Starke Cyberabwehr mit XDR
Schutz für KMU

Philipp Geßner
Strategic Partner Development Manager (DACH)

MSP
Barracuda.
Your journey, secured.

Was wir verhindern wollen

Forbes

$70 Million Demanded As REvil Ransomware Attackers Claim 1 Million Systems Hit

Ransomware Attack Reported at Insurance Giant AXA One Week After It Changes Cyber Insurance Policies in France

BBC | Sign in | Home | News | Sport | Reel | Worklife | Trav

Meat giant JBS pays $11m in ransom to resolve cyber-attack

10 June

The New York Times

The Colonial Pipeline Cyberattack | What to Know | Pipeline Resumes | $5 Million Ransom | DarkSide Says Shutting Down | Weaknesses in U.S. Cybersecurity

Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers

The payment clears the way for gas to begin flowing again, but it risks emboldening other criminal groups to take American companies hostage by seizing control of their computers.

Aktuelle Situation

Organisationen jeder Größe sind gefährdet.

Ransomware-Forderungen eskalieren und ein Ende ist nicht in Sicht, und Cyber-Versicherungen lösen das Problem nicht.

Geschäftsmodell: Ransomware, eine relativ einfache Geldquelle

Wenn sie Sie jetzt nicht erwischen, werden sie es später wieder versuchen.

Grundlegende Sicherheits Strategien

Email & Social Engineering

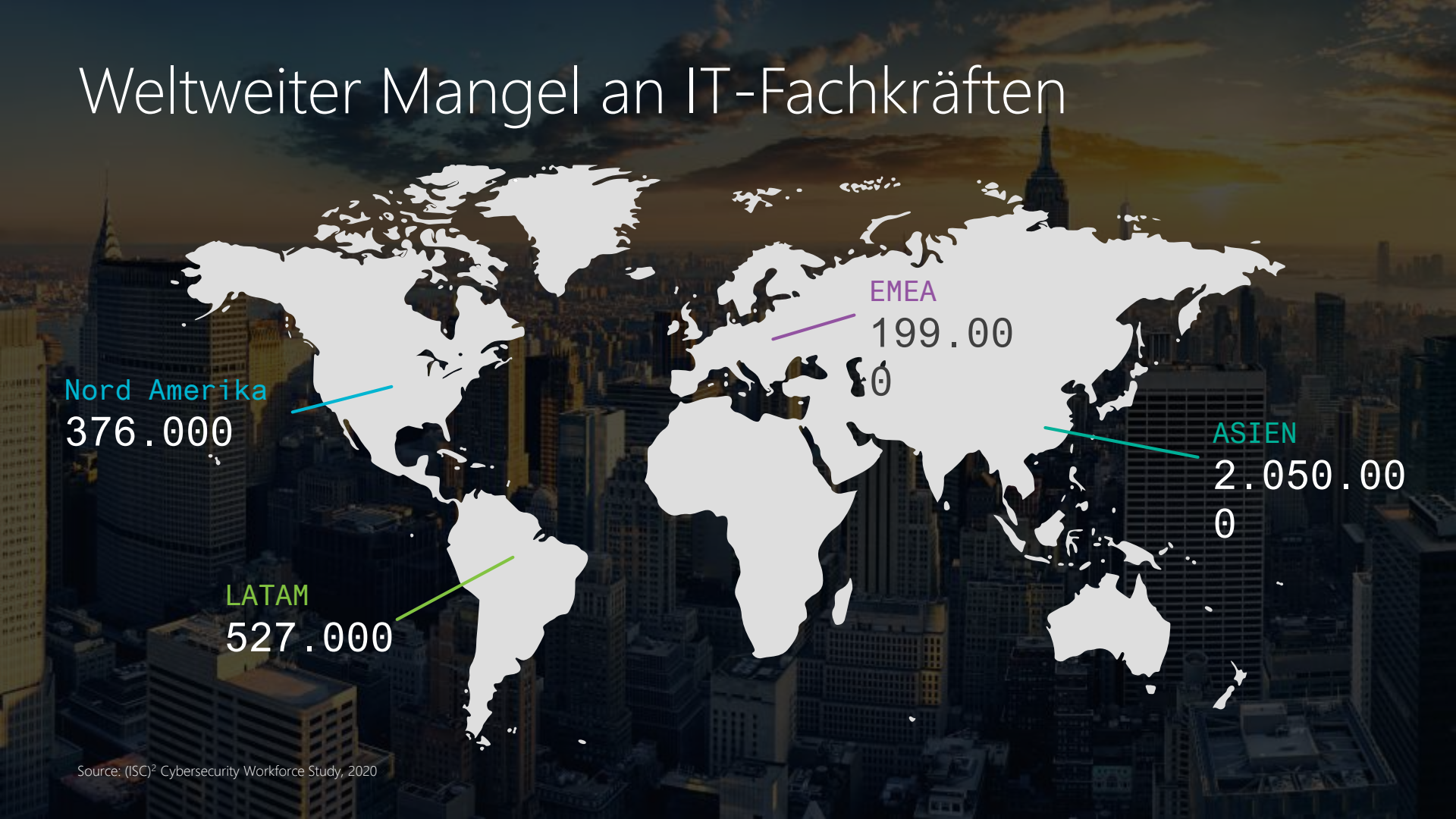
Network & App Protection

Backup & Recovery


So einfach ist das!


Warum ist die IT-Security nicht ganz so einfach?

Weltweiter Mangel an IT-Fachkräften



Source: (ISC)² Cybersecurity Workforce Study, 2020

Weltweiter Mangel an IT-Fachkräften

Source: (ISC)² Cybersecurity Workforce Study, 2020

Grundlegende Cyber-Hygiene für Unternehmen

1

Festlegen, was geschützt werden muss

2

Konzentrische Ringe der Sicherheit aufbauen

3

Überwachung der Umgebung

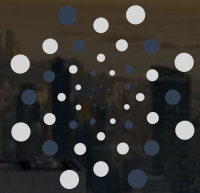
4

Reaktionszeit verkürzen

5

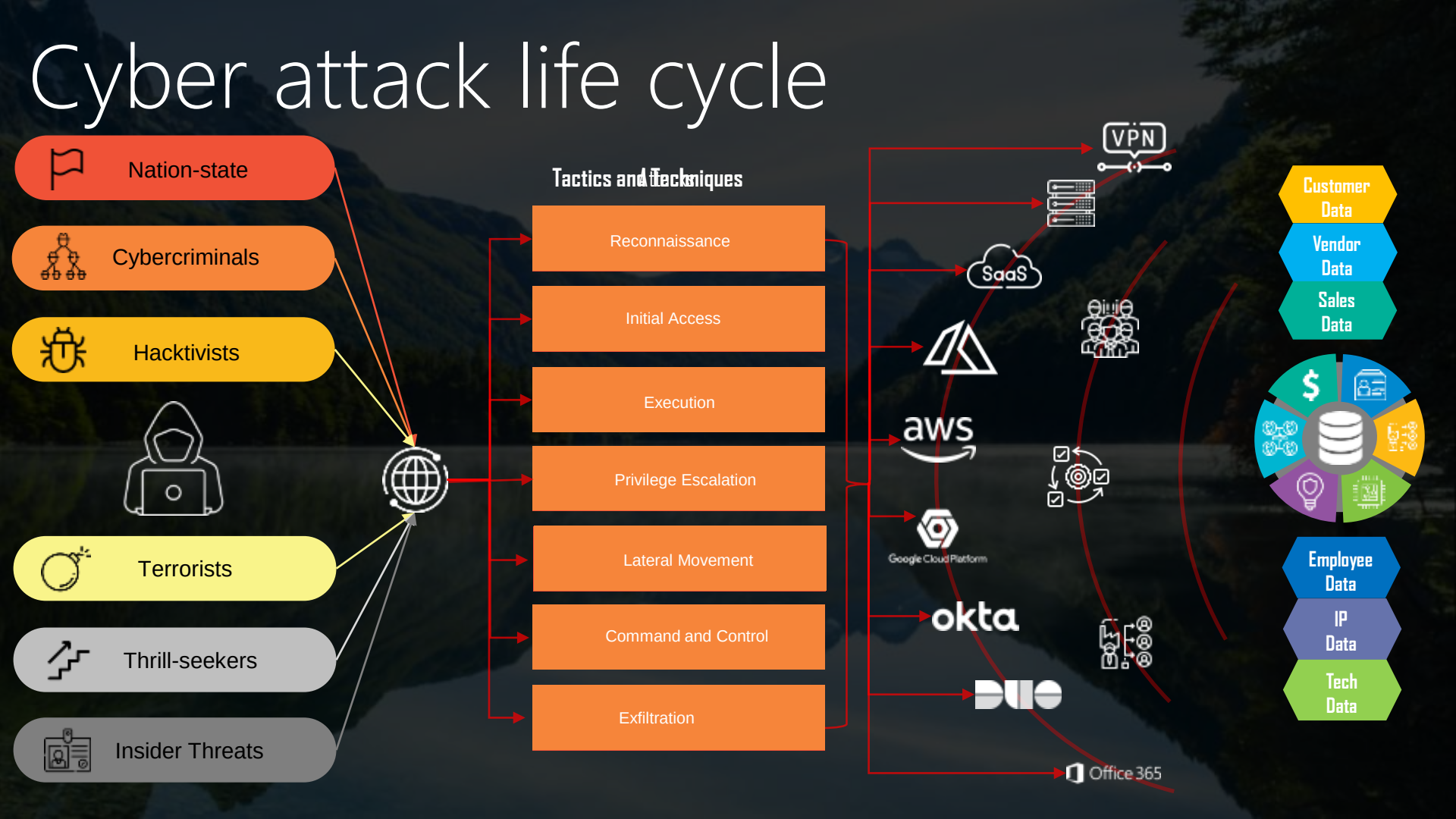
Mitarbeiter, Prozesse und Technologie sichern

Cybersecurity Landschaft



	2000	2007	2014	2022
Gerät	Desktop/Laptop	Mobile	IoT (Internet of Things)	IoE (Internet of Everything)
Hacker	Script Kiddies	Criminal Ecosystem	Hacktivists	Non-State Actors
Perimeter	Controlled Access	Wide Access	Hybrid Cloud	kein Perimeter
Attacken	Intrusiv	Disruptiv	Destructive	Verheerend

Cyber attack life cycle



XDR – was bedeutet das?

eXtended visibility

Was überwachen wir?

- Authentifizierung
- Cloud
- Kritische Server
- E-Mail
- Endgeräte
- Netzwerk
- SaaS

Detection

Was erkennen wir?

- Kontoübernahme
- Denial of Service
- Anomale Privilegienerweiterung
- Kompromittierung von Geschäfts-E-Mails
- Zero-Day-Angriff
- Malware und Ransomware

Response

Wie reagieren wir?

- Konto deaktivieren
- IP-Sperre
- Passwort zurücksetzen
- Host-Quarantäne
- Instance Re-Deploy
- Nachrichten blockieren

Managed XDR bedeutet, dass ein SOC mitgeliefert wird.

XDR Workflow

Ereignisse

E-Mail senden oder empfangen

Datei-Downloads

Passwortänderungen

eXtended Visibility

SIEM

SOAR Technologie

SOC

Detection

Alarm-Analyse

Ausgereiftes SOC

Mehrere Datenquellen

Response

Alarm

Eine Nummer zum Anrufen

Kunde/Reseller

DURCHSCHNITTLICHER VIERTELJAHRESBERICHT

94,072,642 EREIGNISSE | 2.710 ANALYSIERTE ALARME | 16 WARNMELDUNGEN

EDR vs. MDR vs. XDR

EDR

Endpoint detection and response

- Fokus auf Endpunkt-Bedrohungen
- Fähigkeit zur Blockierung oder Quarantäne von Malware
- Untersuchung von Bedrohungen auf Endpunktebene

MDR

Managed detection and response

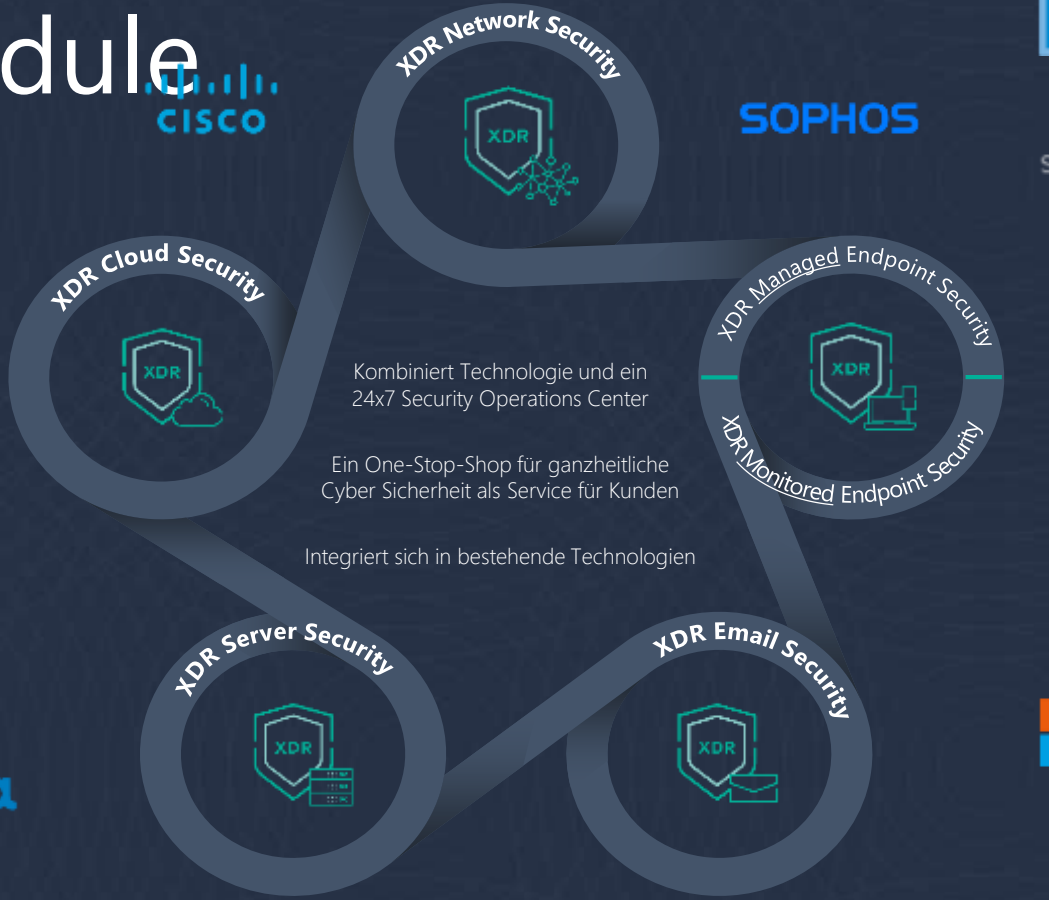
- Anbieter, der Erkennungs- und Reaktionsdienste anbietet
- SOC-Dienste anbietet, um bei der Sichtung von Sicherheitswarnungen zu helfen
- Sicherheitstools wie SIEM oder SOAR implementieren

XDR

eXtended visibility, detection and response

- Umfasst EDR und MDR mit der Möglichkeit, Transparenz über alle Daten zu schaffen
- Erkennt Angriffe von Cloud- und SaaS-Anwendungen, Firewalls usw.
- Automatische Entschärfung von Bedrohungen durch bidirektionale Integration zwischen Sicherheitstools und der XDR-Plattform

Integrationen und Module



MSP Barracuda XDR™

cisco

SOPHOS

SONICWALL

Azure

citrix

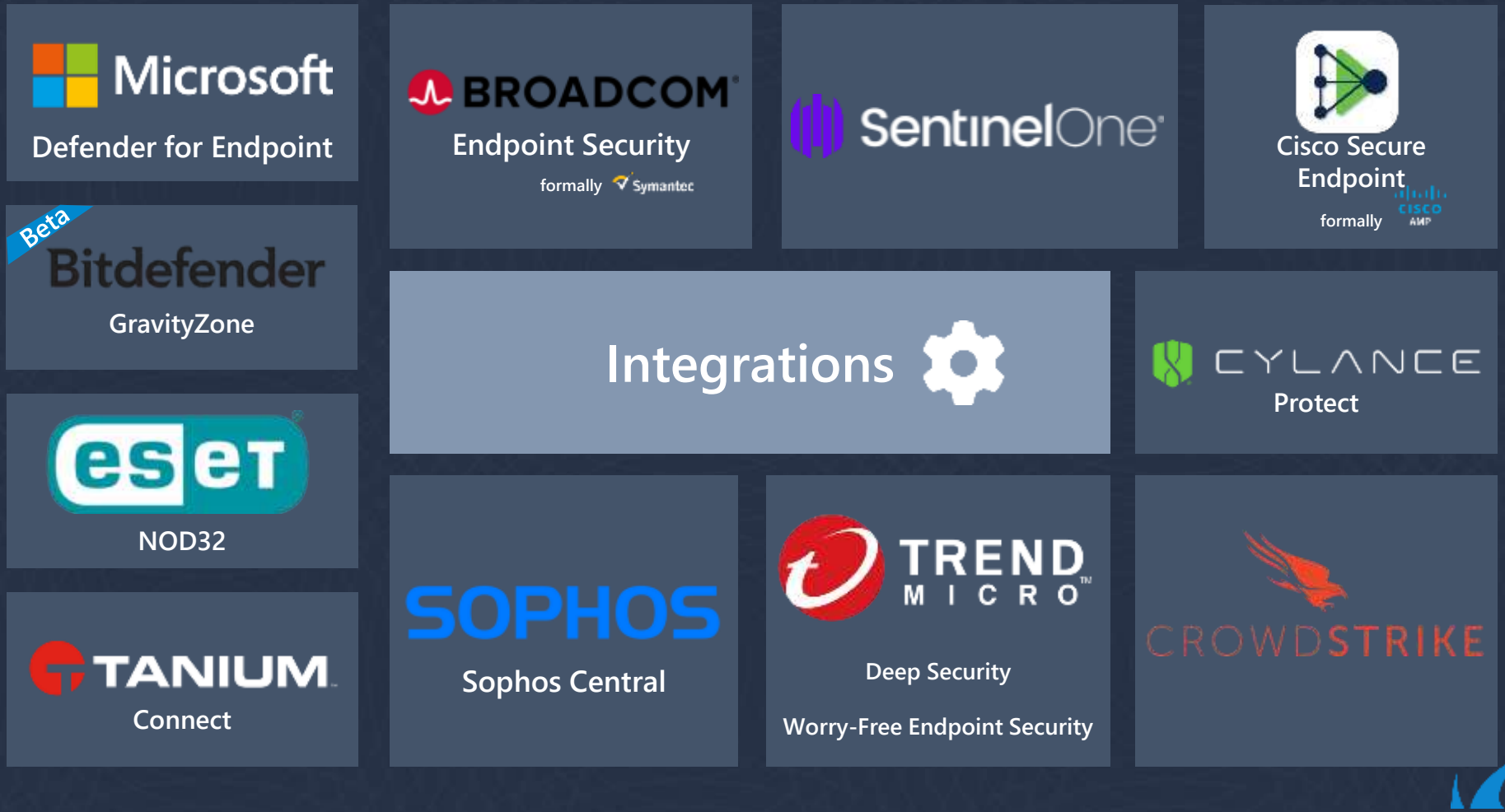
SentinelOne

Google Workspace

Office 365

amazon web services

okta


Microsoft
Defender for Endpoint
BROADCOM
Endpoint Security
formally Symantec
SentinelOne
Cisco Secure
Endpoint
formally Cisco AMP
Beta
Bitdefender
GravityZone
Integrations
CYLANCE
Protect
eset
NOD32
SOPHOS
Sophos Central
TREND MICRO
Deep Security
Worry-Free Endpoint Security
CROWDSTRIKE
TANIUM
Connect

SOC Security Alert

Barracuda XDR™

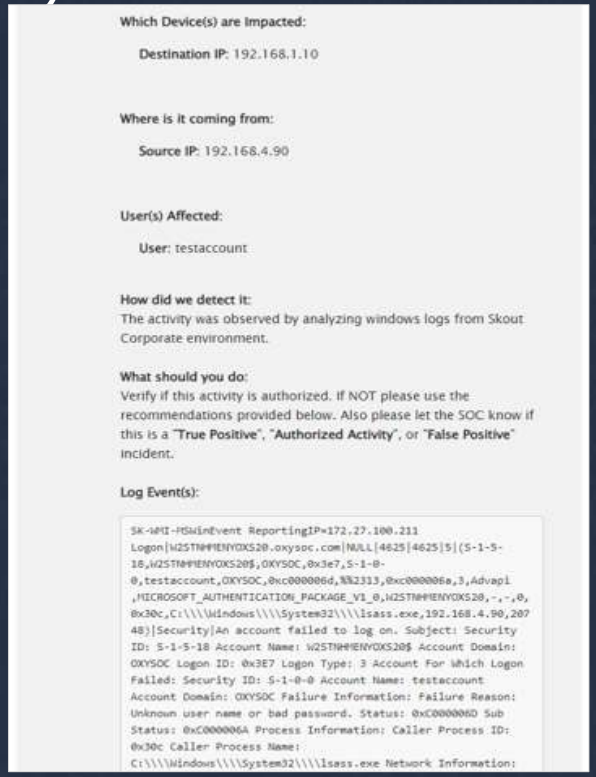
SECURITY OPERATIONS CENTER ALERT

Your request (6702583) has been updated. To add additional comments, reply to this email.

Eric Russo (Barracuda SKOUT Managed XDR)
Apr 7, 2023, 1:35 PM EDT

Incident Name: SKOUT Security Monitoring – GLB.AU.UNI Brute Force Authentication User Attempt
Organization Name: Skout Corporate
Risk: low
Analyst: Eric Russo
Ticket #: 6702583
Time the incident occurred: Apr 7, 1:35 PM

What is the Threat:
Barracuda SKOUT SOC has identified suspicious communication between the internal hosts "192.168.4.90" and "192.168.1.10" for the user "testaccount". This traffic has triggered an alarm for a possible bruteforce authentication attempt. A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. The Windows Security substatus for this activity is "0xC000006A", which means user logon with misspelled or bad password.



Which Device(s) are Impacted:

Destination IP: 192.168.1.10

Where is it coming from:

Source IP: 192.168.4.90

User(s) Affected:

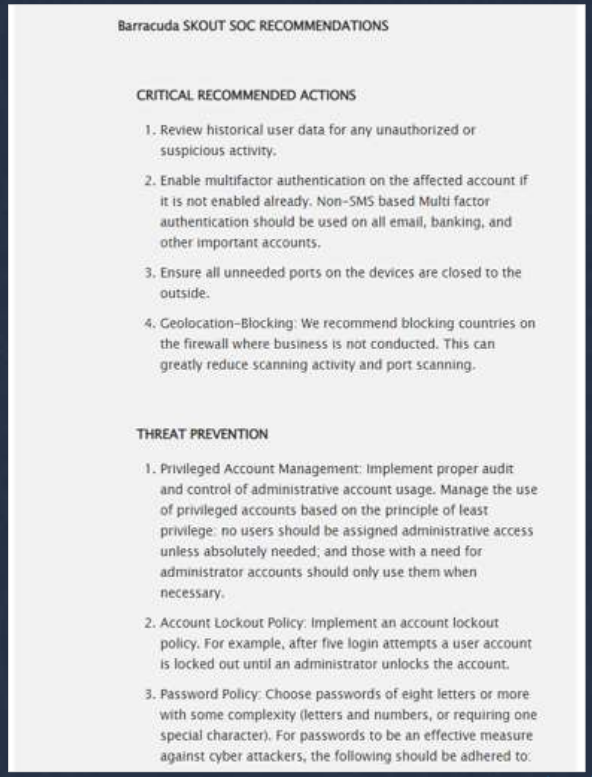
User: testaccount

How did we detect it:
The activity was observed by analyzing windows logs from Skout Corporate environment.

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

Log Event(s):

```
SK-WMI-MSWinEvent ReportingIP=172.27.100.211
Logon|W2STNMMENYOXS20.oxysoc.com|NULL|4625|4625|5|(S-1-5-
18,W2STNMMENYOXS20$,OXYSOC,0x3e7,S-1-0-
0,testaccount,OXYSOC,0xc000006d,%%2313,0xc000006a,3,Advapi
,MICROSOFT_AUTHENTICATION_PACKAGE_V1_0,W2STNMMENYOXS20,-,-,0,
0x30c,C:\\\\Windows\\\\System32\\\\lsass.exe,192.168.4.90,207
48)|Security|An account failed to log on. Subject: Security
ID: S-1-5-18 Account Name: W2STNMMENYOXS20$ Account Domain:
OXYSOC Logon ID: 0x3E7 Logon Type: 3 Account For Which Logon
Failed: Security ID: S-1-0-0 Account Name: testaccount
Account Domain: OXYSOC Failure Information: Failure Reason:
Unknown user name or bad password. Status: 0xC000006D Sub
Status: 0xC000006A Process Information: Caller Process ID:
0x30c Caller Process Name:
C:\\\\Windows\\\\System32\\\\lsass.exe Network Information:
```



Barracuda SKOUT SOC RECOMMENDATIONS

CRITICAL RECOMMENDED ACTIONS

1. Review historical user data for any unauthorized or suspicious activity.
2. Enable multifactor authentication on the affected account if it is not enabled already. Non-SMS based Multi factor authentication should be used on all email, banking, and other important accounts.
3. Ensure all unneeded ports on the devices are closed to the outside.
4. Geolocation-Blocking: We recommend blocking countries on the firewall where business is not conducted. This can greatly reduce scanning activity and port scanning.

THREAT PREVENTION

1. Privileged Account Management: Implement proper audit and control of administrative account usage. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
2. Account Lockout Policy: Implement an account lockout policy. For example, after five login attempts a user account is locked out until an administrator unlocks the account.
3. Password Policy: 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:

Barracuda SOC

SOC Managers

Sr. Cyber Analysts

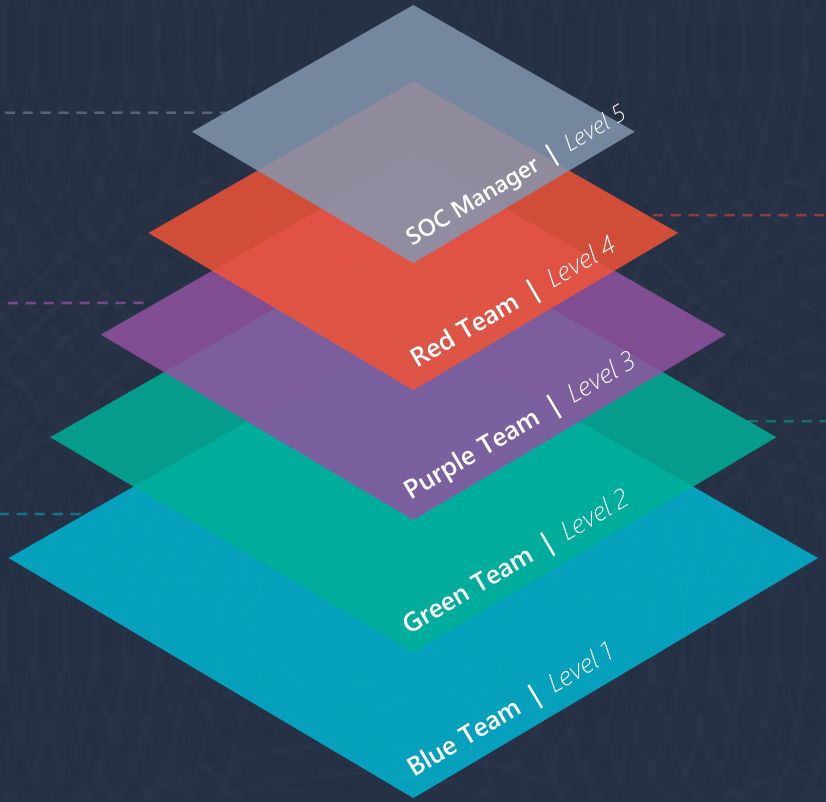
Improve Efficiency

Endpoint Protection MGMT
Device Policy Management
Attack and Defend Exercises
Threat Hunting
Research and Dev
Incident Response

Cyber Analysts

Detect ATT&CKS

Defensive Security
Oppose Red Team
Protect System and data
Incident Analysis
Vulnerability Scans
Email Analyst



Sr IR/Attack Analysts

Exploit Weaknesses

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

Endpoint Engineers

Endpoint Security

Offensive Security
Oppose Blue Team
Incident Responders
Use Case development
Attack Detection methods
Threat Hunting

Barracuda ist für Sie da!

Email Protection

- Barracuda Email Protection™ — INCIDENT RESPONSE (formerly Barracuda Forensics + Incident Response)
- Barracuda Email Protection™ — IMPERSONATION PROTECTION (formerly Barracuda Sentinel)
- Barracuda Cloud-to-Cloud Backup™
- Barracuda Email Protection™ — EMAIL GATEWAY DEFENSE (formerly Barracuda Essentials)
- Barracuda Email Protection™ — SECURITY AWARENESS TRAINING (formerly Barracuda PhishLine)
- Barracuda Cloud Archiving Service™

App & Cloud Security

- Barracuda Cloud Security Guardian™
- Barracuda Web Application Firewall™
- Barracuda WAF-as-a-Service™

Network Security

- Barracuda CloudGen Firewall™
- Barracuda CloudGen WAN™
- Barracuda CloudGen Access™

Data Protection

- Barracuda Cloud-to-Cloud Backup™
- Barracuda Data Inspector™
- Barracuda Backup™


Thank You
Barracuda.
Your journey, secured.