more security. usd

CLOUD SECURITY SCORING

Wie Schwachstellen in der Cloud bewerten?

OWASP Chapter Cologne, 21. Mai 2026

EINFÜHRUNG

Agenda

- Einführung
- Schwachstellen in der Cloud
- Vorstellung *Cloud Security Scoring*
- Beispiele aus der Praxis
- Fragen und Diskussion

Vorbemerkungen …

- Vortrag mit relativ viel Theorie – Motivation aber aus der alltäglichen Arbeitspraxis!
- An dieser Stelle keine ausführlichere Auseinandersetzung mit anderen Bewertungsverfahren.
- Es ist ein Entwurf, ein Zwischenstand, ein Vorschlag für ein Problem – Feedback wichtig!

SCHWACHSTELLEN IN DER CLOUD

Cloud Security als Herausforderung

- Ausgangssituation:
  - Konfigurationsfehler sind auch Schwachstellen, aber andere als in Software.
  - Bewertung von Schwachstellen in der Konfiguration von Cloud Services gefordert (meist CVSS wie auch bei klassischen Pentests).
  - Bestehende Scoring-Systeme nicht vollständig geeignet, es fehlen Metriken.
    - Beispiel: Auswirkungen erfolgreicher Ausnutzung einer Schwachstelle sind mit bestehenden Metriken nur schwer erfassbar.
  - Cloud Security Tools (z.B. Prowler, Steampipe) liefern meist nur einfache, zu grobe und nicht nachvollziehbare Bewertungen.

OWASP Top 10:2025

1. A01:2025 - Broken Access Control
2. A02:2025 - Security Misconfiguration
3. A03:2025 - Software Supply Chain Failures
4. A04:2025 - Cryptographic Failures
5. A05:2025 - Injection
6. A06:2025 - Insecure Design
7. A07:2025 - Authentication Failures
8. A08:2025 - Software or Data Integrity Failures
9. A09:2025 - Security Logging and Alerting Failures
10. A10:2025 - Mishandling of Exceptional Conditions

OWASP Top 10:2025

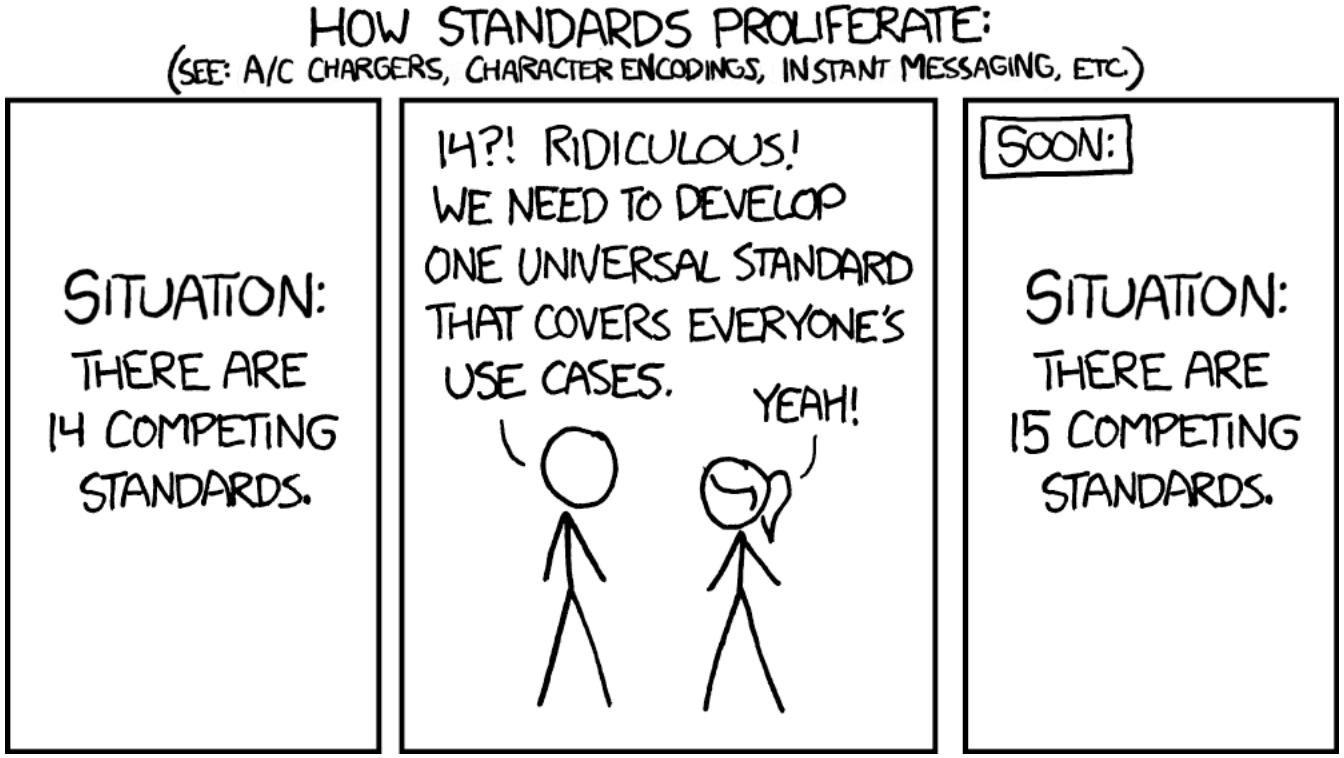
1. A01:2025 - Broken Access Control
2. A02:2025 - Security Misconfiguration
3. A03:2025 - Software Supply Chain Failures
4. A04:2025 - Cryptographic Failures
5. A05:2025 - Injection
6. A06:2025 - Insecure Design
7. A07:2025 - Authentication Failures
8. A08:2025 - Software or Data Integrity Failures
9. A09:2025 - Security Logging and Alerting Failures
10. A10:2025 - Mishandling of Exceptional Conditions

OWASP Top 10:2025

1. A01:2025 - Broken Access Control
2. A02:2025 - Security Misconfiguration
3. A03:2025 - Software Supply Chain Failures
4. A04:2025 - Cryptographic Failures
5. A05:2025 - Injection
6. A06:2025 - Insecure Design
7. A07:2025 - Authentication Failures
8. A08:2025 - Software or Data Integrity Failures
9. A09:2025 - Security Logging and Alerting Failures
10. A10:2025 - Mishandling of Exceptional Conditions

Yet Another Scoring System?

- Wir erfinden das Rad nicht neu!
- Wir haben von bestehenden Verfahren passende Metriken übernommen oder angepasst und nur fehlende ergänzt.
- Vorbilder: CVSS, CWSS, CCSS, OWASP Risk Rating Methodology
- Direkte Integration in CVSS-basierte Prozesse ist möglich.



Quelle: https://xkcd.com/927/

VORSTELLUNG CLOUD SECURITY SCORING

Vorbemerkungen zum Scoring-System

- Es soll ermöglichen, Schwachstellen
  - zu charakterisieren,
  - ihre verschiedenen Eigenschaften über Metriken zu erfassen und
  - ihren Schweregrad zu approximieren und quantitativ zu bewerten.
- Allgemeine Verwendung des Begriffs *Bedrohungsakteur* (anstelle von *„Angreifer“*), nicht auf Menschen beschränkt.
- Bei verschiedenen Bedrohungsakteuren soll zunächst ein Score für jede Gruppe einzeln berechnet werden, für die Gesamtbewertung der Schwachstelle gilt der höchste Score.
- Bewertung berücksichtigt Umgebung, Schwachstellen werden dennoch individuell bewertet.
- Verkettung von miteinander verbundenen Schwachstellen ist möglich.

Cloud Security Scoring (CS2)

Exploitability Metrics

- Threat Actor
- Ease of Exploit
- Remediation Level

Impact Metrics

- Confidentiality Impact
- Integrity Impact
- Availability Impact
- Scope
- Potential Spread
- Business Impact

Setting Effectiveness

- Setting Effectiveness

Übersicht Metriken

- **Exploitability Metrics**
  Wie ausnutzbar ist die Schwachstelle? Wie speziell sind die Zugangsvoraussetzungen? Wie aufwendig ist die Ausnutzung? Wie effektiv sind die getroffenen Gegenmaßnahmen?
- **Impact Metrics**
  Welche technischen und wirtschaftlichen Auswirkungen gibt es?
- **Setting Effectiveness**
  Wie stark wird die Verwundbarkeit durch die Behebung der Schwachstelle mitigiert?

Cloud Security Scoring (CS2)

Exploitability Metrics

- Threat Actor
- Ease of Exploit
- Remediation Level

Impact Metrics

- Confidentiality Impact
- Integrity Impact
- Availability Impact
- Scope
- Potential Spread
- Business Impact

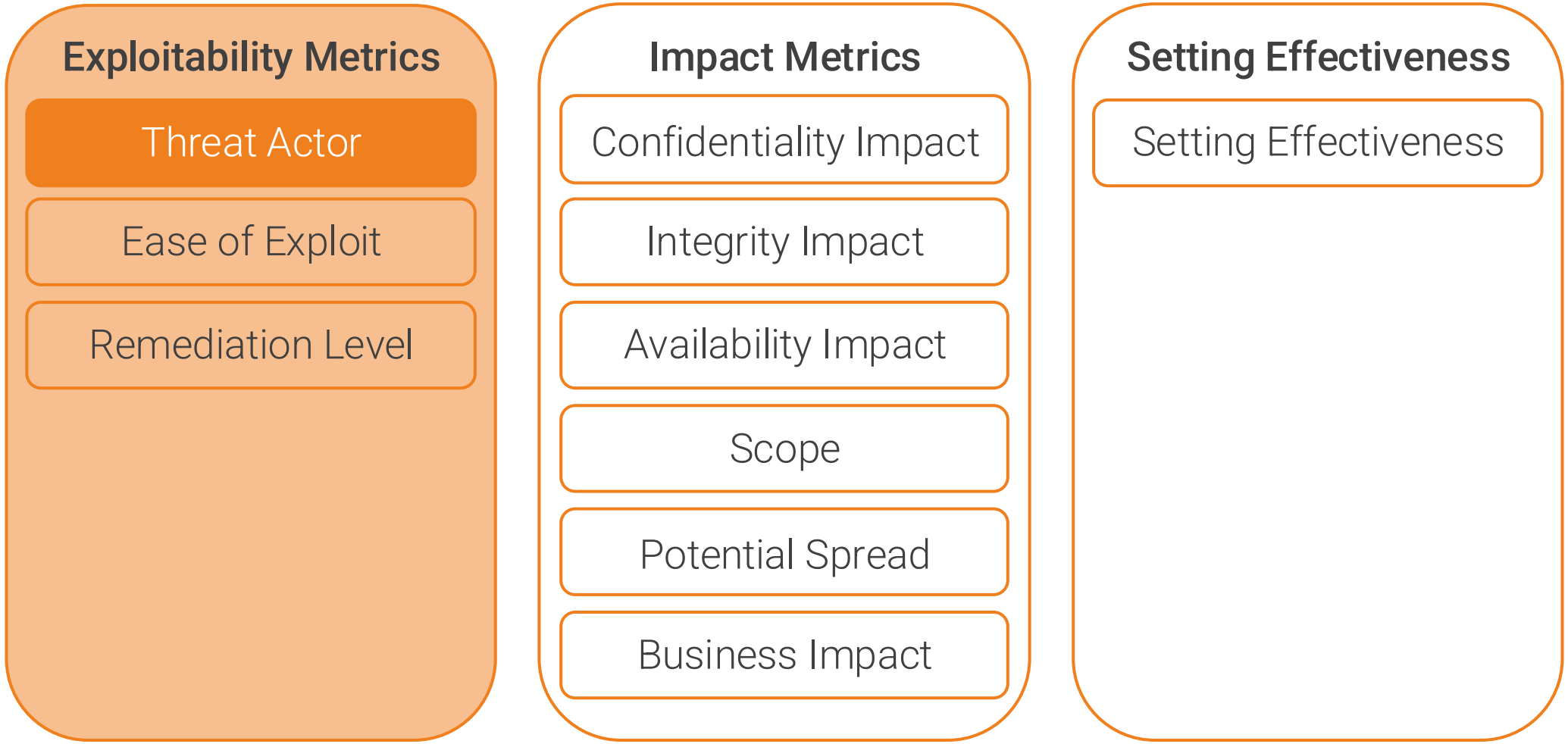
Setting Effectiveness

- Setting Effectiveness

Exploitability Metrics

- Threat Actor
  - Erfasst die Größe der Gruppe der betrachteten Bedrohungsakteure.
- Ease of Exploit
  - Erfasst den erforderlichen Aufwand zur Ausnutzung der Schwachstelle.
- Remediation Level
  - Erfasst Eigenschaften der Umgebung, die eine Ausnutzung erschweren oder verhindern.

Cloud Security Scoring (CS2)



Exploitability Metrics: Threat Actor

- Erfasst die Größe der Gruppe der betrachteten Bedrohungsakteure.
- Bei Unklarheit sollte allgemeiner die Wahrscheinlichkeit für mindestens einen Ausnutzungsversuch innerhalb eines Jahres bewertet werden.
- Sollte die Ausnutzung der Schwachstelle in mehreren Schritten erfolgen, an denen potenziell verschiedene Bedrohungsakteure beteiligt sind, so ist der Wert für die kleinste der verschiedenen Gruppen von Bedrohungsakteuren zu verwenden.

Wert	Beschreibung
Individual	Die relevante Gruppe von Bedrohungsakteuren besteht aus <= 3 Personen.
Small Number of People	Die relevante Gruppe von Bedrohungsakteuren ist stark eingeschränkt. Gruppen von etwa 10 Personen fallen in diese Kategorie.
Limited Number of People	Die relevante Gruppe von Bedrohungsakteuren ist zwar begrenzt, aber umfasst eine größere Anzahl an Personen. Gruppen von etwa 40 Personen fallen in diese Kategorie.
Anyone	Die relevante Gruppe von Bedrohungs-akteuren ist entweder uneingeschränkt (wie z.B. jeder Internetnutzer) oder so groß, dass mit mindestens einem Ausnutzungsversuch inner-halb eines Jahres gerechnet werden muss.

Cloud Security Scoring (CS2)

Exploitability Metrics

- Threat Actor
- **Ease of Exploit**
- Remediation Level

Impact Metrics

- Confidentiality Impact
- Integrity Impact
- Availability Impact
- Scope
- Potential Spread
- Business Impact

Setting Effectiveness

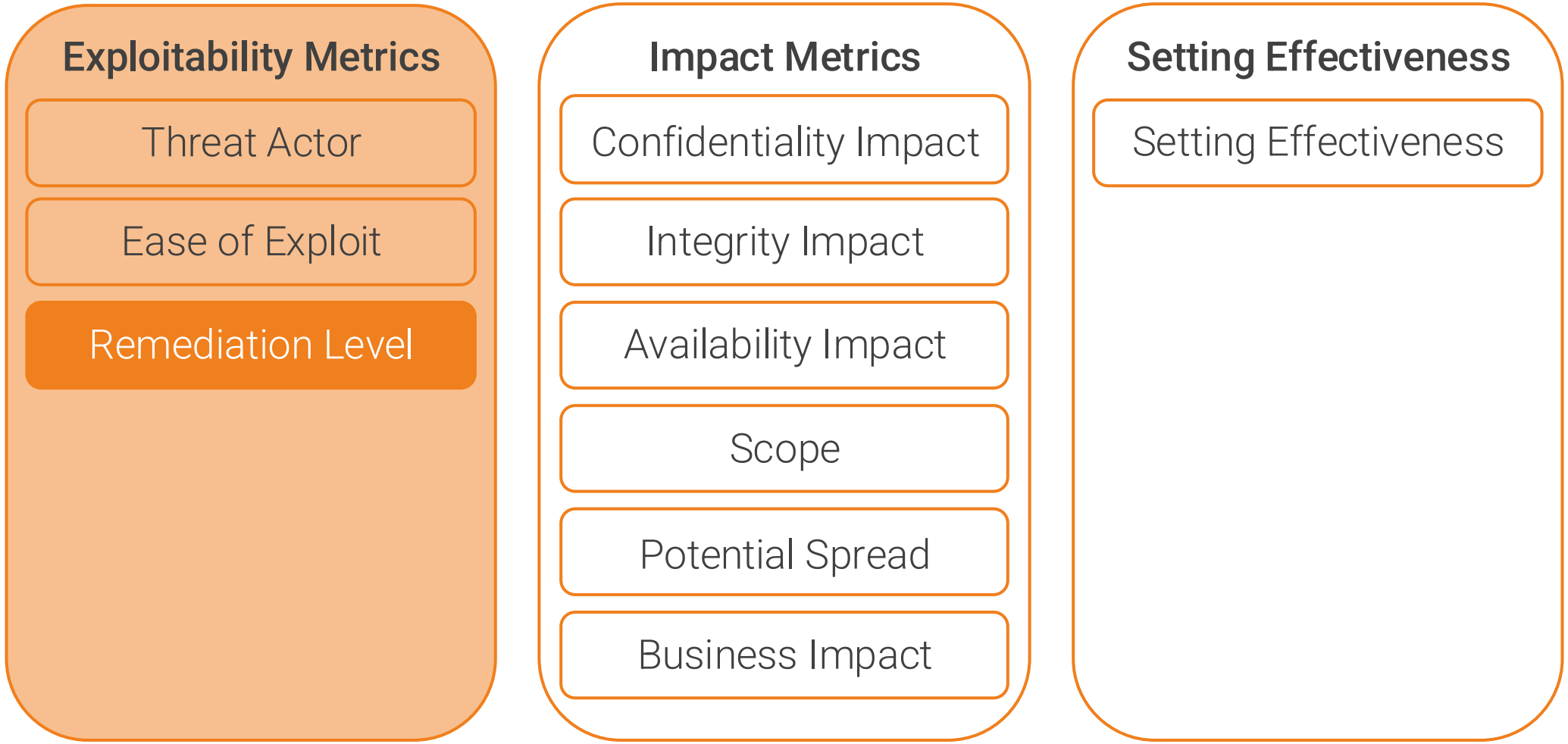
- Setting Effectiveness

Exploitability Metrics: Ease of Exploit

- Erfasst den Aufwand der Ausnutzung der Schwachstelle. Bei externen Bedrohungsakteuren umfasst der Aufwand u.U. auch den geschätzten Aufwand, initialen Zugriff zu erlangen.
- So weit wie möglich wird die Schwachstelle bzw. der Angriffspfad isoliert von der restlichen Umgebung betrachtet. Mitigierende Maßnahmen, die an anderer Stelle getroffen werden, werden in dieser Metrik nicht erfasst (hierfür gibt es die Metrik Remediation Level).

Wert	Beschreibung
Impractical	Die Ausnutzung erfordert einen sehr hohen Aufwand des Bedrohungsakteurs oder grob fahrlässiges Handeln auf Seiten der Opfer. Dass ein Ausnutzungsversuch zum Schadensfall führt ist daher in der Regel nicht zu erwarten.
Hard	Der Aufwand der Ausnutzung wird durch gezielte und weitreichende Maßnahmen deutlich erhöht.
Feasible	Das Ausnutzen erfordert einen signifikanten Aufwand. Bedrohungsakteuren, die bereit sind diesen Aufwand aufzubringen, gelingt es jedoch mit hoher Wahrscheinlichkeit die Schwachstelle ausnutzen.
Trivial	Das Ausnutzen der Schwachstelle erfordert keinen oder nur einen sehr geringen Aufwand.

Cloud Security Scoring (CS2)

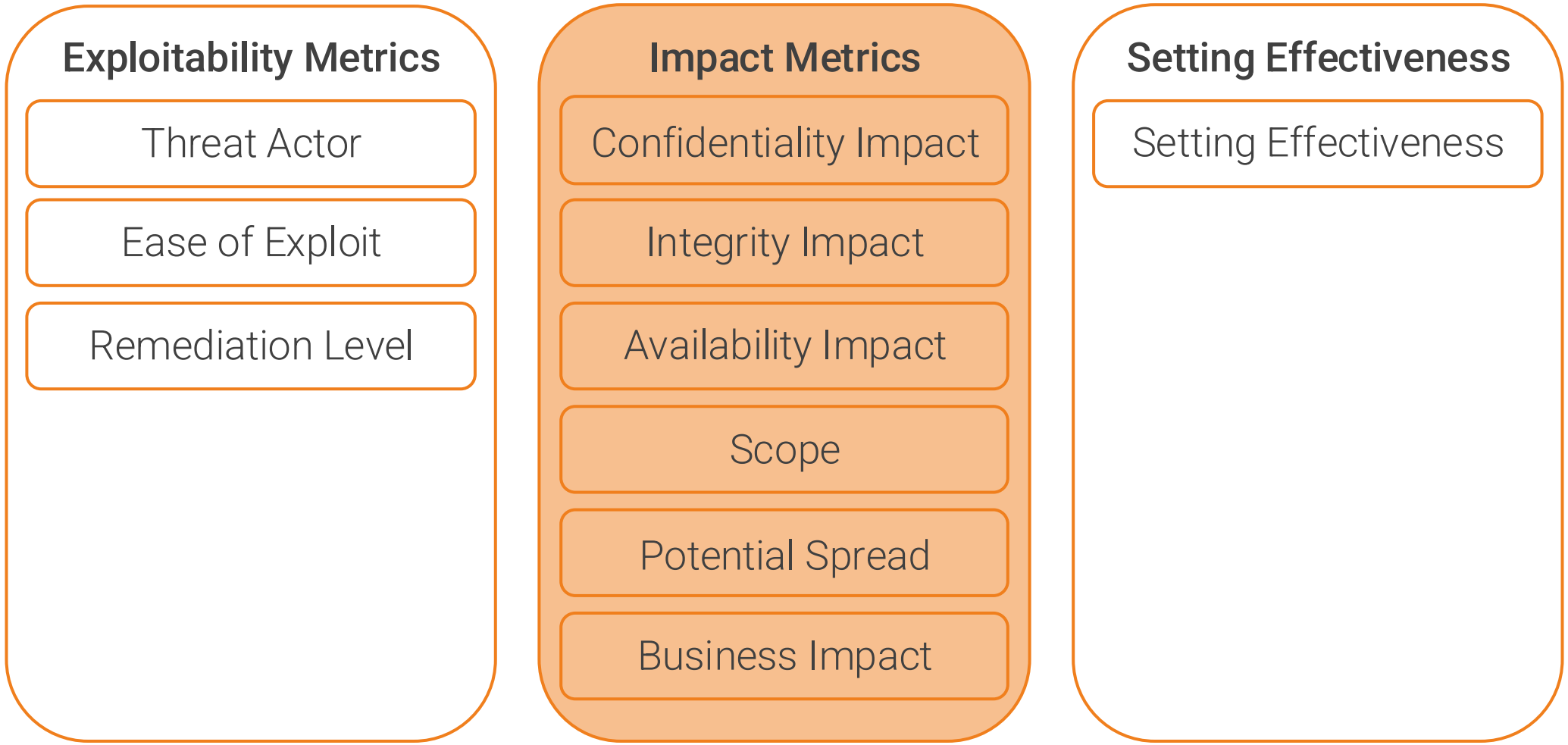


Exploitability Metrics: Remediation Level

- Diese Metrik erfasst Eigenschaften der Umgebung, die eine Ausnutzung erschweren oder verhindern.
- Außerdem werden Eigenschaften der Umgebung berücksichtigt, die die Auswirkungen einer Ausnutzung abschwächen.
- In dieser Metrik werden ausschließlich Eigenschaften berücksichtigt, die nicht in die Bewertung von Ease of Exploit eingeflossen sind.

Wert	Beschreibung
Complete	Aufgrund von Eigenschaften der Umgebung ist die Ausnutzung der Schwachstelle im aktuellen Zustand der Umgebung nicht möglich. Die gesamte Bewertung der Schwachstelle wird durch diese Einstufung stark verringert, sie kann aber größer als 0 sein.
Sound	Die Ausnutzung der Schwachstelle in der Umgebung ist nur schwer möglich oder alle Auswirkungen werden nahezu vollständig aufgehoben.
Indirect	Es ist unwahrscheinlich, dass in der Umgebung ein Bedrohungsakteur die Schwachstelle ausnutzt und dadurch relevante Auswirkungen entstehen.
Limited	In der Umgebung ist die Ausnutzung der Schwachstelle erschwert oder einem Teil der Auswirkungen wird entgegengewirkt. Die Eigenschaften sind jedoch nicht weitreichend genug.
None	In dieser Umgebung existieren keine Eigenschaften, die die Ausnutzung bedeutend erschweren.

Cloud Security Scoring (CS2)



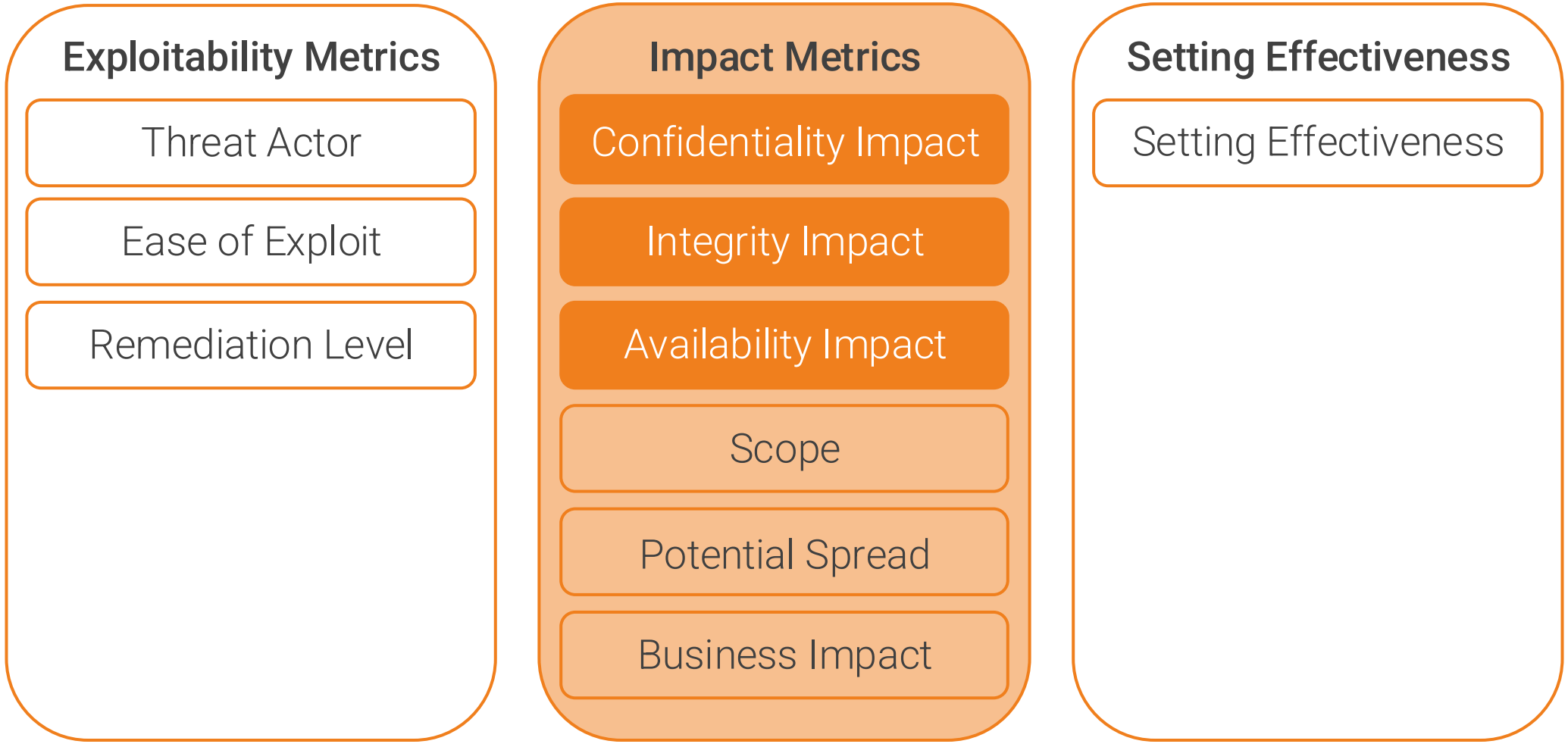
Impact Metrics

- [Confidentiality | Integrity | Availability] Impact
  - Erfasst den Grad der absehbaren direkten Auswirkung auf die [Vertraulichkeit | Integrität | Verfügbarkeit] eines Assets, die sich aus einem Vorfall ergeben, bei dem die Schwachstelle ausgenutzt wird.
- Scope
  - Erfasst Umfang der Assets, deren [Vertraulichkeit | Integrität | Verfügbarkeit] betroffen ist.
- Potential Spread
  - Erfasst die Größe des Bereichs, der durch Ausnutzung der Schwachstelle erreichbar wird, dessen Ressourcen aber nicht direkt betroffen sind.
- Business Impact
  - Erfasst den Umfang der wirtschaftlichen Auswirkungen.

Impact Metrics

- Innerhalb der Impact Metrics wird der Grad der absehbaren direkten Auswirkung der Ausnutzung erfasst. Es liegt im Ermessen des Analysten, welche Auswirkungen absehbar direkt aus der Ausnutzung folgen. Die Auswirkungen sollen aber auf das betroffene Asset bezogen sein und keinen weitergehenden Angriff erfordern. Wenn der Bedrohungsakteur durch die Ausnutzung der Schwachstelle Berechtigungen erlangt, mit denen er auf Ressourcen zugreifen oder sie konfigurieren kann, sollen die durch den Zugriff oder die Veränderung entstehenden Auswirkungen zu den absehbar direkten Auswirkungen gezählt werden.
- Das primär betroffene Asset kann die Komponente sein, die die Schwachstelle enthält, in einigen Fällen ist sie es aber nicht: Das primäre Asset ist das Objekt von Wert, durch dessen Kompromittierung ein Schaden entstehen kann.

Cloud Security Scoring (CS2)

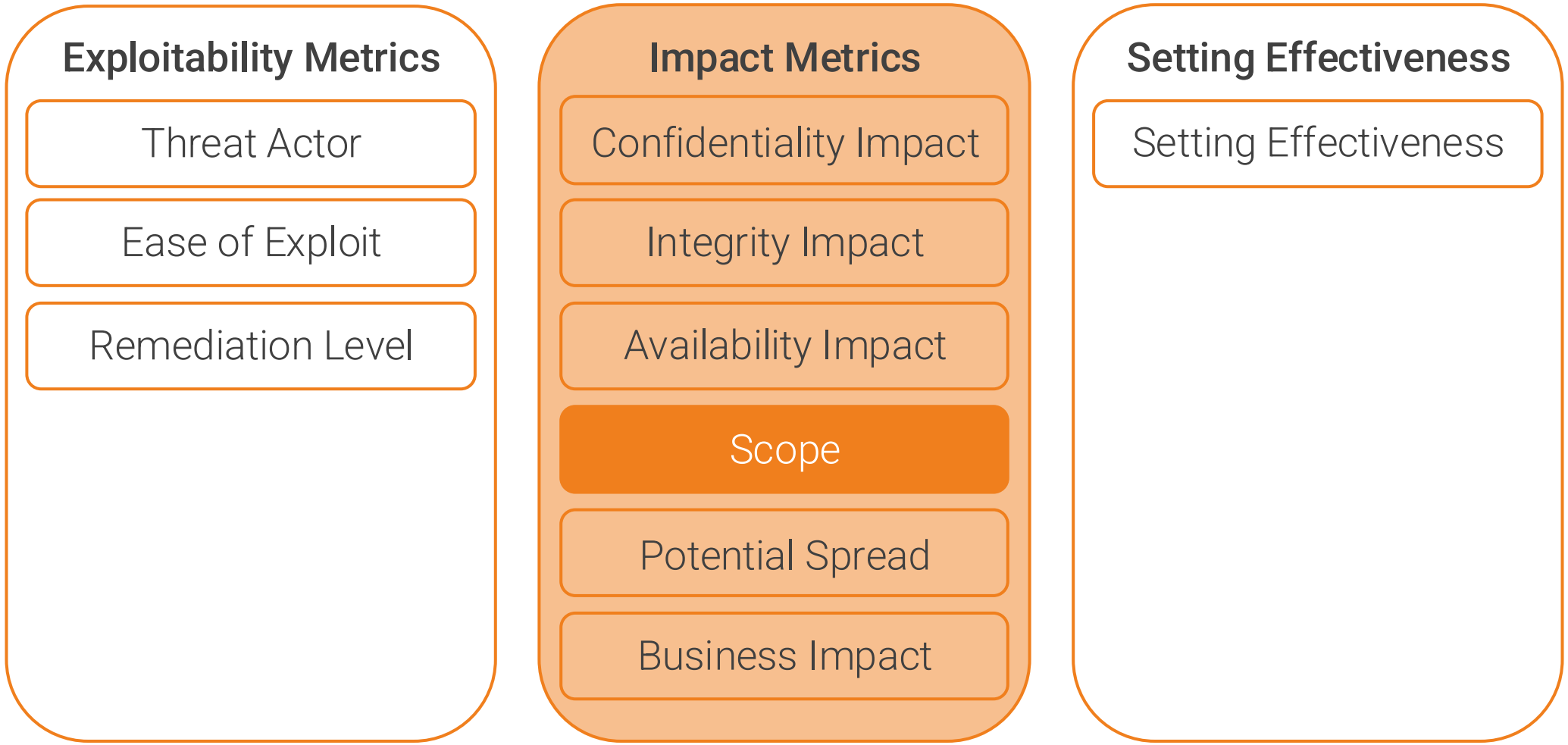


Impact Metrics: [Confidentiality | Integrity | Availability] Impact

- Diese Metrik erfasst den Grad der absehbaren direkten Auswirkung auf die [Vertraulichkeit | Integrität | Verfügbarkeit] eines Assets, die sich aus einem Vorfall ergeben, bei dem die Schwachstelle ausgenutzt wird.
- Diese Metrik ist ohne die Metriken *"Scope"* und *"Setting Effectiveness"* nicht vollständig. Über Scope wird der Umfang der betroffenen Ressourcen berücksichtigt. Über Setting Effectiveness wird erfasst, wie sehr das untersuchte Bedrohungsszenario durch das Beheben der Schwachstelle mitigiert wird.

Wert	Beschreibung
None	Für das betroffene Asset entsteht keine Auswirkung auf die [Vertraulichkeit | Integrität | Verfügbarkeit].
Low	Der Grad der Auswirkungen auf die [Vertraulichkeit | Integrität | Verfügbarkeit] des betroffenen Assets ist gering. Bei Auswirkungen auf die Verfügbarkeit ist das der Fall, wenn die Verfügbarkeit nur kurzzeitig verletzt ist. Wenn Angreifer keine Kontrolle darüber haben, welche Daten sie kompromittieren können, ist dieser Wert ebenfalls zu wählen.
High	Der Grad der Auswirkung auf die [Vertraulichkeit | Integrität | Verfügbarkeit] des betroffenen Assets ist hoch.

Cloud Security Scoring (CS2)

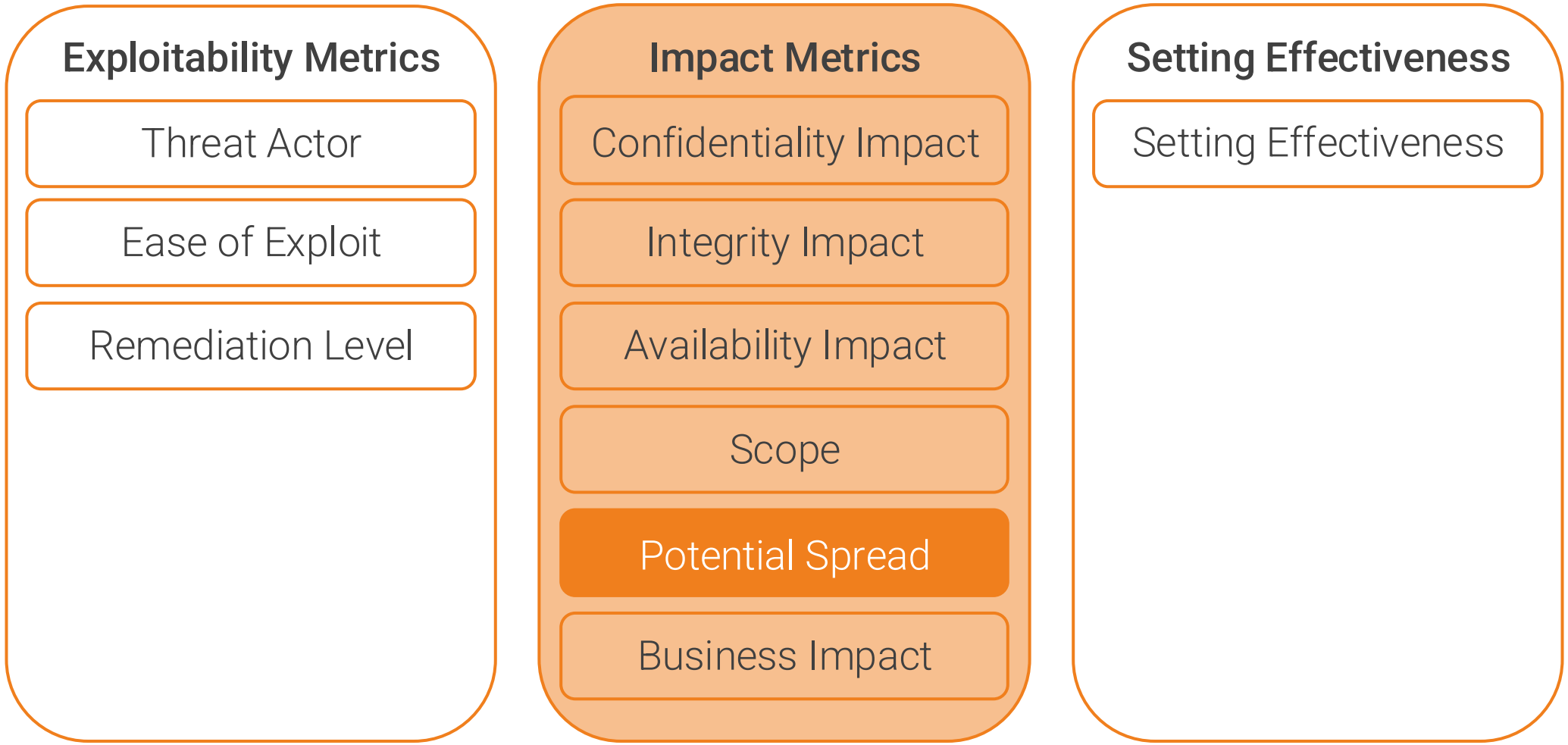


Impact Metrics: Scope

- Die Metriken [Confidentiality | Integrity | Availability] Impact erfassen die Auswirkungen bezüglich eines betroffenen Assets. Der Umfang der Assets, für die die dort getroffenen Bewertungen gelten, wird über diese Metrik erfasst.
- Der Umfang bezieht sich dabei möglichst auf die Anzahl der betroffenen Assets und die Menge der betroffenen Daten, bezieht aber auch das Verhältnis zur gesamten Cloud-Umgebung mit ein.

Wert	Beschreibung
Narrow	Der Umfang ist sehr gering. Nur ein Asset oder einzelne Daten sind betroffen.
Low	Der Umfang ist gering. Nur sehr wenige Assets oder wenige Daten sind betroffen.
Moderate	Der Umfang ist moderat. Mehrere Assets oder eine größere Menge an Daten sind betroffen.
High	Der Umfang ist hoch. Viele Assets sind betroffen, die einen nennenswerten Anteil der Cloud-Umgebung ausmachen. Alternativ ist eine große Menge an Daten betroffen, wie beispielsweise alle Daten einer Datenbank.
Extensive	Der Umfang ist sehr hoch. Ein Großteil der Cloud-Umgebung und/oder eine sehr große Datenmenge ist betroffen.

Cloud Security Scoring (CS2)

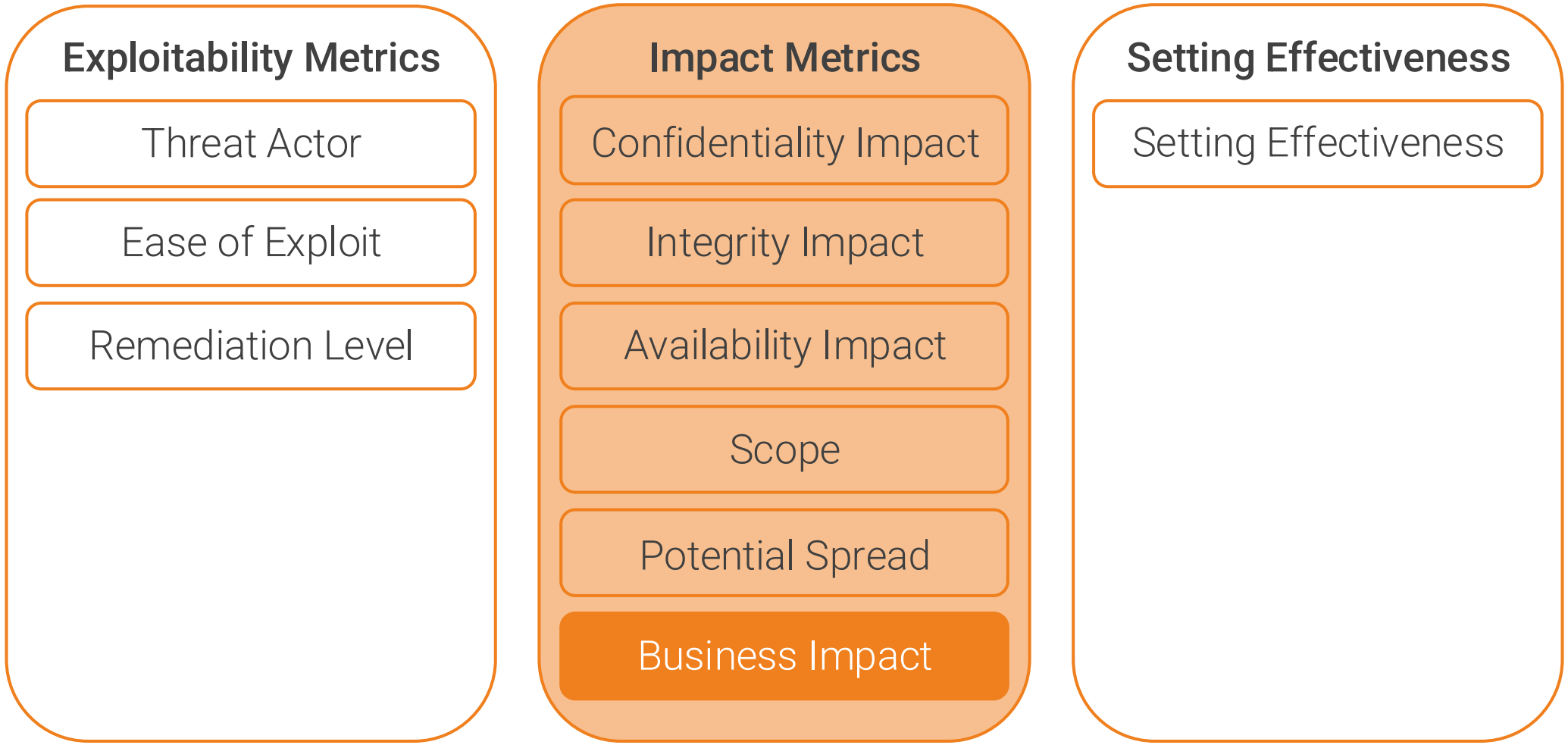


Impact Metrics: Potential Spread

- Diese Metrik erfasst die Größe des Bereichs, der durch Ausnutzung der Schwachstelle erreichbar wird, dessen Ressourcen aber nicht direkt betroffen sind.
- Es wird nur der erreichbare Bereich einbezogen, der nicht bereits über die Metriken [Confidentiality | Integrity | Availability] Impact und Scope berücksichtigt wird.
- Alternativ kann es auch berücksichtigt werden, wenn durch die Schwachstelle detaillierte Informationen über die Cloud-Umgebung erlangt werden können.
- Ein Angreifer, der die dafür notwendigen Zugangsvoraussetzungen erfüllt, kann von der Schwachstelle profitieren und Ressourcen innerhalb dieses Bereichs angreifen. Ziel der Metrik ist es, die indirekten Auswirkungen zu approximieren.

Wert	Beschreibung
None	Ein Angreifer kann nicht von der Schwachstelle profitieren, um weitere Ressourcen zu erreichen.
Limited	Ein Angreifer kann von der Schwachstelle profitieren, um weitere Ressourcen zu erreichen. Die Anzahl der Ressourcen ist jedoch sehr gering und der Bereich in denen sie vorliegen eingegrenzt.
Moderate	Ein Angreifer kann von der Schwachstelle profitieren und einen zusammenhängenden Bereich erreichen, in dem mehrere Ressourcen vorliegen.
High	Ein Angreifer kann von der Schwachstelle profitieren und mehrere Bereiche der Cloud-Umgebung oder verbundener Umgebungen erreichen.

Cloud Security Scoring (CS2)

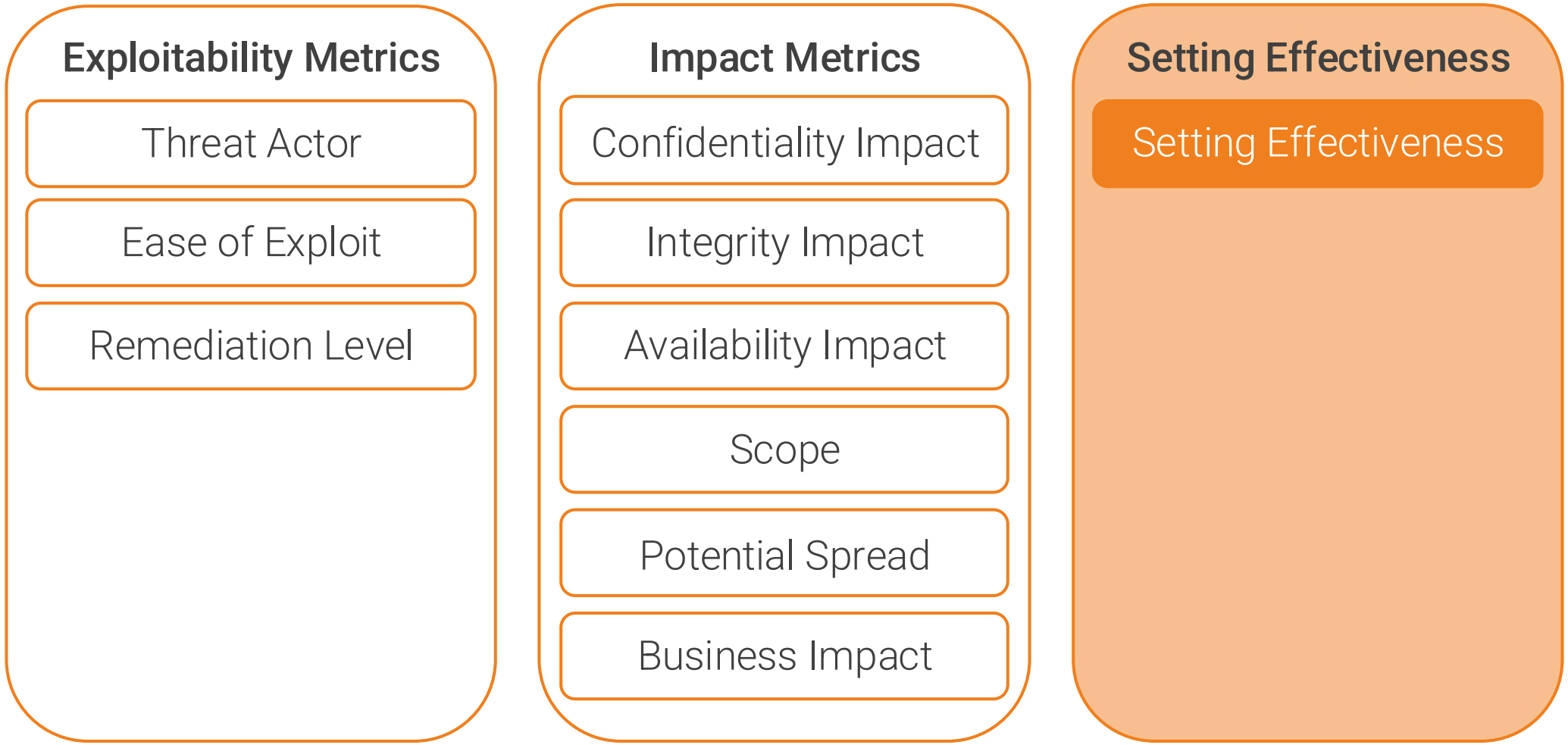


Impact Metrics: Business Impact

- Diese Metrik erfasst den Umfang der wirtschaftlichen Auswirkungen auf die verantwortliche Organisation. Für die Bewertung ist es erforderlich, den Verwendungszweck der betrachteten Cloud-Umgebung und den Wert der betroffenen Assets zu kennen. In der Bewertung sollten die direkten und indirekten Schäden berücksichtigt werden, die der Organisation entstehen, die für die Cloud-Umgebung verantwortlich ist.
- Neben den Werten, um den Umfang der wirtschaftlichen Auswirkungen zu beschreiben, gibt es den Wert *"Not Defined"*. Dieser Wert kann gewählt werden, wenn die wirtschaftlichen Auswirkungen mit den vorliegenden Informationen nicht bestimmbar sind. In diesem Fall werden die Auswirkungen über die vorangegangenen Metriken der Impact Metrics charakterisiert und die Schwere der Schwachstelle auf diese Weise approximiert. Wenn in dieser Metrik hingegen ein Wert ungleich *"Not Defined"* gewählt wird, werden die anderen Metriken der Impact Metrics für die Berechnung der approximierten Schwere nicht mehr verwendet.

Wert	Beschreibung
Negligible	Im Fall einer erfolgreichen Ausnutzung entstehen keine oder keine nennenswerten wirtschaftlichen Auswirkungen.
Low	Die im Fall einer erfolgreichen Ausnutzung entstehenden wirtschaftlichen Auswirkungen sind gering.
Medium	Die im Fall einer erfolgreichen Ausnutzung entstehenden wirtschaftlichen Auswirkungen sind ernst zu nehmen, stellen aber keine Gefahr für die Organisation dar.
High	Die im Fall einer erfolgreichen Ausnutzung entstehenden wirtschaftlichen Auswirkungen sind so hoch, dass es einen deutlichen Effekt auf die jährliche Bilanz gibt.
Critical	Die im Fall einer erfolgreichen Ausnutzung entstehenden wirtschaftlichen Auswirkungen sind so hoch, dass die Existenz der Organisation gefährdet ist.
Not Defined	Die Metrik wird nicht verwendet. Die Auswirkungen werden allein durch die vorangegangenen Metriken der Impact Metrics bestimmt und beschränken sich daher auf die technischen Auswirkungen.

Cloud Security Scoring (CS2)



Setting Effectiveness

Erfasst, wie stark die Verwundbarkeit bezüglich des über die anderen Metriken charakterisierten Bedrohungsszenarios durch die Behebung der Schwachstelle mitigiert wird.

Wert	Beschreibung
Limited	Die Behebung der Schwachstelle verringert die Verwundbarkeit geringfügig, indem sie den Aufwand für den Bedrohungsakteur leicht erhöht oder die Auswirkungen in einigen Fällen verringert.
Indirect	Die Behebung der Schwachstelle verringert die Verwundbarkeit deutlich. Dennoch bleibt das Bedrohungsszenario in weiten Teilen unverändert bestehen.
Adequate	Die Behebung der Schwachstelle behebt die Verwundbarkeit bezüglich der betrachteten Bedrohung nicht vollständig, ist aber ein angemessenes Mittel, um ihr zu begegnen.
Complete	Die Behebung der Schwachstelle verhindert das Eintreten des Bedrohungsszenarios vollständig.
Not Applicable	Die Metrik ist auf die betrachtete Schwachstelle nicht anwendbar. Die Verwendung dieses Wertes führt zur gleichen Bewertung wie die Einstufung als *"Complete"*.

BEISPIELE AUS DER PRAXIS

Praxisbeispiel: Public Storage

- „Klassiker“ im Bereich Cloud Security
- Konfiguration der Policies für Speicherservices wie AWS S3 oder Azure Blob Storage ermöglicht (unabsichtlich) öffentlichen Zugriff.
- Jeder Internetnutzer hat damit direkten Lesezugriff auf den Speicher.
- Änderung der Policy z.B. bei AWS S3 zu „Block public access“ verhindert öffentlichen Zugriff.

Bewertung (berechnet)	
Threat Actor	
Ease of Exploit	
Remediation Level	
Confidentiality Impact	
Integrity Impact	
Availability Impact	
Scope	
Potential Spread	
Business Impact	
Setting Effectiveness	

Praxisbeispiel: Public Storage

- „Klassiker“ im Bereich Cloud Security
- Konfiguration der Policies für Speicherservices wie AWS S3 oder Azure Blob Storage ermöglicht (unabsichtlich) öffentlichen Zugriff.
- Jeder Internetnutzer hat damit direkten Lesezugriff auf den Speicher.
- Änderung der Policy z.B. bei AWS S3 zu „Block public access“ verhindert öffentlichen Zugriff.

Bewertung (berechnet)	Critical (10)
Threat Actor	Anyone
Ease of Exploit	Trivial
Remediation Level	None
Confidentiality Impact	High
Integrity Impact	None
Availability Impact	None
Scope	High
Potential Spread	None
Business Impact	Not Defined
Setting Effectiveness	Complete

Praxisbeispiel: No Phishing-Resistant MFA for Admins

- Administratoren nutzen keine Phishing-resistente Multi-Faktor-Authentifizierung (MFA).
- Kompromittierung administrativer Nutzerkonten ermöglicht in meisten Fällen vollständige Kompromittierung von Cloud-Umgebungen.
- Nutzung Phishing-resistenter MFA-Methoden wie FIDO2-Security-Token (Hardware wie z.B. YubiKey) reduziert Risiko von Account-Übernahmen bzw. Identitätsdiebstahl sehr stark.

Bewertung (berechnet)	
Threat Actor	
Ease of Exploit	
Remediation Level	
Confidentiality Impact	
Integrity Impact	
Availability Impact	
Scope	
Potential Spread	
Business Impact	
Setting Effectiveness	

Praxisbeispiel: No Phishing-Resistant MFA for Admins

- Administratoren nutzen keine Phishing-resistente Multi-Faktor-Authentifizierung (MFA).
- Kompromittierung administrativer Nutzerkonten ermöglicht in meisten Fällen vollständige Kompromittierung von Cloud-Umgebungen.
- Nutzung Phishing-resistenter MFA-Methoden wie FIDO2-Security-Token (Hardware wie z.B. YubiKey) reduziert Risiko von Account-Übernahmen bzw. Identitätsdiebstahl sehr stark.

Bewertung (berechnet)	Medium (5.8)
Threat Actor	Anyone
Ease of Exploit	Hard
Remediation Level	None
Confidentiality Impact	High
Integrity Impact	High
Availability Impact	High
Scope	Extensive
Potential Spread	High
Business Impact	Not Defined
Setting Effectiveness	Adequate

Praxisbeispiel: No Outbound Traffic Control

- Public Clouds (z.B. AWS, Azure, GCP) bieten mehrere Arten von Network Security Controls (NSC), um Datenflüsse zu steuern.
- Häufig werden Datenflüsse nur an einer Stelle über ein NSC gesteuert, ausgehender Datenverkehr wird noch häufiger gar nicht oder zu wenig reglementiert.
- Im Sinne von „defense in depth“ sollten Datenflüsse an verschiedenen Stellen und durch mehrere NSC gesteuert werden, auch ausgehender Datenverkehr ist auf das Notwendige zu beschränken.

Bewertung (berechnet)	
Threat Actor	
Ease of Exploit	
Remediation Level	
Confidentiality Impact	
Integrity Impact	
Availability Impact	
Scope	
Potential Spread	
Business Impact	
Setting Effectiveness	

Praxisbeispiel: No Outbound Traffic Control

- Public Clouds (z.B. AWS, Azure, GCP) bieten mehrere Arten von Network Security Controls (NSC), um Datenflüsse zu steuern.
- Häufig werden Datenflüsse nur an einer Stelle über ein NSC gesteuert, ausgehender Datenverkehr wird noch häufiger gar nicht oder zu wenig reglementiert.
- Im Sinne von „defense in depth“ sollten Datenflüsse an verschiedenen Stellen und durch mehrere NSC gesteuert werden, auch ausgehender Datenverkehr ist auf das Notwendige zu beschränken.

Bewertung (berechnet)	Low (2.3)
Threat Actor	Small Number of People
Ease of Exploit	Trivial
Remediation Level	None
Confidentiality Impact	High
Integrity Impact	None
Availability Impact	None
Scope	Extensive
Potential Spread	None
Business Impact	High
Setting Effectiveness	Adequate

ZUSAMMEN-FASSUNG

Zusammenfassung

Vorstellung des Cloud Security Scoring (CS2):

System zur Bewertung von Schwachstellen in der Konfiguration von Cloud Services

Mit CS2 ist es möglich:

- Schwachstellen zu charakterisieren und ihre Eigenschaften über Metriken zu erfassen,
- ihren Schweregrad zu approximieren und quantitativ zu bewerten,
- die Umgebung und den Business Impact zu berücksichtigen,
- miteinander verbundene Schwachstellen zu verketten und
- das System in bestehende Prozesse ähnlich wie CVSS zu integrieren.

FRAGEN UND DISKUSSION

Vielen Dank für die Aufmerksamkeit

more security. usd

Dr. Kai Schubert

usd HeroLab

Cloud Security Team

E-Mail: kai.schubert@usd.de
Telefon: +49 151 29268952

more security. usd

usd AG

Frankfurter Str. 233, Haus C1
63263 Neu-Isenburg

Telefon: +49 6102 8631-190
E-Mail: vertrieb@usd.de

usd HeroLab

www.usd.de
https://herolab.usd.de