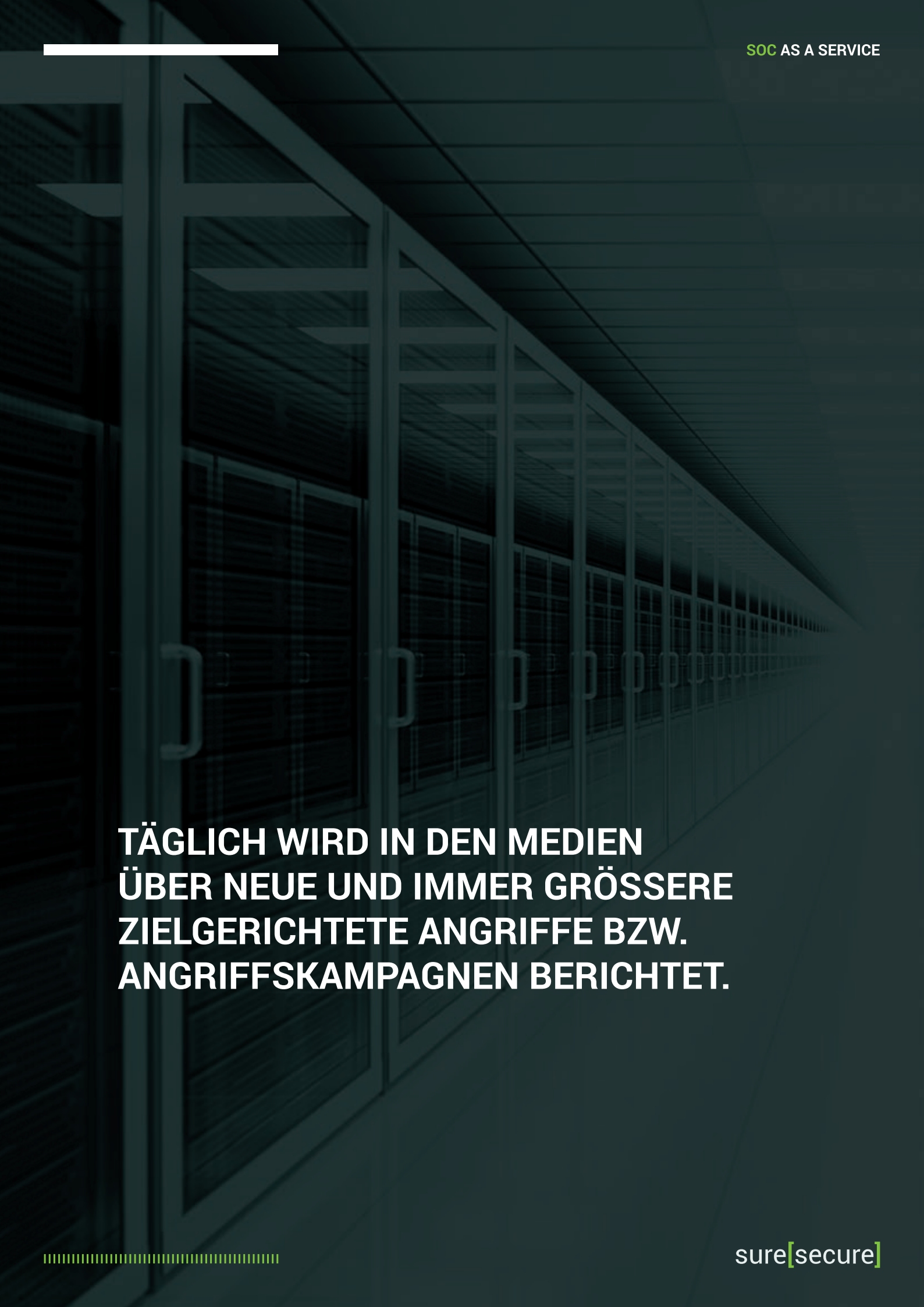
MANAGED SECURITY SERVICES

SOC AS A SERVICE

sure[secure]

00 INHALT



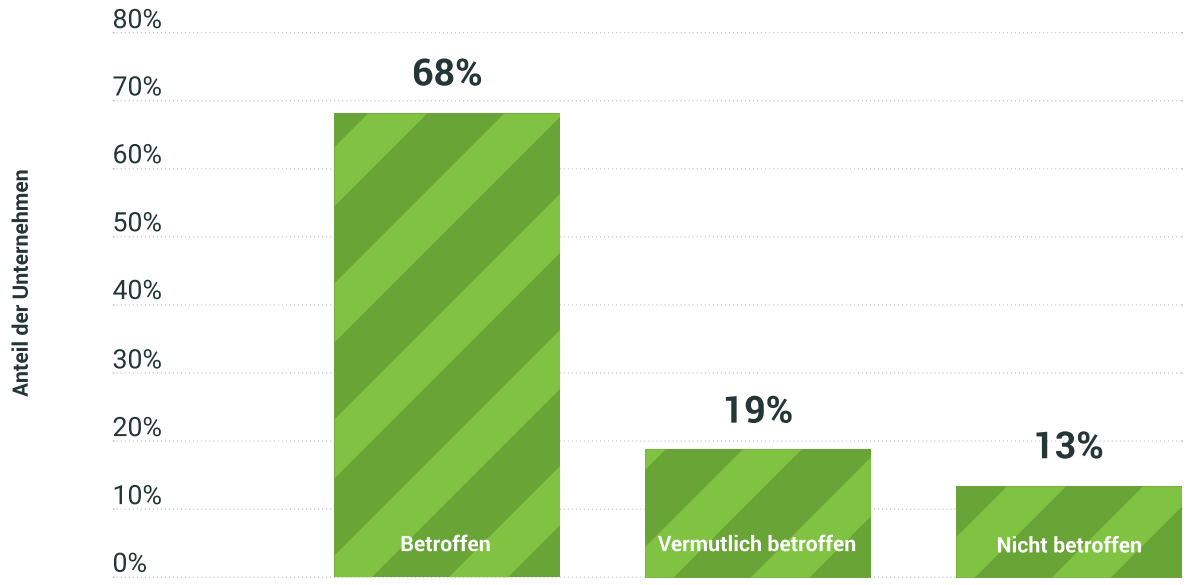
TÄGLICH WIRD IN DEN MEDIEN ÜBER NEUE UND IMMER GRÖSSERE ZIELGERICHTETE ANGRIFFE BZW. ANGRIFFSKAMPAGNEN BERICHTET.

01

SECURITY OPERATION CENTER

Da Cyber-Angriffe immer öfter und in größeren Kampagnen erfolgreich sind, ist der Bedarf für eine übergreifende und zentrale Monitoring Plattform für IT-Security Incidents in Deutschland höher denn je. Viele Unternehmen haben erkannt, dass Sie derzeit keine Möglichkeit besitzen einen Sicherheitsvorfall frühzeitig zu erkennen. Regelmäßig fehlen Informationen, Prozesse und Ressourcen und so ist die Reaktion auf Cyber-Angriffe nicht zielgerichtet und meist viel zu spät.

War Ihr Unternehmen in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen?



Quelle: Bitkom ©Statista 2018
Weitere Informationen: Deutschland; Bitkom Research; 2018; n = 503 Unternehmen mit mind. 20 Mitarbeiter

Vielen Unternehmen ist daher mittlerweile bewusst, dass sich nicht die Frage stellt ob ein Angriff auf Unternehmen erfolgreich sein könnte, sondern nur wann ein erfolgreicher Angriff stattfindet. Daher ist es notwendig bereits frühzeitig in ein Sicherheitsinformationssystem zu investieren. Im Falle eines erfolgreichen Angriffs können so die relevanten Informationen blitzschnell korreliert werden und zielgerichtete automatisierte Gegenmaßnahmen eingeleitet werden.

02 SURESECURE KONZEPT

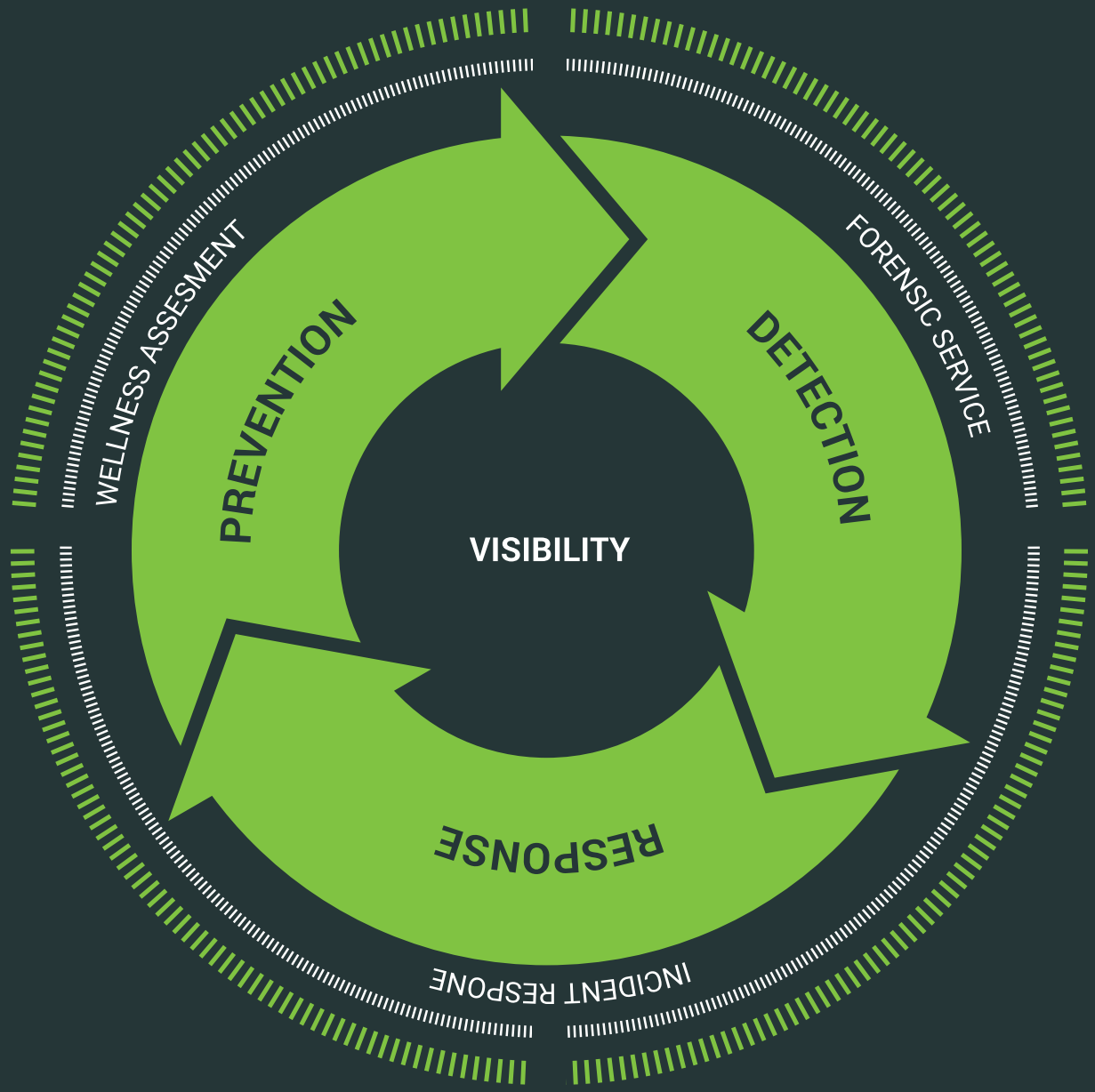
Obwohl vielen Unternehmen bewusst ist, dass der Einsatz einer SIEM Lösung unbedingt notwendig ist, scheitert das Projekt jedoch oft bereits vor der Konzeptionierung. In der Regel liegt das an den folgenden Gründen:

- **Es existieren unzählige Angriffs-Modelle und Use Cases**
- **Die notwendigen Log-Quellen können nicht identifiziert werden**
- **Das Log-Volumen wird oft falsch eingeschätzt**
- **Kein geschultes Personal für Betrieb und Wartung**
- **Die Einführung eines SIEMs bedarf eines zu langen Zeitraums**

[s]

Für all diese Probleme hat die suresecure Lösungen entwickelt und ermöglicht somit den kosteneffizienten Einsatz eines SOC as a Service ohne Kompromisse in der IT-Sicherheit. Bereits bei dem konzeptionellen Entwurf des Services wurde unter Berücksichtigung einer optimalen Skalierung auf vorhandene Industriestandards gesetzt.

Die bereitgestellten Erkennungen orientieren sich an dem MITRE ATT&CK Framework. Dieses Framework beschreibt gängige Techniken, welche durch Angreifer genutzt werden, und teilt diese in abstrakte Kategorien. Die Ausnutzung der entsprechenden Technik mag im konkreten Angriffsfall variieren, die grundlegende Technik bleibt aber identisch. Daher kann mit einer Erkennung eine Vielzahl an Angriffsvarianten erkannt werden.
Das ATT&CK Framework beschreibt diese Techniken auch in Form von IOCs. Hierbei wird wiederrum auf die Industriestandards STIX und TAXII gesetzt. Der Kreis schließt sich, wenn dann durch die Verteilung der IOCs im Netzwerk Angriffe automatisiert aktiv blockiert werden.


PREVENTION
DETECTION
RESPONSE
VISIBILITY
WELLNESS ASSESMENT
FORENSIC SERVICE
INCIDENT RESPONSE

03 MODULE

Das SOC as a Service Angebot der suresecure ist modular aufgebaut und ermöglicht es den Unternehmen, aus einem umfangreichen Portfolio genau die Use-Cases umzusetzen, welche benötigt werden. Somit ist es möglich in einem kleinen Umfang zu starten und das IT-Sicherheitsniveau immer weiter auszubauen. Thematisch gliedert sich das SOC in 5 Module auf.

- Network Monitoring
- Endpoint Monitoring
- Authentication Monitoring
- Vulnerability Scanning
- Automated Response

04 NETWORK MONITORING

Die Netzwerkkommunikation basiert noch heute größtenteils auf veralteten und unsicheren Protokollen. Daher ist es besonders wichtig diese Protokolle auf Anomalien zu überprüfen. Der Einsatz von Perimeter Firewalls wird heutzutage in Unternehmensnetzwerken nicht mehr diskutiert. Diese alleine bieten jedoch keinen ausreichenden Schutz für das gesamte Netzwerk, sobald der Angreifer sich einmal Zugriff auf die Umgebung verschafft hat, steht die Firewall außen vor.
Sei es durch das verschicken einer Malware über SMTP, der Ausnutzung von DNS zur Steuerung dieser oder aber das Ausführen von Schadcode über DHCP. Über das Netzwerk gelingt es dem Angreifer in der IT-Umgebung der Unternehmen Fuß zu fassen, sich auszubreiten und gezielt Aktionen durchzuführen.
Das SOC der suresecure ist in der Lage Anomalien im Unternehmensnetzwerk frühzeitig zu entdecken und die Verbreitung in Ihrer Systemumgebung einzudämmen.

05 ENDPOINT MONITORING

In nahezu allen Sicherheitsvorfällen ist der Endpoint für den Angreifer der Eintrittspunkt. Daher ist es unerlässlich in einem SOC umfassende forensische Logs auf dem Endpoint zu sammeln. Diese sollten sich nicht nur auf die Informationen des Anti-Virus Produktes beschränken, sondern alle sicherheitsrelevanten Ereignisse unabhängig von den Erkennungen des Anti-Virus Herstellers.

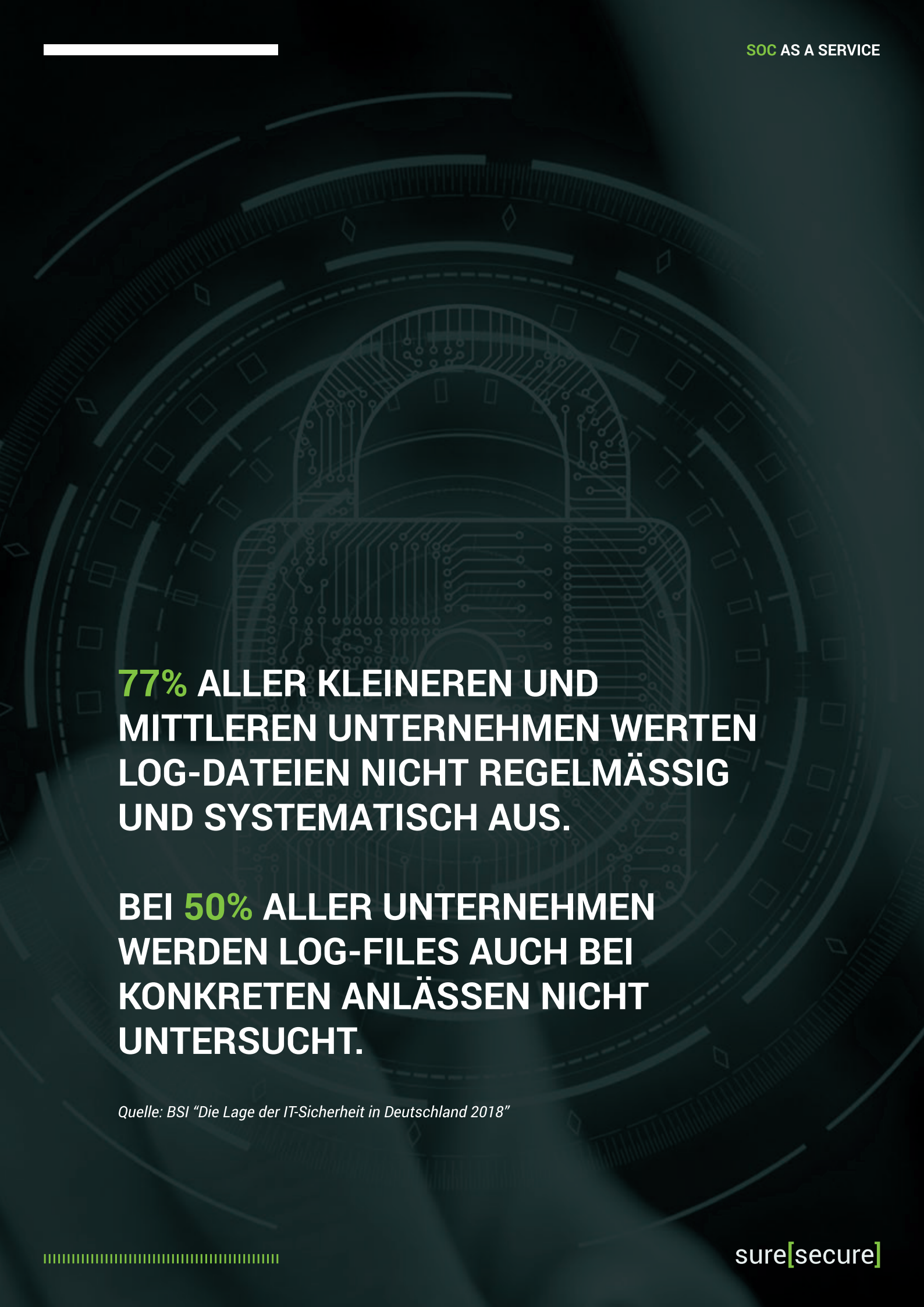
Als Datenbasis wird hier unter anderem die Anpassung von Registry-Werten, das starten von verdächtigen Prozessen oder auch das Ausführen von codierten Powershell Befehlen erhoben. Dies ist nur ein Bruchteil von Informationen, die genutzt werden können, um einen Angriff auf das System zu identifizieren.

06 AUTHENTICATION MONITORING

Für den Angreifer gibt es viele Möglichkeiten sich unautorisiert Zugriff auf Systeme zu beschaffen.
Sei es durch die Übermittlung eines Trojaners, das Ausnutzen einer Software-schwachstelle oder der Durchführung einer Brute Force-Attacke.
Das Authentication Monitoring Modul erkennt gängige Angriffsmethoden, mit denen Angreifer sich privilegierte Zugriffe verschaffen. Weiterhin ist es möglich, das Anmeldeverhalten der Benutzer zu analysieren und bei Anomalien eine Meldung zu erzeugen.
Berücksichtigt werden hier diverse Standard-Protokolle wie beispielsweise Kerberos, Radius oder SAML. Im Falle einer Infektion oder der Verbreitung im internen Netz behalten Sie dadurch den Überblick und können gezielte Aktionen durchführen.

07 VULNERABILITY SCANNING

Das Vulnerability Scanning ist ein essentieller Baustein bei der Bewertung des Informationssicherheits-Risikos. Durch dieses Modul werden Schwachstellen auf Systemen festgestellt und auf Basis dessen eine Risikobewertung der Assets durchgeführt.
Diese Informationen sind Bestandteil eines jeden Patch-Management Prozesses. Sollte ein Intrusion Prevention System zum Einsatz kommen, ist es möglich die gefundenen Schwachstellen dem System zu übermitteln, damit automatisiert Schutzmaßnahmen umgesetzt werden können die einen sicheren Betrieb des Systems weiterhin ermöglichen.



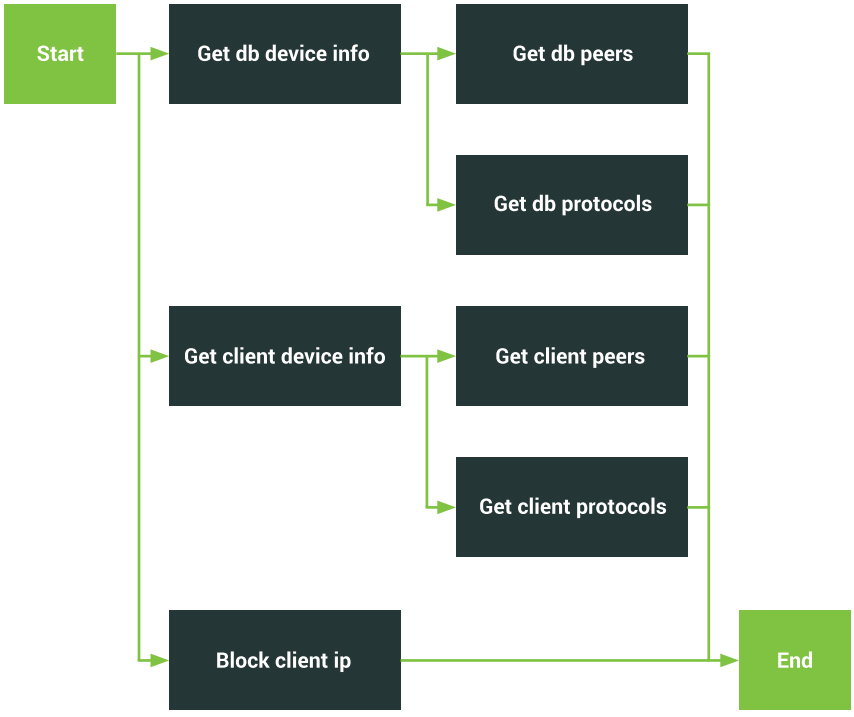
77% ALLER KLEINEREN UND MITTLEREN UNTERNEHMEN WERTEN LOG-DATEIEN NICHT REGELMÄSSIG UND SYSTEMATISCH AUS.

BEI **50%** ALLER UNTERNEHMEN WERDEN LOG-FILES AUCH BEI KONKRETEN ANLÄSSEN NICHT UNTERSUCHT.

Quelle: BSI "Die Lage der IT-Sicherheit in Deutschland 2018"

08 AUTOMATED RESPONSE

Das SOC as Service ist in der Lage, nahezu in Echtzeit und automatisiert auf Alarme zu reagieren. Unzählige Szenarien sind hier denkbar, wie z.B. das Blockieren von IP-Adressen auf der Firewall, die Isolation von Clients oder die Deaktivierung eines Netzwerk-Ports auf dem Switch. Diese Aktionen werden über die mehr als 1.200 APIs der Hersteller umgesetzt, welche durch das SOC der suresecure unterstützt werden.
Selbstverständlich geschieht dies immer unter Berücksichtigung mehrerer Faktoren und der Kritikalität des zu blockierenden Objekts. Dies soll verhindern, dass bei einem False Positive plötzlich die Produktion oder andere Business-kritische Systeme gestört werden.
Grundlage für diese automatisierten Reaktionen bilden hier sogenannte Security Playbooks. Diese beschreiben standartisierte Vorgehensweisen im Umgang mit definierten Sicherheitsvorfällen. Sollte beispielsweise ein Verschlüsselugnstrojaner im Netzwerk aktiv sein, so kann automatisch der Kontakt zum Angreifer über die Firewall geblockt und der User, mit dem die Verschlüsselung durchgeführt wird, deaktiviert werden.



09 LOG-VOLUMEN

In der Konzeptionierungsphase ist es von essentieller Bedeutung, alle relevanten Log-Quellen zu identifzieren, die Schnittstellen zu definieren und das mögliche Volumen zu schätzen. Bei den Schnittstellen gibt es eine Vielzahl von Möglichkeiten. Diese müssen pro System dediziert geprüft werden.
Die suresecure bietet hier einen erheblichen Mehrwert: Zum einen durch die Auswahl der am besten geeigneten Schnittstellen bezogen auf das Quell-System, zum anderen aber auch durch die Reduzierung und korrekte Einschätzung des Log Volumens.
Durch effiziente Filtertechniken werden nur die sicherheitsrelevanten Logs verarbeitet. Dadurch wird die Bandbreite geschont, die Menge der irrelevanten Meldungen minimiert, die Effizienz gesteigert - und das bei einer Senkung der Kosten.

10 BETRIEB UND WARTUNG

Eine SOC Plattform selbst zu betreiben ist für viele Unternehmen unerschwinglich. Anders als bei dem Betrieb klassischer Lösungen, wie beispielsweise Virenscannern, wird dediziertes Security-Personal benötigt, welches sich regelmäßig mit neuen Angriffsmustern auseinandersetzt und Erkennungsmechanismen analysiert, die Plattform auf dem neusten Stand hält, Anpassungen und Entwicklungen einpflegt und die Konfiguration fortlaufend anpasst.
Ein großer Anteil bei den Wartungstätigkeiten fällt bei der Entwicklung neuer Erkennungsmechanismen an, angepasst auf die dynamische Bedrohungslage. Insbesondere hier besteht die Gefahr, dass bei Ausbleiben der Wartung bereits nach einigen Monaten die Effizienz sinkt.
Die Analysten der suresecure führen genau diese Tätigkeiten täglich aus und werden fortlaufend in der Analyse und Beseitigung von Sicherheitsvorfällen sowie dem Betrieb der SOC Plattform geschult. Die Arbeit der Security Analysten wird ebenfalls durch das Hinzuziehen von Threat Intelligence Quellen unterstützt. Daher wird die Rate von False Positives so gering wie möglich gehalten. Bei der Bewertung von Sicherheitsvorfällen werden stets mehrere Faktoren berücksichtigt.

LEGEN SIE SELBST DEN UMFANG UNSERER MANAGED SECURITY FÜR IHR UNTERNEHMEN FEST.

10x5

Servicebereitschaft
MO - FR
07:00 - 17:00 Uhr

14x5

Servicebereitschaft
MO - FR
07:00 - 21:00 Uhr

24x7

Servicebereitschaft
Nonstop
24h

11

EINFÜHRUNG IN DIE SOC PLATTFORM

Der modulare Aufbau der SOC Plattform ermöglicht es, den Umfang granular fest zu legen. Use-Cases sind schnell implementiert und werden regelmäßig getestet und erprobt. Einzig kleinere Anpassungen auf die individuellen Unternehmen müssen vorgenommen werden.

Durch die konzeptionelle Vorarbeit und die technische Erfahrung der suresecure ist es möglich, die Einführungszeit eines SOC von mehreren Monaten auf einige Tage zu reduzieren. Lassen Sie sich nicht weiter von der vermeintlichen Komplexität eines Security Operation Centers abschrecken und gehen Sie den ersten Schritt in Richtung SOC as a Service.

suresecure GmbH
Hausbroicher Str. 296D
47877 Willich

Telefon +49 (0) 2156 974 90 60
Telefax +49 (0) 2156 975 49 78

info@suresecure.de
www.suresecure.de

sure[secure]