© 2022 SPLUNK INC.

Welche Teile des Sicherheitsbetriebs können an einen **Managed Security Service Provider (MSSP) ausgelagert werden?**

		Szenario 1 Erweiterung des eigenen SOCs	Szenario 2 Co-Managed SOC		Szenario 3 Fully Managed SOC
Kunde übernimmt	SOC BETRIEB	Level 2+ Event Handling Incident Response Level 1 Triage and Alert-Priorisierung	Level 2+ Event Handling Incident Response	Level 2+ Incident Response	Endgültige Entscheidung über Maßnahmen zur Incident Response
	TECHNOLOGIE	SIEM / SOAR	SIEM / SOAR	SIEM / SOAR	
MSSP übernimmt	SOC BETRIEB	1. Kunde nutzt ausgelagerte Analysten (Erweiterung) 2. Der Kunde erhält regelmäßig Berichte und Risikoanalysen	Level 1 Triage and Alert-Priorisierung	Level 1 Triage and Alert-Priorisierung Level 2+ Event Handling	Level 1 Triage and Prioritization Level 2+ Event Handling Incident Response
	TECHNOLOGIE				SIEM / SOAR

Level des SOC-Betriebs

**Level 2+ = Level 2 oder Level 3*

Level 1

- Echtzeit Security-Event-**Monitoring** und Level-1-**Incident Investigation**
- **Priorisierung von** Security Alerts

Level 2

- Event Handling: **komplexe Analyse von Vorfällen**
- Unterstützung bei der **Abwehr** von Angriffen

Level 3

- Incident Response
- Threat Hunting: Unterstützung **komplexer Incident Response-Prozesse**
- **Forensische Analyse**, z. B. mit Threat Intelligence

splunk> turn data into doing