Barracuda Managed XDR

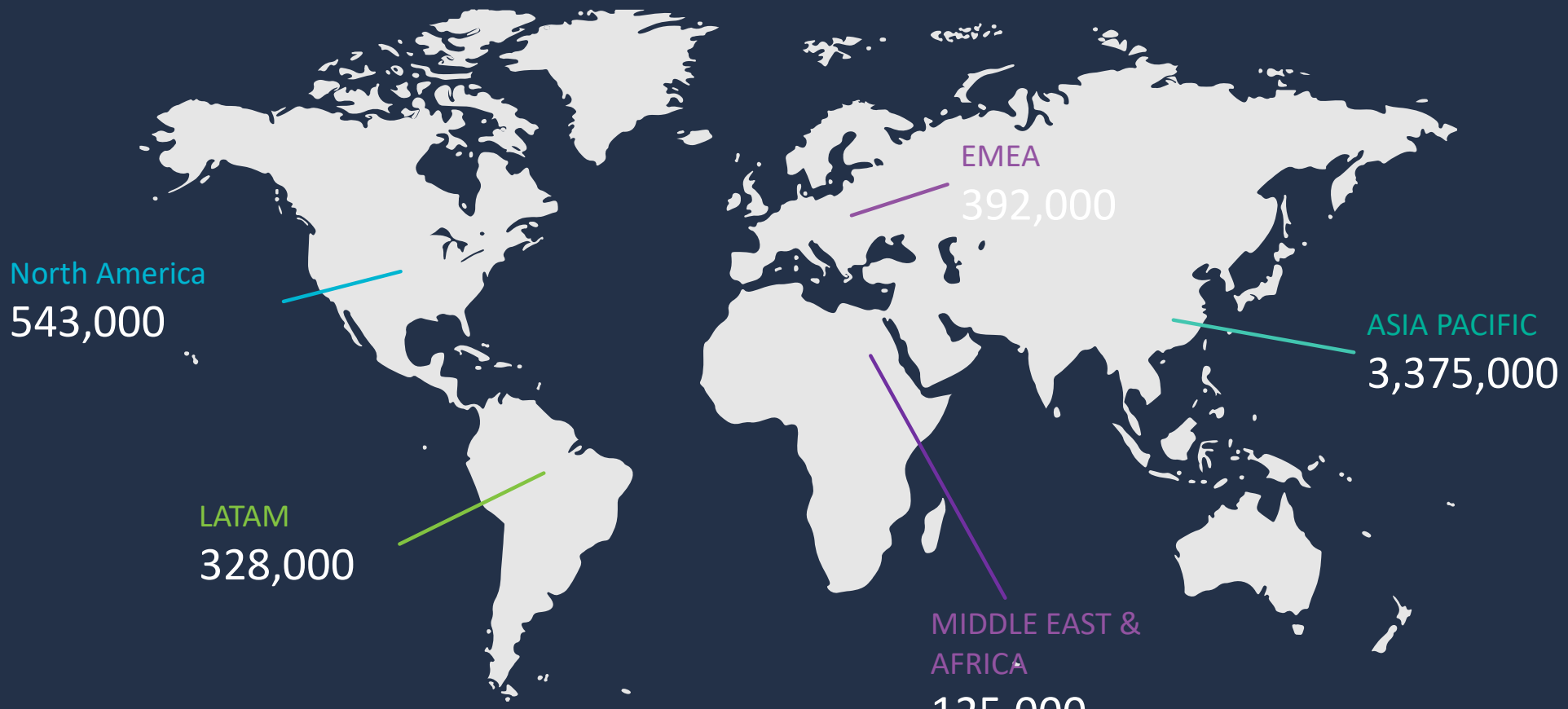
TD SYNNEX 22.05.25

Agenda

1. EDR, XDR, SOC, SIEM – Was zum...!?
2. Wie funktioniert Barracuda XDR?
3. SOC Service
4. NIS2 Checkliste

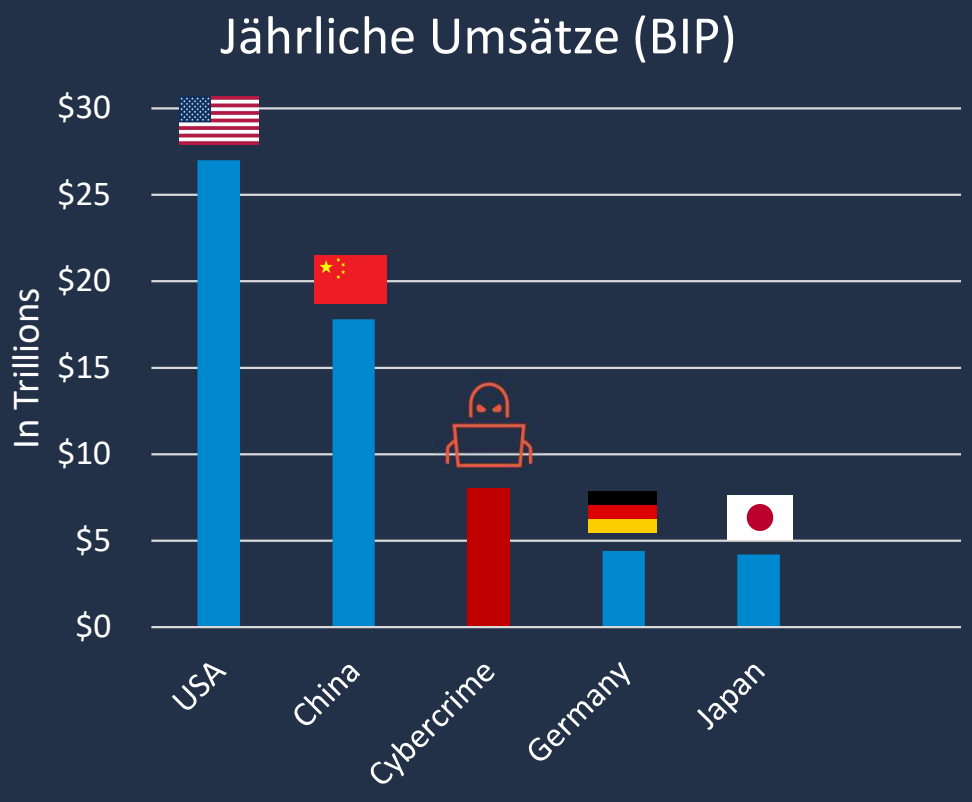
Die Hürden in der Cybersicherheit

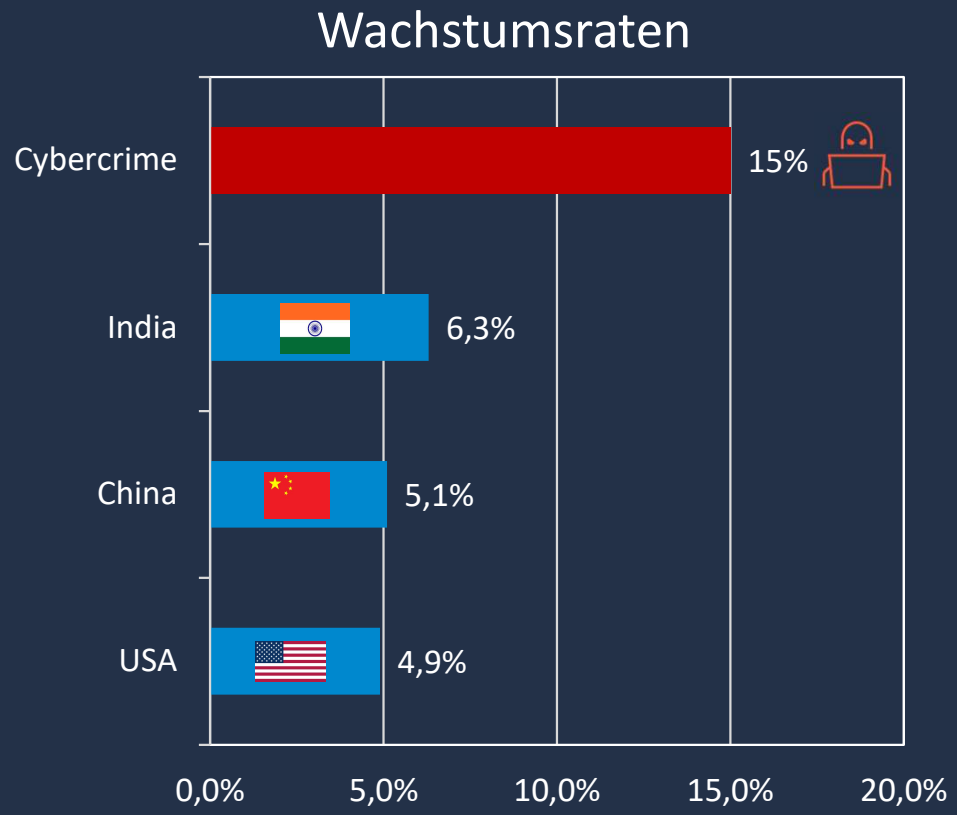
Sicherheitsexperten weltweit gesucht



Source: (ISC)² Cybersecurity Workforce Study, 2024

Cybercrime: Eine Industrie für sich





Boardroom Cybersecurity Report, Cybersecurity Ventures

Von EDR zu XDR

Barracuda XDR - Integrationen

Herausforderungen für Unternehmen

Wenig und teure IT-Security Fachleute

Langsame Erkennung und Reaktion resultiert in längere *dwell time*

Zu viele Dashboards und Insellösungen

Übermäßige Menge an Alarmen und false positives

Gesetzliche Vorgaben und Compliance Richtlinien

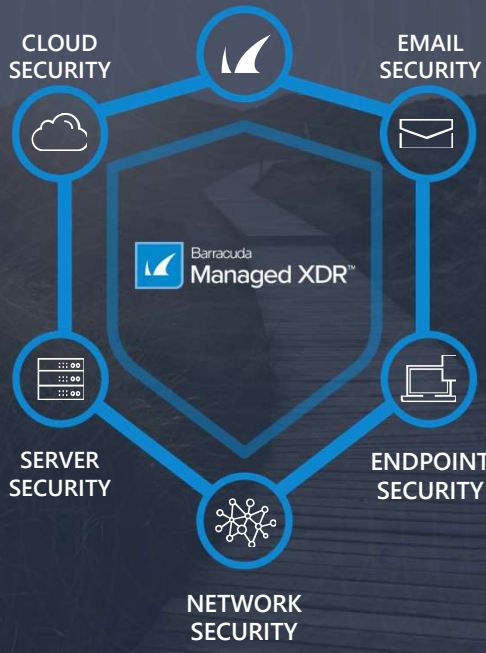
Barracuda Managed XDR

24/7/365 SOC

Eine 24/7/365 SOC-Abdeckung ist entscheidend, um eine kontinuierliche Erkennung von Bedrohungen, eine schnelle Reaktion und eine Minimierung des Risikos durch ausgeklügelte Angriffe, die jederzeit auftreten können, zu gewährleisten.

Zentralisierung

Zentralisierte Sicherheitsdaten in einem verwalteten SIEM bieten umfassende Transparenz, eine schnellere Erkennung von Bedrohungen und eine schnellere Reaktion auf Vorfälle durch integrierte Echtzeitanalysen über alle Sicherheitsebenen hinweg.



Automation & AI

Automatisierung und KI in einer XDR-Lösung sind entscheidend für die schnelle Identifizierung und Neutralisierung von Bedrohungen in Echtzeit, die Verkürzung der Verweildauer und die Minimierung potenzieller Schäden in der gesamten Sicherheitsumgebung.

Proactive Threat Hunting

Proaktive Threathunting identifiziert und entschärft potenzielle Cyber-Bedrohungen, bevor sie Schaden anrichten können. Dieser proaktive Ansatz ermöglicht es Unternehmen, den sich entwickelnden Bedrohungen immer einen Schritt voraus zu sein, und sorgt für einen zuverlässigen Schutz und ein sicheres Gefühl.

Barracuda XDR

Security Event Workflow

Monitored & Gewartet von unseren **24/7/365 Global Security Operations Center**

Event: Jede einzelne von einem Computer durchgeführte Aktion, die protokolliert oder aufgezeichnet wird

Alarm: Aktivitäten, die mit mehreren Ereignissen korrelieren und ein Risiko darstellen.

Alert: Ein untersuchter Alarm, bei dem der Kunde über ein potenzielles Risiko informiert wird.

XDR Network Security

XDR Network Security

Barracuda XDR Network Security integriert ein Intrusion Detection System (IDS) mit Sicherheitsprotokollen von verschiedenen Netzwerkgeräten und -diensten und bietet so einen umfassenden Überblick über Ihr gesamtes Netzwerk und ermöglicht eine schnellere Erkennung von Anomalien und bösartigen Aktivitäten.

Umfassende Sichtbarkeit

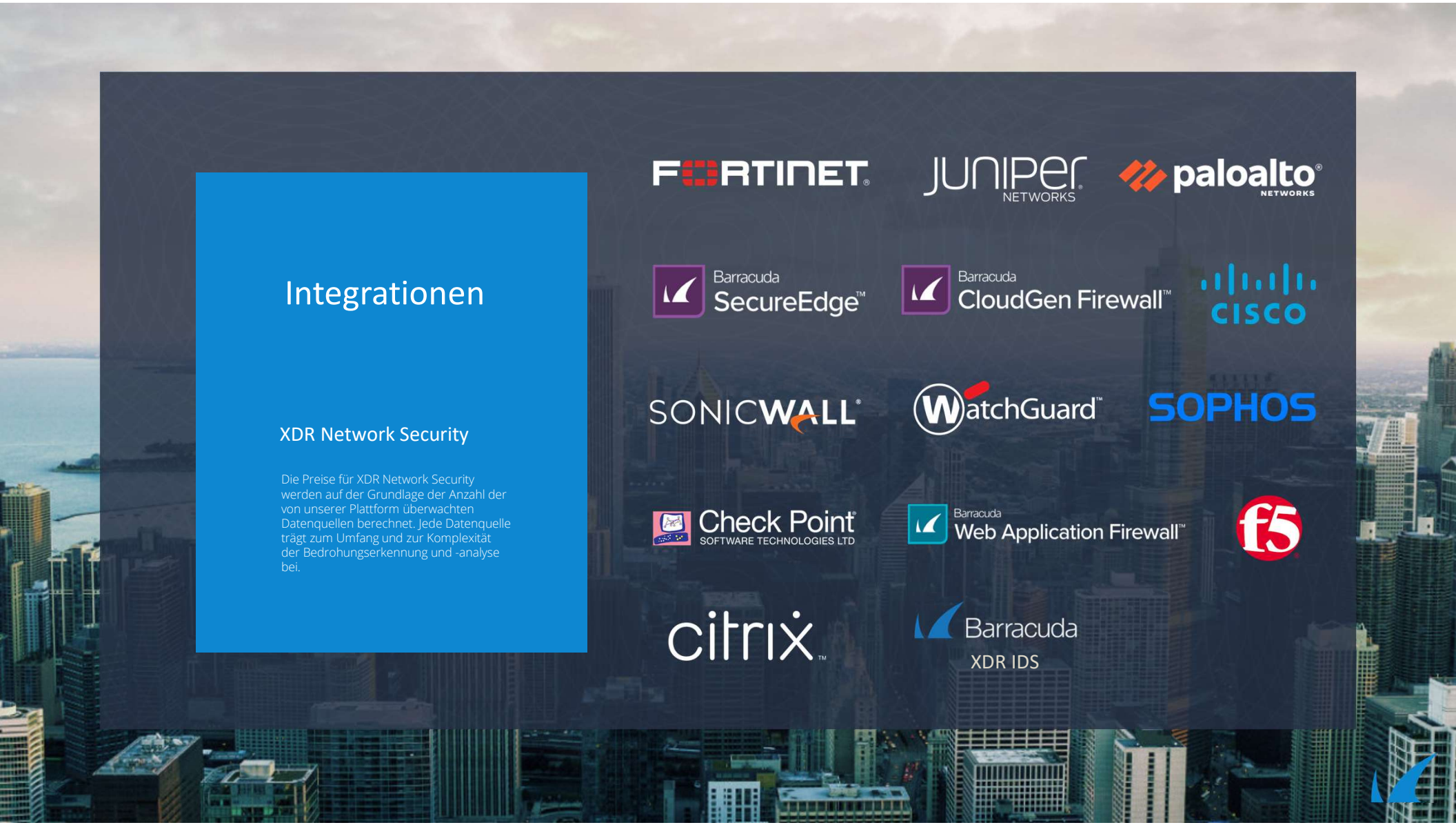
Barracuda XDR Network Security bietet einen umfassenden Einblick in physische Netzwerke und nutzt Daten von unseren IDS, Firewalls und anderen Netzwerkgeräten, um Bedrohungen zu erkennen.

Automated Threat Response

Integrierte SOAR-Funktionen optimieren die Reaktion auf Bedrohungen und blockieren automatisch bösartige IP-Adressen auf der Grundlage von Echtzeitanalysen und vordefinierten Runbooks.

Enhanced Threat Intel

Barracuda Managed XDR nutzt aktuelle Bedrohungsdaten und maschinelles Lernen, um aufkommende Netzwerkbedrohungen zu erkennen und zu blockieren, Fehlalarme zu reduzieren und die Sicherheitseffizienz zu erhöhen.


Integrationen
XDR Network Security
Die Preise für XDR Network Security werden auf der Grundlage der Anzahl der von unserer Plattform überwachten Datenquellen berechnet. Jede Datenquelle trägt zum Umfang und zur Komplexität der Bedrohungserkennung und -analyse bei.
FORTINET
JUNIPER NETWORKS
paloalto NETWORKS
Barracuda SecureEdge™
Barracuda CloudGen Firewall™
CISCO
SONICWALL
WatchGuard™
SOPHOS
Check Point SOFTWARE TECHNOLOGIES LTD
Barracuda Web Application Firewall™
f5
citrix
Barracuda XDR IDS

XDR Endpoint Security

XDR Endpoint Security

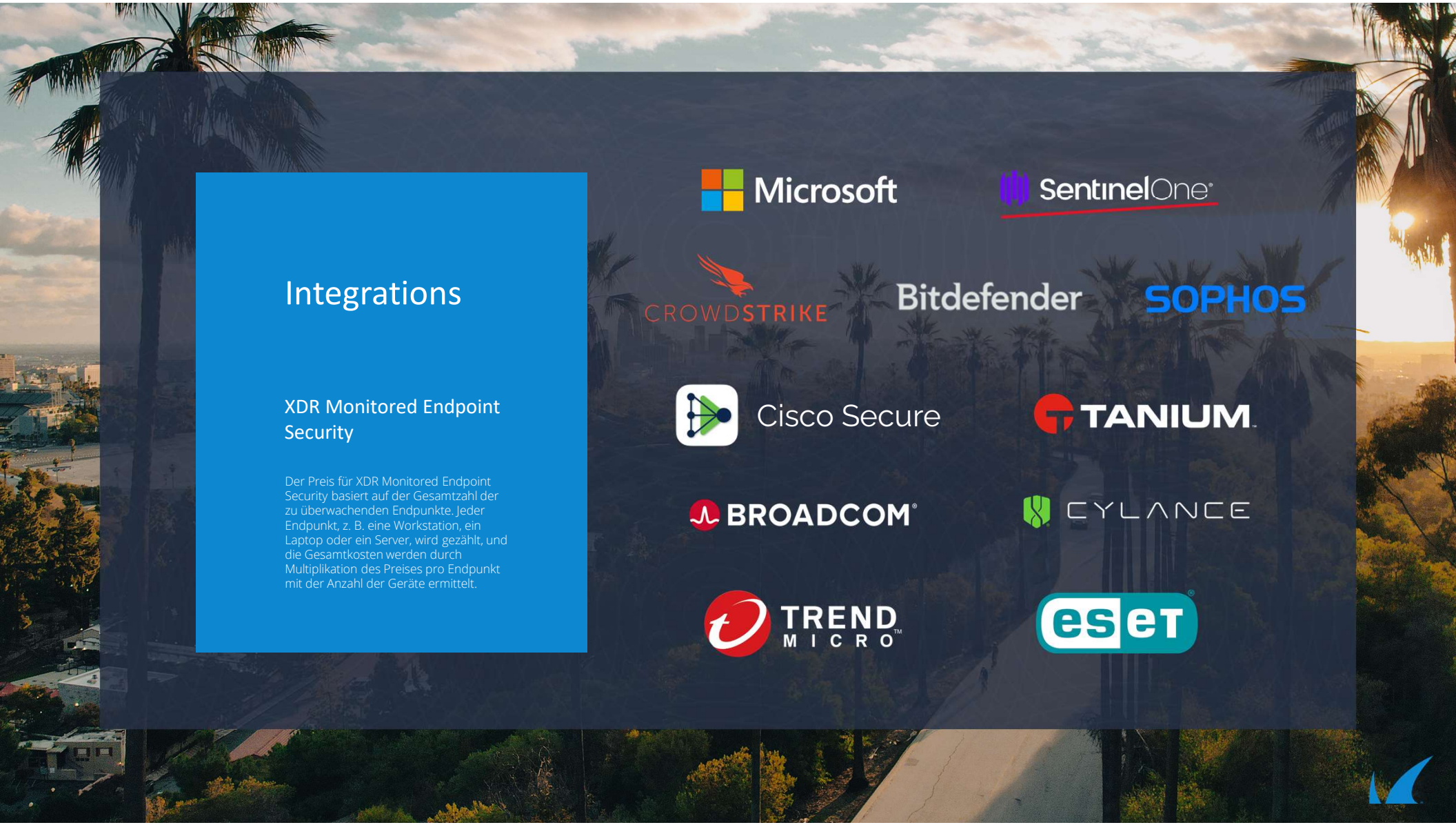
Barracuda XDR Endpoint Security verbessert die Erkennung von Bedrohungen durch die Integration von Daten aus bestehenden Endpunktschutzlösungen, um einen besseren Überblick und eine schnellere Reaktion zu ermöglichen. Unternehmen können Endpunkte auch proaktiver sichern, indem sie Expertenmanagement und kontinuierliche Überwachung durch unser Fully Managed Endpoint Security-Angebot nutzen.

XDR Managed Endpoint Security

Unsere XDR Managed Endpoint Security kombiniert die Leistung der KI-gesteuerten Erkennungs- und Reaktionsfunktionen von SentinelOne mit dem 24/7/365 Security Operations Center (SOC) von Barracuda für eine unvergleichliche Bedrohungsabwehr. Dieser Service umfasst Richtlinienmanagement, umfassende Reaktionsmöglichkeiten, Bedrohungsjagd und kontinuierliche Agenten-Updates zur Aufrechterhaltung der Spitzenleistung.

XDR Monitored Endpoint Security

XDR Monitored Endpoint Security bietet kontinuierliche Transparenz, Korrelation und Analyse von Sicherheitsereignissen auf allen Endpunkten unter Verwendung einer vorhandenen EDR-Lösung. Während sich der Endpunktschutz auf die lokale Erkennung und Blockierung von Bedrohungen konzentriert, verbessert XDR dies durch die Integration von Daten aus Ihrem Endpunktschutz zusammen mit verschiedenen anderen Datenquellen, die Identifizierung komplexer Angriffsmuster und die Beschleunigung der Bedrohungserkennung.


Integrations
XDR Monitored Endpoint Security
Der Preis für XDR Monitored Endpoint Security basiert auf der Gesamtzahl der zu überwachenden Endpunkte. Jeder Endpunkt, z. B. eine Workstation, ein Laptop oder ein Server, wird gezählt, und die Gesamtkosten werden durch Multiplikation des Preises pro Endpunkt mit der Anzahl der Geräte ermittelt.
Microsoft
SentinelOne
CROWDSTRIKE
Bitdefender
SOPHOS
Cisco Secure
TANIUM
BROADCOM
CYLANCE
TREND MICRO
eset

XDR Email Security

XDR Email Security

Barracuda XDR Email Security lässt sich nahtlos in Ihre bestehenden E-Mail-Sicherheitsdienste integrieren, um den Schutz mit verbesserter Transparenz, SIEM-Protokollierung und Echtzeit-Warnungen zu ergänzen - alles innerhalb einer einheitlichen XDR-Plattform. Dieser Service ermöglicht es Unternehmen, E-Mail-basierte Bedrohungen effektiver zu erkennen, zu analysieren und darauf zu reagieren, indem er umfassende Einblicke und eine zentralisierte Überwachung bietet.

Verbesserte Sichtbarkeit

Die Aufnahme von E-Mail-Schutzprotokollen in unsere Managed XDR-Plattform ermöglicht die Korrelation von E-Mail-basierten Bedrohungen mit Daten aus anderen Technologien, um breitere Angriffsmuster oder versteckte Bedrohungen aufzudecken. Die Kreuzkorrelation dieser Daten erhöht die Transparenz, sodass Sicherheitsteams Multi-Vektor-Angriffe erkennen und effektiver auf potenzielle Verstöße reagieren können.

Zentralisierte Protokollierung

Durch die Integration in bestehende E-Mail-Sicherheitsdienste mit SIEM-Protokollierung wird eine zentrale Überwachung ermöglicht, die die Effizienz der Bedrohungsanalyse und der Reaktion auf Vorfälle verbessert.

Alarmierung in Echtzeit

XDR Email Security liefert Echtzeitwarnungen und versetzt Sicherheitsteams in die Lage, E-Mail-basierte Angriffe schnell zu erkennen, zu analysieren und zu entschärfen und so das Risiko von Datenschutzverletzungen und Geschäftsunterbrechungen zu verringern.

Integrations

XDR Email Security

Die Preise für XDR Email Security richten sich nach der Anzahl der lizenzierten Postfächer auf Ihrer E-Mail-Plattform, unabhängig davon, ob es sich um Microsoft 365 oder Google Workspace handelt.

Barracuda Email Protection™ ADVANCED

Barracuda Email Protection™ PREMIUM

Barracuda Email Protection™ PREMIUM PLUS

mimecast

Microsoft Defender for 365

XDR Server Security

XDR Server Security

Barracuda XDR Server Security sammelt, aggregiert und normalisiert Protokolldaten von einigen der kritischsten Windows- und Linux-Server innerhalb eines Netzwerks. Es identifiziert potenzielle Risiken mithilfe der XDR-Analyseplattform, Threat Intelligence und des Security Operations Center.

Erweiterte SIEM-Protokollierung

Barracuda XDR Server Security verbessert die Erkennung von Bedrohungen durch das Sammeln und Normalisieren von Protokolldaten von kritischen Windows- und Linux-Servern, was einen umfassenden Einblick in die Netzwerkaktivitäten ermöglicht und wertvolle Erkenntnisse zur Identifizierung potenzieller Risiken liefert.

Active Directory

Durch die Integration mit Active Directory hilft Barracuda XDR Server Security bei der Erkennung von unbefugtem Zugriff, verdächtigen Kontoaktivitäten und potenziellen Versuchen der Privilegienerweiterung und bietet so eine wichtige Verteidigungsebene für die Verwaltung des Benutzerzugriffs und den Schutz sensibler Daten.

Analyse von Nutzerverhalten

Die fortschrittliche Analyseplattform von XDR überwacht die Verhaltensmuster der Benutzer und ermöglicht die Identifizierung anomaler Aktivitäten, die auf böswillige Absichten oder Insider-Bedrohungen hindeuten können.

XDR Cloud Security

XDR Cloud Security

Barracuda XDR Cloud Security überwacht Cloud-Dienste, um böswillige Aktivitäten zu erkennen und abzuschwächen. Dabei konzentriert sich die Lösung auf Risiken wie unbefugten Zugriff auf Mailboxen, Admin-Änderungen, unmögliche Logins und Brute-Force-Angriffe. Durch die Analyse der Cloud-Infrastruktur und des Nutzerverhaltens hilft es, Schwachstellen bei Identitäten, Assets und Privilegien in Echtzeit zu identifizieren und ermöglicht so eine proaktive Erkennung von Bedrohungen und eine schnelle Reaktion, um einen potenziellen Verstoß zu entschärfen.

Automated Threat Response

Automated Threat Response für Microsoft 365 ermöglicht die Behebung von Kontokompromittierungen und verkürzt die Zeit zwischen Erkennung und Schadensbegrenzung. Dieser proaktive Ansatz trägt dazu bei, die Auswirkungen von Angriffen zu mindern, einen kontinuierlichen Schutz zu gewährleisten und die allgemeine Sicherheitslage zu verbessern.

Verhaltensanalyse

Barracuda XDR Cloud Security nutzt fortschrittliche Analysen, um die Cloud-Infrastruktur und das Nutzerverhalten zu untersuchen und Schwachstellen bei Identitäten, Assets und Berechtigungen in verschiedenen Cloud-Technologien zu identifizieren.

Umfassende Cloud-Transparenz

Barracuda XDR Cloud Security bietet tiefe Einblicke in Cloud-Umgebungen und ermöglicht die Echtzeit-Überwachung verschiedener Cloud-Dienste und Benutzeraktivitäten, um Schwachstellen bei Identitäten, Assets und Berechtigungen zu identifizieren und zu beheben.

Integrations

XDR Cloud Security

Der Preis für XDR Cloud Security richtet sich nach der Anzahl der lizenzierten Postfächer in Ihrer Microsoft 365- oder Google Workspace-Umgebung. Dieser „All-you-can-eat"-Service bietet umfassenden Schutz ohne zusätzliche Kosten für die Integration mehrerer Cloud-Plattformen oder -Dienste.

Microsoft 365

Microsoft Entra ID (Azure)

Google Workspace

amazon web services

DUO

okta

Barracuda SOC

SOC Leadership

Sr. Cyber Analysts

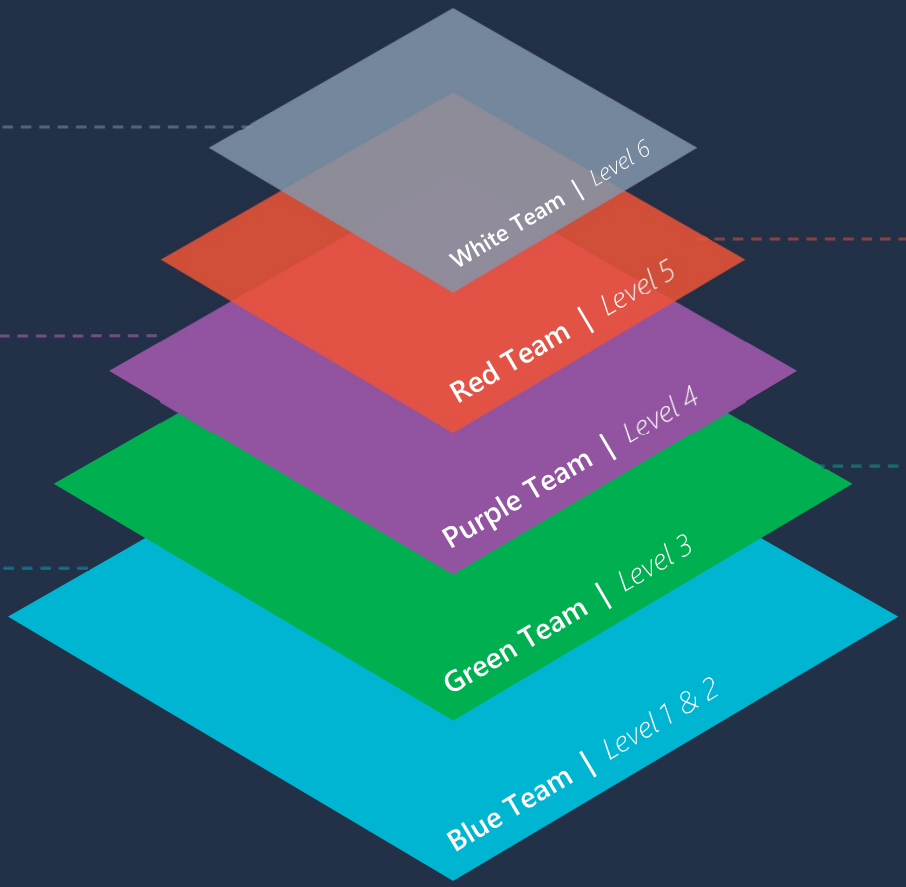
Improve Efficiency

Collaborative Security
Improve both Red/Blue Team
Workflow Automation
Process Enhancements
Customer Escalations
Emerging Threats

Cyber Analysts

Detect Attacks

Defensive Security
Oppose Red Team
Protect System and data
Incident Guidance



Security Engineers

Exploit Weaknesses

Offensive Security
Oppose Blue Team
Use Case development
Attack Detection methods
Threat Intelligence
Threat Hunting
New Threats R&D

Endpoint Engineers

Endpoint Security

Endpoint Protection MGMT
Device Policy Management
Attack and Defend Exercises
Malware Analysis
Threat Hunting
Research and Dev

SOC Maturity Matrix

Not all SOCs are created equal

	LEVEL 1 Basic	LEVEL 2 Intermediate	LEVEL 3 Advanced	LEVEL 4 Optimized	LEVEL 5 Innovative
People	Blue Team Analysts, business hours coverage	Blue Team, 24x7 Coverage	24x7 SOC team with specialized roles (Blue, Green)	24x7 SOC team with advanced roles (Purple, Red)	24x7 Global SOC Blue, Green, Purple, Red, White Teams with regional presence (AMER, EMEA, APAC)
Skills	Network Security, Operating Systems knowledge, Email analysis	IDS and IPS knowledge. SOC tools such as SIEM	Cloud Computing, Endpoint security, audit and threat analysis, adversary attack tactics and techniques	Deep experience with live attacks ranging from various ATPs. Advanced SOC tools such as SOAR	Comprehensive skill set, covering all aspects of defensive and offensive security tools along with development and AI/ML expertise. R&D into new security advancements & optimizations
Certifications	Security+, Network+	CIEH, CySA+	AWS Cloud Practitioner, Azure Fundamentals	GIAC, AWS Solutions Architect, AWS Developer	CISSP, AWS, Azure, CISA, CSAP, ISO 27001, AWS Security, GCIH, C|EH, GIAC, and CySA+, Security+, Network+
Process	Simple incident escalation and out of the box rules	Runbooks/playbooks, threat hunting, basic emerging threats coverage	Security risk classification, manual allow and blocklist capabilities, custom SIEM rules	Advanced threat hunting, attack and defend exercises, log correlation across multiple data sources	Advanced runbook mapping, attack and defend exercises, incident response guidance and threat hunting. Automated allow and blocklist capabilities. Faster zero-day coverage
Technology	Basic SIEM	Advanced SIEM, Open-source threat intelligence	EDR resources, malware sandbox	SOAR, 300+ signature-based detections mapped to MITRE ATT&CK, cloud lab	State of the art SIEM, SOAR, TIP with 11B+ IOCs, 900+ ML-based detections, MITRE ATTACK framework mapping, attack labs, automated threat defense

Barracuda XDR™

Compliance

Security

Privacy

Barracuda XDR Alert

Barracuda XDR™

SECURITY OPERATIONS CENTER ALERT

Your request 33468731 has been updated. To add additional comments, reply to this email.

Eric Russo (Barracuda SKOUT Managed XDR)
8/9/2023, 2:50 PM EDT

Barracuda XDR - GLB.AU.CAS Office 365 Impossible Travel

Field	Value
ID	33468731
Subject	Barracuda XDR - GLB.AU.CAS Office 365 Impossible Travel
Type	Alert
Impact	High
MITRE ATT&CK® Tactic	Credential Access
MITRE ATT&CK® Technique	Forced Authentication
Created Time	8/9/2023, 2:50 PM EDT
Completed Time	8/10/2023, 3:06 PM EDT
Account	Acme Inc
Description	Incident Name: GLB.AU.CAS Office 365 Impossible Travel Organization Name: Acme Inc MITRE ATT&CK: Tactic - Credential Access (TA0006) & Technique - Forced Authentication (T1187) Risk: Low Ticket #: 33468731 Time the incident occurred: Wednesday August 09 2023, 18:49 PM UTC

What is the Threat:
Barracuda XDR has detected successful Office 365 sign-in events from distinct locations that would constitute an impossible travel scenario. This rule logic looks at distances over 1000 KMs and required speeds of travel over 800 KM/H between 2 login events. The detection algorithm calculates the distance and speed required to travel between two sets of geo coordinates from the Office 365 logs below and determines if such travel is possible, even by the fastest means. This may indicate that the user's credentials were compromised, therefore, please see recommendations below. If this is authorized activity, please let us know and we will tune the alerts accordingly.
CAUTION: Geo-Location and VPN Detection via source IP address is not a perfect science, so we cannot guarantee accuracy.

Impossible Travel Summary

- Impacted user: blueteam@skoutsiemtestingsandbox.onmicrosoft.com
- Distance between the two logins: 3585km (2222.08 mi)
- Required speed of travel: 3594 KMH (2156.4MPH)
- Time between the two logins: 59.85 Minutes
- Total logins analyzed in past 24 hours: 4

We compared these logins...

First Login
Timestamp 2023-08-09T17:33:20 UTC
Source IP 2603:7080:100:8a:4cb0:247e:1192:c852
IP Threat Intel Reputation: 0/93
VPN Detected False - No specific VPN service name identified
Geo-IP Location Albany, New York, United States

Second Login
Timestamp 2023-08-09T18:33:11 UTC
Source IP 2607:fb90:8782:8944:954c:2192:416:1b4e
IP Threat Intel Reputation: 0/93
VPN Detected False - No specific VPN service name identified
Geo-IP Location Las Vegas, Nevada, United States

Known Email Breaches:
Email: blueteam@skoutsiemtestingsandbox.onmicrosoft.com
Result: We searched our threat intelligence and provided the results for any potentially leaked information for this user in a previous alert.

How did it occur:
Potential weak credentials, adversary password spraying, or phishing emails.

How did we Detect it:
This activity was observed by analyzing Office 365 logs coming from Acme Inc.

What should you do:
Verify if this activity is authorized. If NOT please use the recommendations provided below. Also please let the Barracuda XDR SOC know if this is a "True Positive", "Authorized Activity", or "False Positive" incident.

BARRACUDA XDR RECOMMENDATIONS
1. De-escalate the account privileges or fully disable the user account to protect sensitive assets on your network until a full investigation can be completed.
2. Implement Multi-Factor Authentication (MFA) or Configure Office 365 conditional access policies to further secure accounts.
3. Reset the users credentials: Choose passwords of eight letters or more with some complexity (letters and numbers, or requiring one special character). For passwords to be an effective measure against cyber attackers, the following should be adhered to:
- Should use a combination of uppercase and lowercase letters, numbers, special characters, e.g. @, #, -, _ , $, !
- Should be at least, 12-14 characters in length
- Passwords should be unique and different for every account that requires a password
- Passwords should never be shared; with anyone!
- Passwords should never be written down
- Do NOT reuse old passwords
4. If the account in question was compromised through a successful phishing attempt, we recommend checking to see if other users received the same phishing message and removing the suspicious message from all inboxes.

Thank You,
Barracuda XDR SOC
SOC@BARRACUDA.COM
US: +1 855-838-4500 | IRE: +353 1 513-7503 | UK: +44 20 3695-8498 | APAC: +61 2 7228 1891

Alert Priority & SLA

Low Risk

SLA
8 Stunden

Escalation Method

- Email oder Ticket Integration
- Barracuda XDR Dashboard

Beschreibung

Aktivitäten, die zur Kenntnisnahme beitragen, aber möglicherweise keine Maßnahmen erfordern

Beispiel

- User account erstellt
- Datenscans
- Passwortänderung

Medium Risk

SLA
1 Stunde

Escalation Method

- Email oder Ticket Integration
- Barracuda XDR Dashboard

Beschreibung

Aktivität, die Maßnahmen erfordert, aber als Einzelereignis in der Regel nicht zu erheblichen Auswirkungen führen würde

Beispiel

- Verdächtiger Login(versuch)
- Brute-force Angriff
- Threat intelligence matches

High Risk

SLA
20 Minuten

Escalation Method

- Telefonanruf
- Email oder Ticket Integration
- Barracuda XDR Dashboard

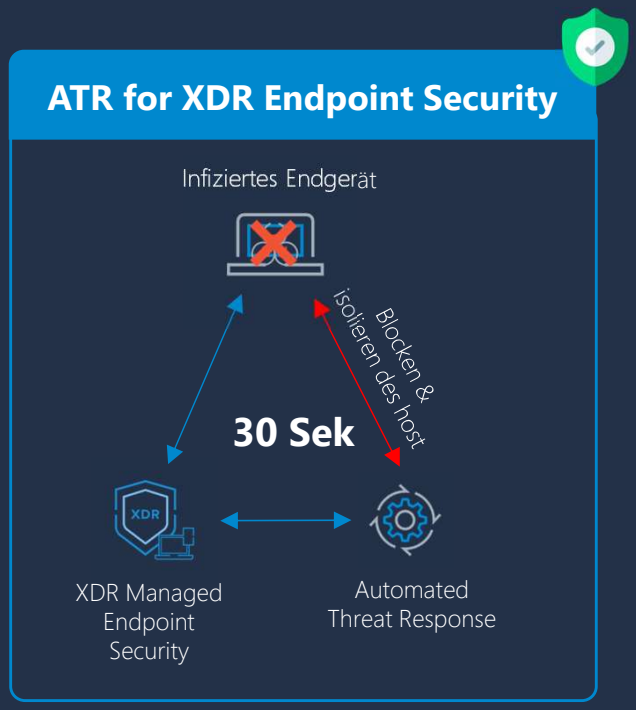
Beschreibung

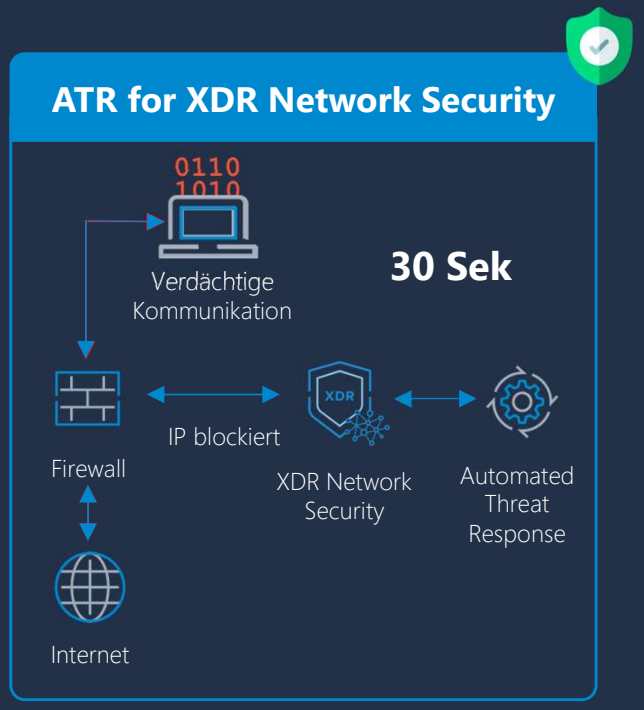
Aktivitäten, die das Potenzial haben, der Umwelt des Kunden schweren Schaden zuzufügen

Beispiel

- Malware oder Ransomware
- Ausnutzung von Zugriffsrechten
- Hacking tool erkannt

Automated Threat Response





SOAR

Security Orchestration Automation & Response

Erfassung

Beseitigt Fehlalarme und fügt den erfassten Telemetriedaten zusätzlichen Kontext hinzu, z. B. die mit einer IP-Adresse verbundene Geolokalisierung.

Interpretation

Identifiziert ähnliche Ereignisdaten aus mehreren Telemetriequellen, um Muster zu erkennen, und hilft darüber hinaus, falsch-positive Ergebnisse zu entfernen

Deduktion

Identifiziert ähnliche Alarme und Warnungen und fasst sie zu einem einzigen Vorfall zusammen

Lösung

Aktives Blockieren wird innerhalb der Assets implementiert, z. B. indem eine Firewall eine bösartige IP-Adresse in ihre Blockierliste aufnimmt.

Runbooks

Schritt-für-Schritt-Anleitung, die erklärt, wie man auf einen Vorfall reagiert

NIS 2 Checkliste

- Risikomanagement
- Erkennung und Reaktion
- Systemüberprüfung
- Protokollierung
- Prozesse definieren
- Updates
- Meldepflicht
- Lieferkette
- Mitarbeiterschulung

Warum Barracuda Managed XDR?

Technical Advancements

- 24/7/365 Mature Global Security Operations Center
- Fully Managed SIEM
- Herstellerunabhängig
- Automated Threat Response mit SOAR
- Komplettes Managed Endpoint protection & response
- Robustes Threat Intelligence mit mehr als 11 Milliarden IOCs
- Generative AI/ML-Regeln, abgebildet auf das MITRE-Framework
- Proactive Threat Hunting

Business Advantages

- Einfache Lizenzierung
- Keine Extrakosten für Onboarding
- Keine Mindestabnahmemenge
- Ala carte bundling
- Keine Extrakosten für Datenstrom
- White-glove onboarding
- Wöchentliche Threat Advisories
- Multi-tenant Capabilities
- Customizable executive reporting

Partnerschaftlicher Erfolg

Einheitlcihes Partner Program

Das Barracuda-Partnerprogramm bietet unseren Partnern exklusive Ressourcen, Schulungen und Support, um das Wachstum zu beschleunigen und den Erfolg unserer Kunden zu fördern.

Pre & Post Sales Support

Das Barracuda-Partnerprogramm stellt sicher, dass Partner in jeder Phase des Verkaufszyklus auf die Bedürfnisse ihrer Kunden eingehen können.

Co-Brandable Marketing

Partner erhalten Zugang zu brandingfähigen Assets, gemeinsam veranstalteten Webinaren, Marketing Campaign-in-a-Box-Ressourcen und persönlichen Veranstaltungsmöglichkeiten, die es ihnen erleichtern, professionelle, zielgerichtete Marketinginitiativen zu entwickeln, die bei ihrem Publikum Anklang finden.

Partner Success & Technical Support

Partner erhalten Zugang zu brandingfähigen Assets, gemeinsam veranstalteten Webinaren, Marketing Campaign-in-a-Box-Ressourcen und persönlichen Veranstaltungsmöglichkeiten, die es ihnen erleichtern, professionelle, zielgerichtete Marketinginitiativen zu entwickeln, die bei ihrem Publikum Anklang finden.

Thank You

Barracuda
Your business, secured.