24/7, 365 Tage im Jahr
- Sofortige Alarmierung
- Bei verdächtigen Aktivitäten an die definierte Alarmkette
- Detaillierte Berichte
- Regelmäßige Updates und Analysen

Geschäftschancen für Partner

- **Erweitertes Angebot für eure Kunden**
- **Was machen andere MDR Anbieter? Was fehlt?**
- **Incident Response Team gründen! Regie behalten!**
- **Wiederkehrende Einnahmen realisieren**
- **Abonnement-Modelle steigern Umsätze.**
- **Vertrauen und Zuverlässigkeit herstellen**
- **Jahrzehntelange Erfahrung und hochqualifizierte Experten**
- **Erwartbares Feedback:**
- **"Seit wir das 24/7 Co-Monitoring von WithSecure nutzen, fühlen wir uns sicherer und können uns endlich wieder auf unser Kerngeschäft konzentrieren."**