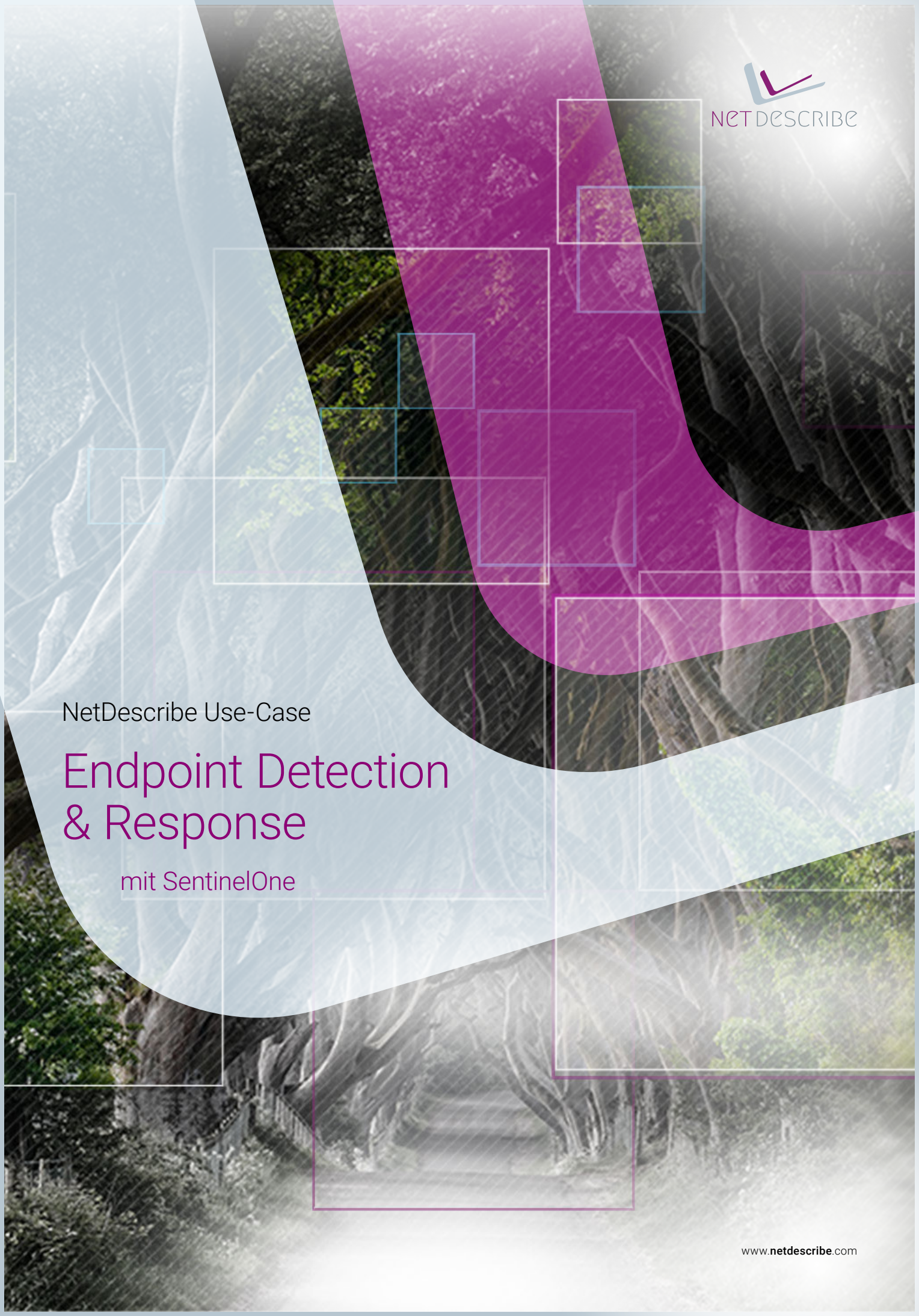


NetDescribe Use-Case

Endpoint Detection & Response

mit SentinelOne

www.netdescribe.com

1. Die Ausgangssituation

Endpoint Security im Wandel

Seit Jahrzehnten beschäftigen sich IT-Spezialisten mit dem Thema Endpoint Security.
Im Normalfall wird die Signatur eines neuen Schadcode von den meisten Antivirenprogrammen erkannt. Entsprechende Regeln werden von den jeweiligen Herstellern eingespielt, um so die Kunden vor Malware zu schützen. In diesem Szenario sind jedoch die IT-Teams die permanent Gejagten. Sie müssen die neuen Methoden der Angreifer erkennen, um sich vor ihnen zu schützen - rund um die Uhr.

Anomalieerkennung mit Hilfe von K.I. und Machine Learning (ML)

Regeln und Signaturen sind wichtig und schützen vor den bekannten Angriffen. Aber was ist mit den Schadprogrammen, die noch niemand kennt - sogenannte Zero-Days*?
Moderne Endpoint Security Tools können zusätzlich zu den hinterlegten Regeln und Signaturen auch das Verhalten von jedem Gerät und User “lernen” und so auf Anomalien reagieren. Diese verhaltensbasierte KI nennt sich EDR/XDR (Endpoint Detection and Response) in Echtzeit.

***Definition: Zero-Day-Exploit** (Definition gemäß BSI)
Die Ausnutzung einer Schwachstelle, die nur dem Entdecker bekannt ist, charakterisiert man mit dem Begriff Zero-Day-Exploit. Die Öffentlichkeit und insbesondere der Hersteller des betroffenen Produkts erlangen in der Regel erst dann Kenntnis von der Schwachstelle, wenn Angriffe entdeckt werden, die auf dieser Schwachstelle basieren. Der Begriff Zero-Day leitet sich also davon ab, dass ein entsprechender Exploit bereits vor dem ersten Tag der Kenntnis der Schwachstelle durch den Hersteller existierte – also an einem fiktiven „Tag Null“. Der Hersteller hat somit keine Zeit, die Nutzer vor den ersten Angriffen zu schützen.

2. Der Use-Case

Die Anforderung an NetDescribe

Unser Kunde aus der Automobilzuliefererbranche stellte an NetDescribe die Anforderung, ein Legacy Antiviren-Programm abzulösen und ein 24/7 Monitoring zu gewährleisten.

Die Bedingungen an das neue System waren folgende:

- State of the Art Lösung
- Erkennung von Regeln und Signaturen
- Überwachung von verhaltensbasierten Anomalien
- Managed Service mit automatisierten Reaktionsmaßnahmen, um die Alarme für den Kunden zu filtern und zu verringern

Die Performance Lösung von NetDescribe - SentinelOne

Nach einer Analyse des Ist-Zustands und einer Beurteilung der gewünschten Anforderungen entschied man sich gemeinsam mit dem Kunden für SentinelOne.
Diese Technologie ermöglicht es Sicherheitsteams nicht nur, sich auf die wichtigsten Warnmeldungen zu konzentrieren, sondern übernimmt durch verhaltensbasierte KI Aufgaben, die bisher ausschließlich von Menschen erledigt werden konnten. Alle Aktivitäten auf einem Gerät werden verfolgt sowie kontextualisiert und schädliche Handlungen in Echtzeit identifiziert. Erforderliche Reaktionen laufen automatisch ab.

Was ist SentinelOne?

SentinelOne ist eine KI-gestützte Endpoint Detection and Response (EDR)-Lösung, die eine einheitliche Analyse von Daten von verschiedenen Endgeräten wie Macs, PCs, Linux-Systemen, IoT-Geräten und Cloud-Workloads ermöglicht. SentinelOne ist für die Erkennung von Sicherheitsbedrohungen, Schwachstellenmanagement und Schutz von Endgeräten konzipiert.
In der heutigen weltweit angespannten Cyber-Bedrohungslage ist ein zuverlässiges Sicherheitskonzept für Unternehmen jeder Größe unerlässlich. Da Angreifer auf Daten auf Servern, in der Cloud oder auf Endgeräten von Mitarbeitern zugreifen können, benötigen Unternehmen vernetzte Systeme für einen zuverlässigen Schutz.

Durch die Integration aller Komponenten bietet SentinelOne eine umfassende Sicht auf die Vorgänge in jeder IT-Infrastruktur. Es sammelt, normalisiert und korreliert Daten von Benutzergeräten, Netzwerken, Cloud-Workloads und Firewalls, um automatisierte Reaktionen zu ermöglichen und IT- und Sicherheitsteams einen umfassenden Überblick zu verschaffen.

Vorteile von SentinelOne als Endpoint Detection and Response (EDR) System:

- Erkennung von Bedrohungen: SentinelOne ermöglicht eine frühzeitige Erkennung von Sicherheitsbedrohungen, indem es Netzwerk-, Benutzer- und Endpunktaktivitäten in Echtzeit überwacht.
- Reaktionsfähigkeit: SentinelOne kann schnell und automatisch auf Sicherheitsbedrohungen reagieren, indem es Bedrohungen isoliert, die Systeme bereinigt oder Benutzerkonten deaktiviert.
- Erweiterte Analysefunktionen: SentinelOne bietet erweiterte Analysefunktionen, um Bedrohungen zu untersuchen und den Ursprung und die Auswirkungen der Bedrohung auf die IT-Infrastruktur zu verstehen.
- Zentralisierte Verwaltung: SentinelOne ermöglicht eine zentralisierte Verwaltung von Sicherheitsrichtlinien, -vorgängen und -ereignissen über eine einheitliche Plattform, was die Betriebseffizienz verbessert.
- Unterstützung bei der Compliance: SentinelOne kann dazu beitragen, Compliance-Anforderungen zu erfüllen, indem es eine detaillierte Protokollierung von Sicherheitsereignissen bietet und hilft, Schwachstellen in der IT-Infrastruktur zu identifizieren und zu beheben.

Zusammenfassend bietet SentinelOne eine effektive Möglichkeit, Sicherheitsbedrohungen zu erkennen, zu analysieren und darauf zu reagieren, wodurch die Gesamtsicherheit und die Compliance von IT-Infrastrukturen verbessert wird.

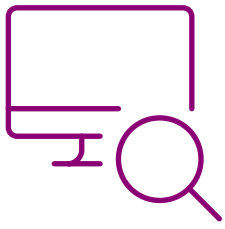
24/7 Managed Detection and Response von SentinelOne

Mit Vigilance Respond werden alle identifizierten Bedrohungen, die Ihr Netzwerk und Ihr Unternehmen gefährden, von Security-Experten untersucht, behoben und dokumentiert, damit Sie Zeit fürs Wesentliche haben.

Was bietet der 24/7 Managed Detection and Response Service von SentinelOne?

- **Rund-um-die-Uhr-Abdeckung (follow the sun)**
  SentinelOne Analysten überwachen Ihre Umgebung täglich rund um die Uhr auf Veränderungen und reagieren im Ernstfall – unabhängig von Ihrem Standort.
- **Kürzere MTTD (mean time to detect) und MTTR (mean time to respond)**
  Durchschnittlich benötigt SentinelOne 18 Minuten, um Vorfälle nicht nur zu entdecken, sondern diese direkt zu beheben. Dies macht Vigilance zum branchenweit schnellsten Managed Detection and Response Service.
- **Weniger Warnungen, mehr Kontext**
  SentinelOne fügt durch die Storyline™-Technologie manuell erzeugten Kontext hinzu, sodass Sie bei der Bündelung, Korrelation und Kontextualisierung von Warnungen noch mehr Zeit sparen.
- **Sicherheit mit Augenmaß**
  Als Erweiterung Ihres Teams triagieren und priorisieren unsere Analysten Ereignisse basierend auf den individuellen Anforderungen Ihres Programms.
- **Dokumentation und Berichte**
  Alle in Ihrer Umgebung identifizierten Bedrohungen werden geprüft, dokumentiert und in die regelmäßig erstellten Berichte aufgenommen.
- **Entlastung Ihrer limitierten IT-Ressourcen**
  Durch die Auslagerung der täglichen Abläufe und Bedrohungssuche an MDR-Experten kann sich Ihr Team auf neue Dinge konzentrieren.

Suchen Sie nach einem Sicherheitstool für Endgeräte, das aktiv Anomalien von Geräten und Usern aufspürt, selbstständig darauf reagiert und kontextbezogene Warnungen für die gesamte Angriffskette liefern kann.



3. Fazit

Mit dem SentinelOne Service Vigilance Respond werden die täglichen Abläufe und die Bedrohungssuche an die SentinelOne MDR (Managed Detection and Response) Experten ausgelagert. Das heißt für Ihr SOC Team mehr Zeit und Ressourcen für Ihre Sicherheitsstrategie.