

Integrierte Verwaltung von IT/OT Sicherheitsprotokollen



Einleitung

Informationstechnologie (IT – Information Technology) und Betriebstechnologie (OT – Operational Technology) wurden einst mit unterschiedlichen Zielsetzungen konzipiert und daher oftmals getrennt verwaltet. Der Wunsch, sowohl Leistung als auch die Feinregulierung von zunehmend komplexeren Netzen zu optimieren, hat jedoch eine Annäherung der beiden Technologien bewirkt. Die Integration kann allerdings eine Herausforderung darstellen, insbesondere im Bereich der Cybersecurity.

Die vorliegende Broschüre behandelt Herausforderungen, mit welchen Unternehmen im Rahmen der Etablierung von nachhaltigen Verwaltungssystemen für Sicherheitsprotokolle in der OT-Umgebung konfrontiert werden. Basierend auf der Verwendung traditioneller IT-Protokollüberwachungen wird letztlich eine Lösungsvariante aufgezeigt.

Viele Schlussfolgerungen der enthaltenen Beispiele stammen aus der Energiebranche. Die aufgezeigten Herausforderungen und Empfehlungen können jedoch auf alle Branchen, in denen OT zum Einsatz kommt, gleichermaßen angewandt werden.

Was versteht man unter Log-Management.

NIST SP 800-92 definiert Log-Management als das Erzeugen, Übermitteln, Speichern, Auswerten und Löschen von Sicherheitsprotokolldaten eines Computers.

Die Energiebranche unterliegt zahlreichen Regulierungen. Log-Management ist dabei ein zentraler Bestandteil der Sicherheitsüberwachung und dient der Einhaltung gesetzlicher Vorschriften. Versorgungsunternehmen verwenden die Protokollüberwachung als Nachweis zur Sorgfaltspflicht, falls es zu einer Sicherheitslücke kommt.

Wie Versorgungsunternehmen die Verwaltung von Sicherheitsprotokollen bewältigen

Versorgungsunternehmen bauen die Infrastruktur ihrer Sicherheitsprotokolle üblicherweise auf einer SIEM-Lösung (Security Information and Event Management) auf. Dies ermöglicht die Sammlung der Protokollierungen, Ereigniskorrelations- und Protokollanalysemöglichkeiten. Diese wiederum liefern erforderliche Berichte und Warnungen bei sicherheitsrelevanten Zwischenfällen, die den erforderlichen Nachweis für die Einhaltung der Cybersicherheitsstandards darstellen.

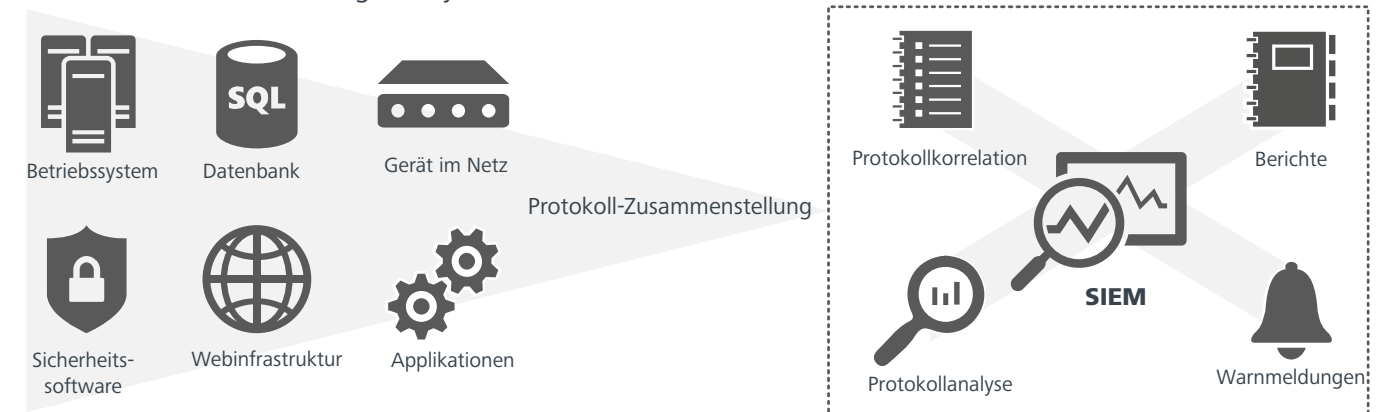


Abb. 1: So funktioniert Log-Management

Herausforderungen bei der Verwaltung von Sicherheitsprotokollen

Erfordernis beträchtlicher Investitionen

Obwohl SIEM-Anbieter eingebaute Korrelationsregeln, Berichte und Warnmeldungen bereitstellen, erfordert die Implementierung einer SIEM-Lösung nach wie vor beträchtliche Investitionen hinsichtlich Schulung und Einstellung von Sicherheitsfachleuten, welche die erfassten Daten analysieren und überwachen. Dies zwingt viele Organisationen, die Protokollüberwachung an ein globales Security Operations Center (SOC) auszulagern um Ressourcen zu sparen. Andere versuchen wiederum, durch die Implementierung einer einzigen SIEM-Lösung in verschiedenen Bereichen Einsparungen zu erzielen. Angesichts der unterschiedlichen Anforderungen, den einzuhaltenden Standards, variierenden Anwendungsfällen, unterschiedlichen Nutzer-Communities sowie divergenten Überwachungs-

strategien führen diese Einflussfaktoren ohne die richtige Integration selten zu einer optimalen Lösung.

Die Lösungen sind für den OT-Bereich häufig untauglich

Die meisten SIEM-Lösungen basieren auf einem IT-Protokoll-Überwachungsverfahren, die die Besonderheiten der OT-Umgebung nicht berücksichtigen. Im Vergleich zur IT-Umgebung verwendet der OT-Bereich üblicherweise eigene Technologien und keine handelsübliche Software, sondern Software mit jeweils eigenem Datenformat. Dies stellt Versorgungsunternehmen, die ein Protokollverwaltungstool zur Ereigniswarnmeldung und -korrelation verwenden möchten, vor große Herausforderungen. Darüber hinaus sind die erfassten Protokolldaten häufig äußerst kontextabhängig und erfordern somit das Verständnis eines erfahrenen

OT-Mitarbeiters. Dies macht die eingebauten SIEM-Korrelationsregeln für den operativen Betriebsbereich untauglich.

Der für die Automatisierung erforderliche Kontext fehlt häufig

Die effiziente und effektive Durchführung der Protokollüberwachung erfordert Automatisierung. Automatisierung wird durch die Schaffung von Korrelationsregeln erreicht, die eine Vielzahl an Protokolleinträgen auf der Grundlage gemeinsamer Werte abgleicht. Das sind beispielsweise Zeitstempel und Attribute, die den Kontext repräsentieren, in dem das Ergebnis zustande gekommen ist. In der Regel fehlen jedoch die OT-kontextabhängigen Daten oder die Protokolleinträge enthalten proprietäre Meldungen oder Codes, die nur für den Software-Anbieter von Bedeutung sind.

Der Kontext ist entscheidend, wenn es darum geht, Herausforderungen zu meistern

Die Schaffung von Kontext ist der Schlüssel zur Bewältigung der Herausforderungen, mit denen Versorgungsunternehmen konfrontiert werden, wenn es zur Implementierung von Lösungen für das Sicherheitsprotokollmanagement kommt.

Die Anwendung des Kontextes auf erfasste Protokolldaten ermöglicht es Versorgungsunternehmen, eine OT-Umgebung effektiv zu überwachen und Sicherheitszwischenfälle zu entdecken.

Schaffen eines Kontexts mit einer Auditpolitik

Eine Auditrichtlinie sollte ein Eckpfeiler der OT-Protokollmanagementstrategie von Versorgungsunternehmen sein. Sie ist ein wertvolles Mittel um den Kontext für Sicherheitszwischenfälle so zu gestalten, dass diese effektiv behandelt werden können. Eine Auditpolitik dokumentiert die Ereignisse, die von Interesse sind, und fasst sie in Kategorien zusammen, die den Sicherheitskontext beschreiben, in welchem die Zwischenfälle entstanden sind. Diese Kategorien sind üblicherweise an jenen Richtlinien angelehnt, die in den vorgeschriebenen Regulierungsstandards enthalten sind (siehe Abb. 2). Das Vorliegen einer Auditrichtlinie hilft darüber hinaus, das Einhalten der Vorschriften nachzuweisen.

Hinweis aus IEC 62443-3-3 ⇒ <i>Das Kontrollsystem muss die Möglichkeit bieten, sicherheitsrelevante Auditaufzeichnungen für die folgenden Kategorien zu erzeugen: Zugriffskontrolle, Anforderungsfehler, Betriebssystemereignisse, Kontrollsystemereignisse, Backup- und Wiederherstellungsereignisse, Konfigurationsänderungen, potenzielle Aufklärungsaktivitäten und Audit-Protokoll-Ereignisse.</i>	Hinweis aus NERC CIP-007-6 ⇒ <i>Protokoll-Ereignisse auf BES-Cyber-System-Ebene (pro BES-Cyber-System-Fähigkeit) oder auf Cyber-Asset-Ebene (pro Cyber-Asset-Fähigkeit) zur Identifizierung und anschließenden Untersuchung von Cybersicherheitszwischenfällen, die mindestens jede der folgenden Ereignisarten beinhalten: festgestellte erfolgreiche Login-Versuche; festgestellte fehlgeschlagene Zugriffsversuche und fehlgeschlagene Login-Versuche; festgestellter schädlicher Code.</i>
---	--

Abb. 2: Beispiele vorgeschriebener Anforderungen, die bei der Festlegung der Auditpolitik berücksichtigt werden könnten

Integration von Bedrohungsdaten

Als Reaktion auf die immer ausgereifteren Cyberangriffe wurden SIEM-Lösungen weiterentwickelt und bieten nun einen anomaliebasierten Ansatz, der in der Theorie dazu beitragen sollte, bisher unbekannte Bedrohungen zu entdecken. Durch den anomaliebasierten Ansatz erhöht sich jedoch die falsch-positiv-Rate beträchtlich, wodurch das Sicherheitsteam mehr Aspekten nachgehen muss und dadurch die Gefahr größer wird, dass tatsächliche Bedrohungen übersehen werden. Um diese ungültigen Indikatoren proaktiv zu verwerfen und sich auf real vorherrschende Bedrohungen konzentrieren zu können, muss eine SIEM-Lösung Bedrohungsdaten integrieren.

Bedrohungsaufklärung ist der Vorgang eine Analyse aufzusetzen, basierend auf der Identifikation, Erfassung und Anreicherung relevanter Informationen. Im Allgemeinen wird Bedrohungsaufklärung durch die Analyse von Widersachern und deren Methoden generiert.

Es besteht jedoch ein beträchtlicher Mangel an Einblicken in die OT-Bedrohungslandschaft, da herkömmliche Sicherheitsanbieter nicht über die für die Generierung von OT-Bedrohungsinformationen erforderlichen Datenquellen, Vorfallreaktionsdaten und das notwendige Fachwissen verfügen. Künftig können Lösungsanbieter Versorgungsunternehmen bei der Generierung verwertbarer Bedrohungsinformationen durch Bedrohungsbewertungen unterstützen.

Damit Sicherheitsexperten Korrelationsregeln erstellen und damit Kompromissindikatoren festlegen können, müssen die Kontextinformationen der Bedrohungsaufklärung auch in den gesammelten Protokolldaten berücksichtigt werden. Die Erstellung einer Auditrichtlinie stellt sicher, dass Querverweise stattfinden. (siehe Abb. 3).

Ereignis in einer bestimmten Kategorie der Auditpolitik	Bedrohungsdaten
Ein Ereignis in der Kategorie <i>Privilegierte Nutzung</i> für Servicenutzer oder integrierte Konten könnte auf einen möglichen Anstieg von Berechtigungen hindeuten.	Akzeptable Nutzungspolitik für das Zielprodukt.
Eine Vielzahl von Ereignissen in der Kategorie <i>Zugriffskontrolle</i> , die verschiedene Nutzer verzeichnen, die Aktivitäten im selben Verantwortungsbereich ausführen, könnten auf eine mögliche Absprache hindeuten.	Die empfohlene Gestaltung der Kontrolle der Aufgabentrennung für das Zielprodukt.
Ein Ereignis der Kategorie <i>Systemänderungskontrolle</i> , das größere Anwendungsänderung verzeichnet und das Fehlen anderer Ereignisse, die bestätigen, dass der Update-Prozess eingehalten wurde, könnte auf ein unerwartetes Patching des Systems, mit der Absicht, Schwachstellen einzufügen, hindeuten.	Festlegung des Update-Prozesses für die Zielumgebung.
Die Verknüpfung eines Ereignisses der Kategorie <i>System außerhalb der Grenzen</i> , das aufzeichnet, wenn Kommunikationsschwellen überschritten werden, mit einem Ereignis der Kategorie <i>Zugriffskontrolle</i> , das den erfolgreichen Datei-Schreibzugriff in einem gemeinsamen Verzeichnis protokolliert, könnte auf eine mögliche Datenaggregation und auf Exfiltrationsversuche hindeuten.	Festlegung des grundlegenden Systems und der Nutzeraktivitäten des Produkts.

Abb. 3: Beispiele dafür, wo ein möglicher Cyberangriff durch Vergleichen der Kategorien der Auditpolitik im SIEM mit Threat Intelligence aufgezeigt werden kann

Erreichen der IT/OT-Integration im Sicherheitsprotokoll

Um eine OT-Umgebung effektiv zu überwachen und Sicherheitszwischenfälle zu erkennen, ist es notwendig, den Kontext auf die gesammelten Protokolldaten anzuwenden. Als Quelle für diesen Kontext können die Auditpolitik der Organisation sowie die Bedrohungsaufklärung des Software-Anbieters verwendet werden.

Dieser Kontext kann zwar in OT-Protokollverwaltungslösungen von Versorgungsunternehmen integriert werden, sie stehen jedoch vor einem Dilemma, wenn sie versuchen, eine Sicherheitsprotokollfunktion über IT- und OT- bereichsübergreifend einzurichten. Es ist zwar äußerst unwahrscheinlich, dass ein Software-Anbieter Korrelationsregeln unterstützen und liefern kann, die über beide Bereiche hinweg funktionieren, allerdings ist es angesichts der erforderlichen Investitionen unrealistisch, seperate SIEM-Lösungen für die IT- und die OT-Umgebung aufrecht zu erhalten.

Eine Lösung für dieses Dilemma besteht darin, eine integrierte Lösung für die Verwaltung von Sicherheitsprotokollen zu implementieren, um die IT- und die OT-Protokollmanagementstrategie des Versorgungsunternehmens zusammenzuführen. Diese Lösung (siehe Abb. 4) erfüllt die regulatorischen Anforderungen (siehe Abb. 5), und zwar mithilfe der folgenden Funktionen:

- **Extrahieren** – Erfassen von Protokolldaten am Speicherort und Versenden der Daten an eine zentrale Komponente.
- **Normieren** – Transformation von Daten aus verschiedenen Quellen in ein einheitliches Format. Das Format sollte Informationen wie ‚Was ist passiert?‘, ‚Wann ist es passiert?‘, ‚Wo ist es passiert?‘, ‚Wer hat es getan?‘ oder ‚Wie ist es passiert?‘ umfassen.
- **Anreichern** – Hinzufügen von Sicherheitsbeschreibungen (d. h. Auditpolitikkategorien) zu Protokolldaten (z. B. als Attribut), die den Kontext beschreiben, in dem es zu dem Ereignis gekommen ist.
- **Filtern** – Verfolgen eines selektiven Ansatzes, bei dem nur Ereignisse, die von Interesse sind, analysiert werden. Die Filter basieren üblicherweise auf Daten, mit denen die Protokolle angereichert wurden.
- **Übertragen** – Senden der relevanten Protokolldaten auf sicherem Wege an die Ziel-SIEM-Lösung.
- **Bewahren** – Behalten einer redundanten Kopie der Protokolldaten, um im Falle des Systemausfalls oder der Verfälschung durch böswillige Nutzer die Verfügbarkeit und Vollständigkeit sicherzustellen.
- **Visualisieren** – Bereitstellen von Adhoc-Forensik für die OT-Mitarbeiter.

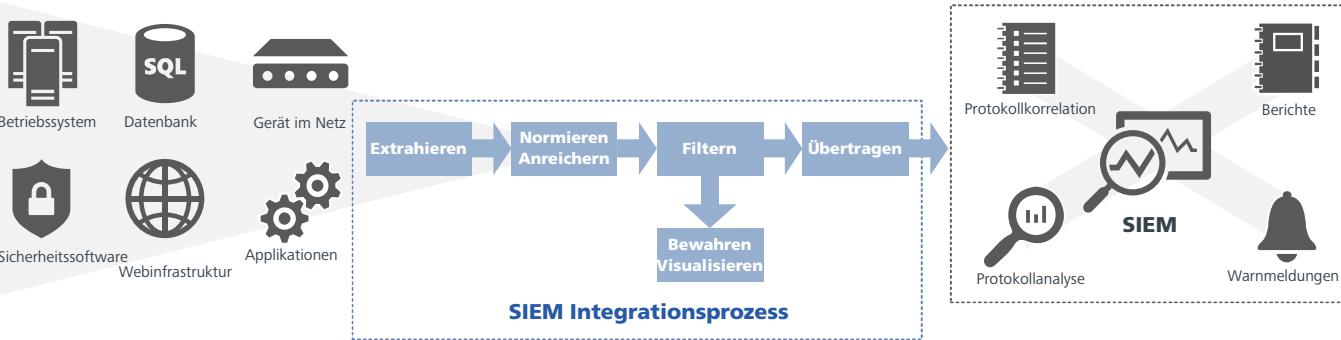


Abb. 4: Integriertes IT/OT-Sicherheits-Log-Management

IT/OT-Integrationsfunktion	Erfüllte Vorschrift
Extrahieren – Erfassen von Protokolldaten am Speicherort und Versenden der Daten an eine zentrale Komponente.	BDEW Whitepaper ⇒ <i>Es muss ein Mechanismus zum automatischen Übertragen der Protokolldaten an die zentrale Komponente verfügbar sein.</i> IEC 62443-3-3 ⇒ <i>Das Kontrollsystem muss die Möglichkeit bieten, Auditereignisse zentral zu verwalten und Auditaufzeichnungen aus einer Vielzahl von Komponenten im gesamten Kontrollsystem in einen systemweiten (logischen oder physischen), zeitkorrelierten Auditpfad zu kompilieren.</i>
Normieren – Umwandeln von Daten aus verschiedenen Quellen in ein durchgängiges Format. Das Format sollte Informationen wie ‚Was ist passiert?‘, ‚Wann ist es passiert?‘, ‚Wo ist es passiert?‘, ‚Wer hat es getan?‘ oder ‚Wie ist es passiert?‘ umfassen.	IEC 62443-3-3 ⇒ <i>Die einzelnen Auditaufzeichnungen müssen den Zeitstempel, die Quelle (ursprüngliches Gerät, ursprünglicher Softwareprozess oder ursprüngliches Konto des menschlichen Nutzers), die Kategorie, den Typ, die Ereignis-ID und das Ergebnis des Ereignisses umfassen.</i> BDEW Whitepaper ⇒ <i>Das System muss Nutzerhandlungen und sicherheitsrelevante Handlungen, Ereignisse und Fehler in einem Auditpfad protokollieren, und zwar unter Verwendung eines Formats, das für die spätere und für die zentrale Analyse geeignet ist.</i>
Anreichern – Hinzufügen von Sicherheitsdeskriptoren (d. h. Auditpolitikkategorien) zu Protokolldaten (z. B. als Attribut), die den Kontext beschreiben, in welchem es zu dem Ereignis gekommen ist.	BDEW Whitepaper ⇒ <i>Sicherheitsereignisse müssen in den Systemprotokollen hervorgehoben werden, um eine einfache und automatische Analyse zu ermöglichen.</i>
Filtern – Verfolgen eines selektiven Ansatzes, bei dem nur Ereignisse, die von Interesse sind, analysiert werden. Die Filter basieren üblicherweise auf Daten, mit denen die Protokolle angereichert wurden.	
Übertragen – Senden der relevanten Protokolldaten sicher an die Ziel-SIEM-Lösung.	IEC 62443-3-3 ⇒ <i>Das Kontrollsystem muss die Möglichkeit bieten, diese Auditaufzeichnungen in Branchenstandardformate zu exportieren, und zwar mittels Analyse durch handelsübliche Protokollanalysetools, beispielsweise SIEM (Security Information and Event Management).</i>
Bewahren – Behalten einer redundanten Kopie von Protokolldaten, um im Falle des Systemausfalls oder der Verfälschung durch böswillige Nutzer die Verfügbarkeit und Vollständigkeit sicherzustellen.	NERC CIP-007-6 ⇒ <i>Sofern dies technisch machbar ist, bewahren Sie entsprechende Ereignisprotokolle der letzten 90 aufeinanderfolgenden Kalendertage auf.</i>
Darstellen – Bereitstellen von Adhoc-Forensik für die OT-Mitarbeiter.	

Abb. 5: Erfüllte Vorschriften mittels integriertem IT/OT-Sicherheitsprotokoll

Zusammenfassung

Die Integration von Informationstechnologie (IT) und Betriebstechnologie (OT), um die Vorteile eines digitalen Netzes zu nutzen, kann für Versorgungsunternehmen eine Herausforderung darstellen. Dies gilt insbesondere für das Sicherheitsprotokoll, da bislang noch keine entsprechenden Tools verfügbar waren, um die Sicherheit in der OT-Umgebung effektiv zu überwachen oder das Protokollmanagement für IT und OT zusammenzubringen.

In der vorliegenden Broschüre wird eine Lösung vorgestellt, die die Lücke zwischen dem IT- und OT-Protokoll der Versorgungsunternehmen schließt. Basierend auf einer Auditrichtlinie bei welcher Bedrohungsinformationen eingebunden werden, wird festgelegt, welche Funktionen erforderlich sind, um diese beiden Strategien erfolgreich zu integrieren. Die Funktionen umfassen den Versand von Daten an eine zentrale Komponente, das Standardisieren des Datenformats, das Anreichern der Daten mit Kontextinformationen, das Herausfiltern irrelevanter Protokolle und das anschließende Senden der relevanten Protokolldaten an das SIEM.

Zu den Vorteilen der Implementierung einer solchen Lösung gehört unter anderem die verbesserte Erfüllung regulatorischer Anforderungen, eine optimierte Sicherheitsüberwachung sowie die effektive Nutzung von Ressourcen.

Bibliografie

1. NIST SP 800-92: Guide to Computer Security Log Management, September 2006, <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf>
2. SANS Whitepaper: Successful SIEM and Log Management Strategies for Audit and Compliance, 4. November 2010, <https://www.sans.org/readingroom/whitepapers/auditing/successful-siem-log-management-strategies-auditcompliance-33528b>
3. Ipswitch Inc., BEST PRACTICES: EVENT LOG MANAGEMENT FOR SECURITY AND COMPLIANCE INITIATIVES, Juli 2010, <https://www.ipswitch.com/resources/bestpractices/log-management-compliance-for-the-healthcare-industry>
4. BALAJI N, Security Information and Event Management (SIEM) – A Detailed Explanation, 31. Mai 2017, <https://gbhackers.com/security-information-and-event-managementsiem-a-detailed-explanation/>
5. Cyber Threat Intelligence <https://dragos.com/Dragos-Insights-into-Building-an-ICS-Security-Operations-Center.pdf>
6. IEC 62443-3-3: System security requirements and security levels
7. NERC CIP-007-6 (Systems Security Management)
8. BDEW Whitepaper

Über den Autor

Ugljesa Novak ist Sicherheitsarchitekt bei OMNETRIC und zertifizierter Fachmann für die Sicherheit von Informationssystemen.

Mit nahezu zehn Jahren Erfahrung im Bereich IT-Sicherheit hat Ugljesa Novak bei vielen Smart-Grid-Projekten Sicherheitskontrollen für Netzkontrollsysteme entworfen und entwickelt.

Seine Erfahrung erstreckt sich über eine Vielzahl von Anbietern, und er hat beispielsweise in Projektteams für Anbieter wie Schneider Electric oder Siemens gearbeitet.

www.omnetric.com

Über OMNETRIC – A Siemens Company

OMNETRIC ermöglicht es Energieversorgern durch die IT-Integration ihrer operativen Prozesse, die Vorteile digitaler Energiesysteme für ihr Geschäft zu nutzen.

Das globale OMNETRIC-Team, bestehend aus Ingenieuren, Informatikern, sowie Sicherheits- und Datenexperten, verfügt über langjährige, branchenspezifische Erfahrung in der Datenanalyse und -verwertung. OMNETRIC hilft seinen Kunden dabei, nachhaltig von Veränderungen im Energiesektor zu profitieren und neue Geschäftsmodelle zu etablieren.

OMNETRIC steht seinen Kunden seit 2014 als innovatives, lösungsorientiertes Technologieunternehmen zur Seite.

Besuchen Sie uns auf www.omnetric.com.

Kontakt

Geschäftliche Anfragen
request@omnetric.com

Marketing und Unternehmenskommunikation
pr@omnetric.com

Stellenangebote
www.omnetric.com/vacancies