DATAGROUP

Begleitdokument Security Services Boarding-Fragebogen

SOC-Hochschulen.NRW

IT’s that simple.

DATAGROUP

Inhaltsverzeichnis

Ziel dieses Dokumentes

Dem Projektteam ist bewusst, dass die Fragen des Fragebogens nicht durch einen Fachbereich alleine beantwortet werden können. Zwecks leichterer Bearbeitung haben wir Ihnen dieses Begleitdokument erstellt, welches sämtliche Fragen des Fragebogens in einem Dokument konsolidiert und sich somit eignet, dass Sie es an die internen relevanten Fachbereiche verteilen können.

Somit soll dieses Dokument Sie dabei unterstützen, die erforderlichen Informationen seitens Ihrer Hochschule zu sammeln und im Nachgang in dem Security Services Boarding-Fragebogen online ausfüllen zu können.

Security Services Boarding-Fragebogens - Einleitungstext

Sehr geehrte Damen und Herren,

im Rahmen des gemeinsamen Projektes **SOC-Hochschulen .NRW** dürfen wir, als DATAGROUP, Ihnen einen abgestimmten Katalog an IT Security Services anbieten.

Damit wir gemeinsam mit Ihnen die IT Security Services in Betrieb nehmen können, benötigen wir vorab von Ihnen nähere Informationen und somit Ihre aktive Unterstützung. Dieser Fragebogen ist in zwei wesentliche Kernelemente unterteilt:

1. **Umfang und Zeitpunkt der Serviceimplementierung für Ihre Hochschule**
2. **Nähere Detailinformationen zu Ihrer IT-Umgebung und Organisation.**

Wir möchten Sie bitten, diesen Fragebogen **spätestens 10 Tage** nach Erhalt des Links abzuschließen. Sollten Sie dies zeitlich nicht schaffen, geben Sie bitte eine kurze Rückmeldung an die Projektleitung des SOC-Hochschulen .NRW Konsortiums, Anja Krämer (*anja.kraemer@konlution.de*).

Weitere Information zum Ausfüllen des Fragebogens:

- Versuchen Sie die Fragen, **nach bestem Wissen und Gewissen** auszufüllen.
  Wir haben den Fragebogen so konzipiert, dass wir für den hier drauf folgenden Fokus-Abstimmungen mit Ihnen effizient gestalten können und Sie besser verstehen, welche Informationen wir von Ihnen benötigen. Ihre Antworten sind aber selbstverständlich nicht in "Stein gemeißelt" und können im weiteren Implementierungsverlauf noch angepasst werden!

Wie geht's nach dem Fragebogen weiter?
Nachdem wir Ihre Fragebogen-Antworten erhalten haben, prüfen wir Ihre Antworten und stimmen uns gemeinsam in einzelnen **Fokus-Abstimmungsterminen** (zu ausgewählten Services) über die weiteren Implementierungsschritte ab und beantworten gerne Ihre Fragen.

Vielen Dank für Ihre Mitarbeit!
Ihr SOC-Hochschulen .NRW-Projektteam der DATAGROUP

Weiterführende Informationen

- ***Mehr zum Projekt SOC-Hochschulen .NRW (Projekt-Landingpage)***
  https://www.datagroup.de/soc-hochschulen-nrw/
- **Gemeinsames Projekt SOC-Hochschulen.NRW-Austauschverzeichnis (Projekt-Share)**
  https://datagrouponline.sharepoint.com/sites/DGHB-HSNRW
- ***Mehr über DATAGROUP***
  https://www.datagroup.de/datagroup/its-datagroup/
- ***Mehr zu den DATAGROUP IT-Security Services***
  https://www.datagroup.de/leistungen/it-outsourcing/security-services/

1. Ihre Organisation: Für wen füllen Sie den Fragebogen aus?

Pflichtfrage: Bitte wählen Sie an dieser Stelle die entsprechende Hochschule aus dem bereitgestellten Drop Down-Liste aus.

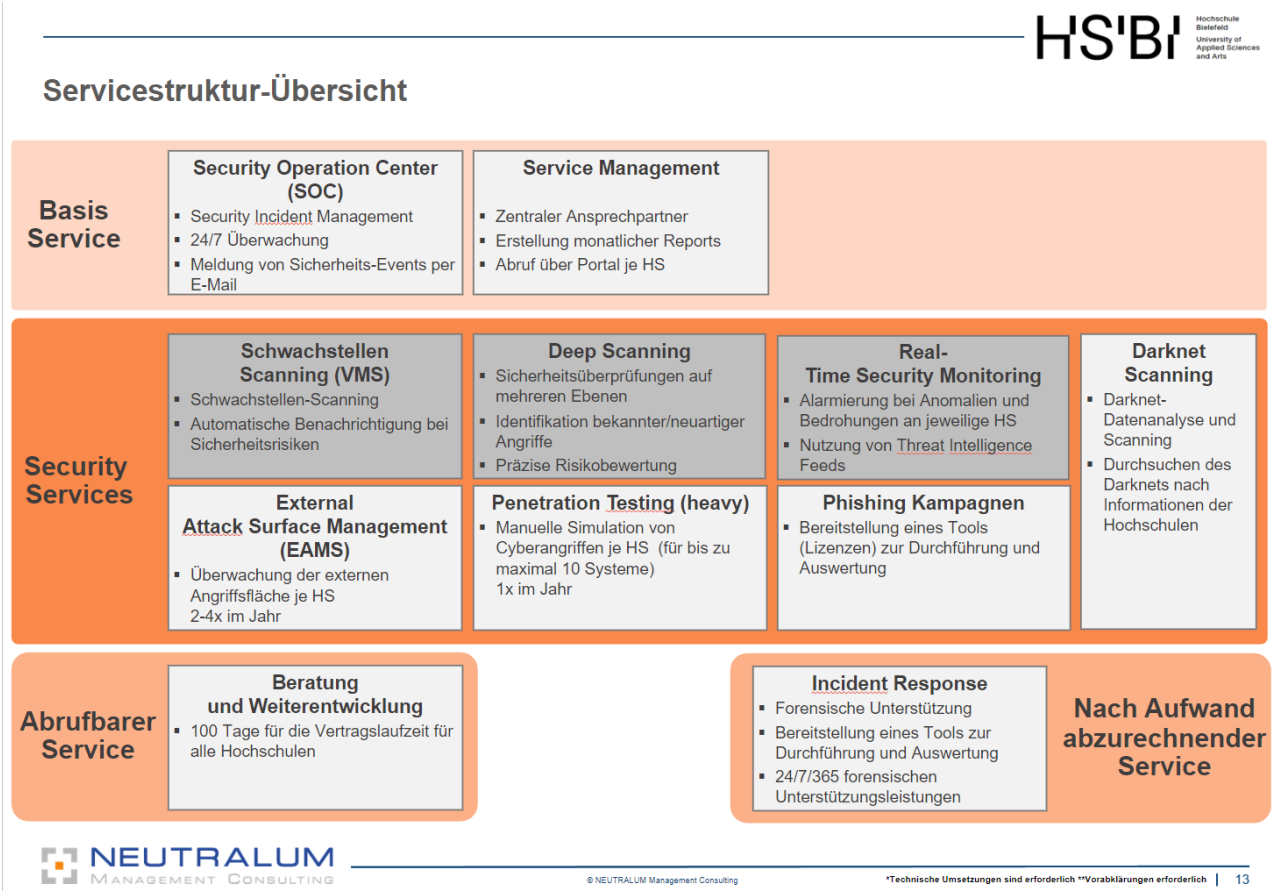
Hinweis: Sollte Ihre Hochschule nicht unter den Auswahlmöglichkeiten auffindbar sein, sprechen Sie uns gerne an!

Umfang und Zeitpunkt der Serviceimplementierung für Ihre Hochschule

Im Rahmen des Projektes SOC-Hochschulen .NRW können Sie aus einen vorab abgestimmten Katalog von IT-Security Services zugreifen. Die einzelnen Services hatten wir Ihnen im Rahmen des gemeinsamen Kick Off-Termins, am 25. Juni 2024 an der Hochschule Bielefeld, näher vorgestellt.

Wir gehen davon aus, dass alle IT-Security Services für alle Hochschulen zum Einsatz kommen. Sollte für Ihre Hochschule das nicht zutreffen, bitten wir dies am Ende dieses Abschnittes (Pkt. 8) näher zu erläutern.

Hinweis: Die Services Security Operations Center (SOC) und Service Management sind essentiell und können daher nicht abgewählt werden.



2. Schwachstellen Scanning (VMS)

Pflichtfrage: Der Schwachstellen Scanning-Service basiert auf einem Vulnerability-Tool, welches darauf ausgelegt ist, Schwachstellen in der IT-Infrastruktur von Hochschulen zu identifizieren, zu bewerten und potenzielle Angriffsflächen aufzuzeigen. Durch kontinuierliches Scannen und Analysieren trägt das System dazu bei, die Sicherheit und Integrität der IT-Umgebung zu gewährleisten und Cyberbedrohungen frühzeitig zu erkennen und zu neutralisieren.

Vorteile für die IT-Sicherheit

- Proaktives Schwachstellenmanagement durch kontinuierliche Identifikation, Bewertung potenziellen Auswirkungen und Aufzeigen von Behebungsmöglichkeiten der Schwachstellen.
- Nachhaltige Verbesserung der IT-Sicherheit durch stetige Verbesserung des gesamten Sicherheitsniveaus.
- Reduzierung von Risiken vor Cyberangriffen durch die frühzeitige Identifikation von Schwachstellen.

Verfügbare Antwortoptionen:

- **JA**, wir wünschen die Implementierung des Schwachstellen Scanning-Services im Rahmen des Projektes bis Ende 2024.
- **JA**, zu einem späteren Zeitpunkt (bitte unter Pkt. 8 näher begründen und frühestmögliches Datum benennen.).
- **NEIN**, grundsätzlich keine Implementierung gewünscht.

3. External Attack Surface Management (EASM)

Pflichtfrage: Das External Attack Surface Management (EASM), hat die Aufgabe, die externe Angriffsfläche der Hochschulen kontinuierlich zu überwachen. Das Ziel ist es, die Risiken von externen Assets zu reduzieren und das gesamte Sicherheitsniveau nachhaltig zu verbessern. Mithilfe von Scan- und Analysemechanismen werden Schwachstellen, Fehlkonfigurationen sowie teilweise unbekannte Assets frühzeitig erkannt und für die Behebung den Hochschulen aufgezeigt, bevor Cyberkriminelle sie ausnutzen können.

Externe Assets umfassen alle digitalen Ressourcen der Hochschule, die über das Internet zugänglich sind, wie Webseiten, Webanwendungen, Cloud-Dienste, extern gehostete Server, DNS-Infrastrukturen, mobile Anwendungen.

Vorteile für die IT-Sicherheit

- Proaktive Reaktion auf die sich verändernde Bedrohungslandschaften.
- Integritätsschutz der digitalen Präsenz der Hochschulen.

Hinweise zu diesem Service

- Für diesen Service müssen Sie die **Einverständniserklärung unseres Partners Locate Risk** unterschreiben.
- *Wir werden diese Form des Penetration Testings erst nach Zeichnung der Einverständniserklärung, vorheriger Terminkoordination und expliziter Freigabe Ihrerseits durchführen.*

Verfügbare Antwortoptionen:

- **JA**, wir wünschen die Implementierung des EASM-Services im Rahmen des Projektes bis Ende 2024.
- **JA**, zu einem späteren Zeitpunkt (bitte unter Pkt. 8 näher begründen und frühestmögliches Datum benennen.).
- **NEIN**, grundsätzlich keine Implementierung gewünscht.

4. Deep Scanning

Pflichtfrage: Der Service Deep Scanning bietet eine tiefgehende Überprüfung hinsichtlich Schwachstellen der jeweiligen dediziert ausgewählten Systeme / Assets. Mit fortschrittlichen Algorithmen werden potenzielle Bedrohungen auf mehreren Ebenen identifiziert, wodurch sowohl bekannte als auch neuartige Angriffe frühzeitig erkannt werden. Die verschiedenen Scan-Profile (intern, extern, authenticated, etc.) ermöglichen es, Schwachstellen und Fehlkonfigurationen in Betriebssystemen, Anwendungen und Netzwerkkomponenten effektiv zu identifizieren. In einem Bericht erhalten die Hochschulen eine Bewertung und Priorisierung des Risikos der gefundenen Schwachstellen sowie Handlungsempfehlungen.

Vorteile für die IT-Sicherheit

- Proaktives Sicherheitsmanagement durch frühzeitige Erkennung von Schwachstellen.
- Verbesserung der Sicherheitslage und Reduzierung potenzieller Auswirkungen von Sicherheitsvorfällen an den Hochschulen
- Integration der Scan-Ergebnisse in das SOAR für eine umfassende Sicherheitsübersicht und -verwaltung.

Hinweise zu diesem Service

- Für diesen Service müssen Sie den Haftungsausschluss Externes Schwachstellenscanning unterzeichnen.

Verfügbare Antwortoptionen:

- **JA**, wir wünschen die Implementierung des Deep Scanning-Services im Rahmen des Projektes bis Ende 2024.
- **JA**, zu einem späteren Zeitpunkt (bitte unter Pkt. 8 näher begründen und frühestmögliches Datum benennen.).
- **NEIN**, grundsätzlich keine Implementierung gewünscht.

5. Penetration Testing (heavy)

Pflichtfrage: Der Penetration Testing (heavy)-Service bietet eine umfassende Sicherheitsprüfung auf Basis von Simulationen realer Angriffsszenarien, um die Widerstandsfähigkeit Ihrer IT-Infrastruktur (Firewalls, Routern und anderen Netzwerkkomponenten) und Webanwendungen (Analyse auf Sicherheitslücken wie SQL-Injection, Cross-Site Scripting (XSS) und andere Schwachstellen) gegenüber potenziellen Angriffen zu gewährleisten. Durch die gezielte Simulation von Angriffsszenarien werden Schwachstellen identifiziert, sodass proaktiv Sicherheitsmaßnahmen ergriffen werden können. Dieser Service ist essenziell für die Erkennung und Behebung von Sicherheitslücken, bevor sie von Angreifern ausgenutzt werden können.

Vorteile für die IT-Sicherheit
Verbesserung der Widerstandsfähigkeit der IT-Infrastruktur durch die Früherkennung und Behebung von Schwachstellen.

- Proaktives Risikomanagement durch die Simulation realer Angriffsszenarien und Identifikation potenzielle Bedrohungen identifiziert.
- Bereitstellung von klaren, benutzerfreundlichen Berichten mit spezifischen Empfehlungen zur Sicherheitsverbesserung gemäß aktuellen Best Practices und Sicherheitsstandards.

Hinweise zu diesem Service

- Wir werden einen Penetration Test (heavy) erst nach Zeichnung des zugehörigen Haftungsausschlusses, vorheriger Terminkoordination und expliziter Freigabe Ihrerseits durchführen.

Verfügbare Antwortoptionen:

- **JA**, wir wünschen die Implementierung des Penetration Testing (heavy)-Services im Rahmen des Projektes bis Ende 2024.
- **JA**, zu einem späteren Zeitpunkt (bitte unter Pkt. 8 näher begründen und frühestmögliches Datum benennen.).
- **NEIN**, grundsätzlich keine Implementierung gewünscht.

6. Darknet Scanning

Pflichtfrage: Der Service Darknet Scanning bietet eine proaktive und umfassende Lösung zur Identifizierung potenzieller Bedrohungen und Risiken im verborgenen Teil des Internets. Durch kontinuierliche Überwachung und Analyse von Darknet-Quellen stärken die Cyberabwehrstrategie und schützen die Hochschulen vor latenten Gefahren.

Es umfasst die Suche nach sicherheitsrelevanten Daten und Inhalten im Darknet wie Benutzerkonten, Keywords und Personen, Informationen zu verdächtigen Aktivitäten, Datenlecks, unbefugten Zugriffe, mögliche Konten-Kompromittierungen sowie IP-Adresse, Domänen, exponierten Personen der Hochschulen.

Vorteile für die IT-Sicherheit

- Proaktive Bedrohungserkennung durch frühzeitige Identifikation und Reaktion potenzieller Bedrohungen aus dem Darknet.
- Stärkung der Cyberabwehrstrategie durch kontinuierliche Überwachung und Analyse.
- Risikominderung durch Reduzierung der Auswirkungen von Sicherheitsvorfällen und Umsetzung schneller Gegenmaßnahmen.

Verfügbare Antwortoptionen:

- **JA**, wir wünschen die Implementierung des Darknet Scanning-Services im Rahmen des Projektes bis Ende 2024.
- **JA**, zu einem späteren Zeitpunkt (bitte unter Pkt. 8 näher begründen und frühestmögliches Datum benennen.).
- **NEIN**, grundsätzlich keine Implementierung gewünscht.

7. Phishing Kampagne

Pflichtfrage: Im Rahmen dieses unmanaged Services werden seitens DATAGROUP Benutzerlizenzen bereitgestellt, mit denen die Hochschulen eigenständig realistische Phishing-Kampagnen entwickeln und durchführen können, um die Reaktionsfähigkeit der Mitarbeitenden auf derartige Bedrohungen zu testen und zu verbessern. Die Umsetzung der Kampagnen erfolgt systemunterstützt und bietet interaktive Trainingsmodule und umfassende Auswertungsmöglichkeiten, um das Sicherheitsbewusstsein nachhaltig zu steigern. Personen, die auf eine simulierte Phishing-E-Mail klicken werden zu einem interaktiven Trainingsmodul weitergeleitet.

Die Lösung bietet grundsätzlich umfassende Integrationsmöglichkeiten, wie beispielsweise die Nutzung von E-Mail-Adressen der Mitarbeitenden für die Kampagnen, sowie Bereitstellung einer Outlook-Integration, mit dem Mitarbeitende verdächtige E-Mails mit einem Klick melden können.

Vorstellbare Vorteile für die IT-Sicherheit

- Verbessertes Sicherheitsbewusstsein durch kontinuierliche Schulungen und realistische Tests.
- Früherkennung und Vermeidung von Phishing-Angriffen durch regelmäßige Kampagnen und Trainings.
- Detaillierte Berichte und Dashboards ermöglichen fundierte Entscheidungen zur Verbesserung der IT-Sicherheit.
- Hohe Flexibilität und Anpassungsfähigkeit der Lösungen und Kampagnen, die den spezifischen Anforderungen der Hochschulen entsprechen.

Verfügbare Antwortoptionen:

- **JA**, wir wünschen die Bereitstellung von *SOPHOS Phish Threat*-Lizenzen im Rahmen des Projektes bis Ende 2024.
- **JA**, zu einem späteren Zeitpunkt (bitte unter Pkt. 8 näher begründen und frühestmögliches Datum benennen.).
- **NEIN**, grundsätzlich keine Implementierung gewünscht.

8. Begründung späterer Starttermin für Services

Sollten Sie für einen der oben genannten Services die (mittlere) Option "***JA**, zu einem späteren Zeitpunkt*" gewählt haben, bitten wir Sie an dieser Stelle um eine kurze Begründung und Nennen des frühestmöglichen Starttermins pro Service.

Antwort als Freitext

Nähere Detailinformationen zu Ihrer IT-Umgebung und Organisation

Im nachfolgenden Abschnitt des Fragebogens benötigen wir von Ihnen organisatorische und technische Detailinformationen, um die Implementierung planen und durchführen zu können

Organisatorische Detailinformationen

Zu Beginn benötigen wir grundsätzliche Angaben zu Ihrer Organisation von Ihnen.

9. Zentrale/r Ansprechpartner

Pflichtfrage*:* Im Rahmen des Projektverlaufs benötigen wir für die gemeinsame Koordination pro Hochschule mindestens einen zentralen Ansprechpartner, den das DATAGROUP-Projektteam kontaktieren wird. Dabei wird es um technische und organisatorische Detailabstimmungen gehen.

Bitte geben Sie an:
- Name, Vorname (Dezernat / Abteilung bzw. ext. Dienstleister, Standort)
- E-Mail-Adresse
- Telefon (optional: Mobiltelefon)

Antwort als Freitext

10. Anzahl der Mitarbeitenden

Bitte geben Sie die relevante Anzahl der IT-Benutzer in Ihrer Hochschule an. Dies umfasst alle Personen in der Verwaltung sowie Lehrkräfte und sonstige Personen, jedoch explizit nicht die Studenten.

Hinweis: Ihrer Rückmeldung nehmen wir als Indikation beispielsweise für die Lizenzbereitstellung von SOPHOS Phish Threat (Phishing Kampagne) oder des Penetrationtests Light (external Attack Surface Management).

Nummerische Antwort

11. Optional: Zentraler technischer Ansprechpartner für Ihre Organisation

Sofern vorhanden, können Sie einen zentralen Zwecks Detailrückfragen z. B. zu Netzwerkthemen

Bitte geben Sie an:
- Name, Vorname (Dezernat / Abteilung bzw. ext. Dienstleister, Standort)
- E-Mail-Adresse
- Telefon (optional: Mobiltelefon)

Antwort als Freitext

12. Optional: Direkter organisatorischer Ansprechpartner für Ihre Organisation

Sofern vorhanden, können Sie uns einen direkten organisatorischen Ansprechpartner benennen, zwecks Detailrückfragen zu z. B. Definition von Meldewegen in Notfallszenarien, Ticketeskalationen, Service Management, etc.).

Bitte geben Sie an:
- Name, Vorname (Dezernat / Abteilung bzw. ext. Dienstleister, Standort)
- E-Mail-Adresse
- Telefon (optional: Mobiltelefon)

Antwort als Freitext

13. Ticket Eröffnung: Benennung von Key Usern für SOC Ticket-Eröffnung

Pflichtfrage: Gemäß des vertraglichen Rahmens dürfen sich in der Betriebsphase nur definierte "Key User", also Personen, die Sie uns vorab kommuniziert haben, an unserem Security Operation Center (SOC) melden. Klassischerweise sind dies Personen, die in der Meldekette eines IT Security-Notfallplans stehen.

Bitte geben Sie an:
- Name, Vorname (Dezernat / Abteilung bzw. ext. Dienstleister, Standort)
- E-Mail-Adresse
- Telefon (optional: Mobiltelefon)

Antwort als Freitext

14. Security Reporting: Benennung zu berechtigenden Personen

Für die bereit zu stellenden Security Services werden wir Ihnen ein Service-Reporting, inkl. Security Dashboard einrichten. Hierzu benötigen wir von Ihrer Seite eine Rückmeldung wen wir auf die bereitzustellenden Reporting-Informationen berechtigen dürfen.

Bitte geben Sie an:
- Name, Vorname
- E-Mail-Adresse

Antwort als Freitext

Meldewege

Eine effiziente Kommunikation und Dokumentation von identifizierten Anomalien und Notfällen ist wichtig, da es im Fall der Fälle zeitnahes Handeln entscheidend ist. Aus diesem Grund ist ein Melde- und Prozessweg im Laufe des Projektes gemeinsam zu definieren. Idealerweise erfolgt die Kommunikation über ein Ticketsystem. Seitens DATAGROUP wird ein Ticketsystem genutzt, welches mit Ihrem Ticketsystem (sofern vorhanden) per E-Mail-Schnittstelle verbunden werden kann.

15. Welche E-Mail-Adresse soll für den Meldeweg vorgesehen werden (operativer Meldeweg- SOC)?

Pflichtfrage.

Antwort als Freitext

Technische Detailinformationen – Netzwerk

Wir werden in dem DATAGROUP-Rechenzentrum hochverfügbare Instanzen für Ihre IT Security Services bereitstellen, um diese für Sie zu betreiben. Damit die Security Services Ihre IT-Umgebungsdaten überwachen kann, benötigen wir zum einen ein besseres Verständnis über Ihre IT-Umgebung und zum anderen müssen wir eine netzwerkseitige Verbindung zwischen Ihrer IT-Umgebung und unserem Rechenzentrum aufbauen.

Koppelung per IPSec-Tunnel

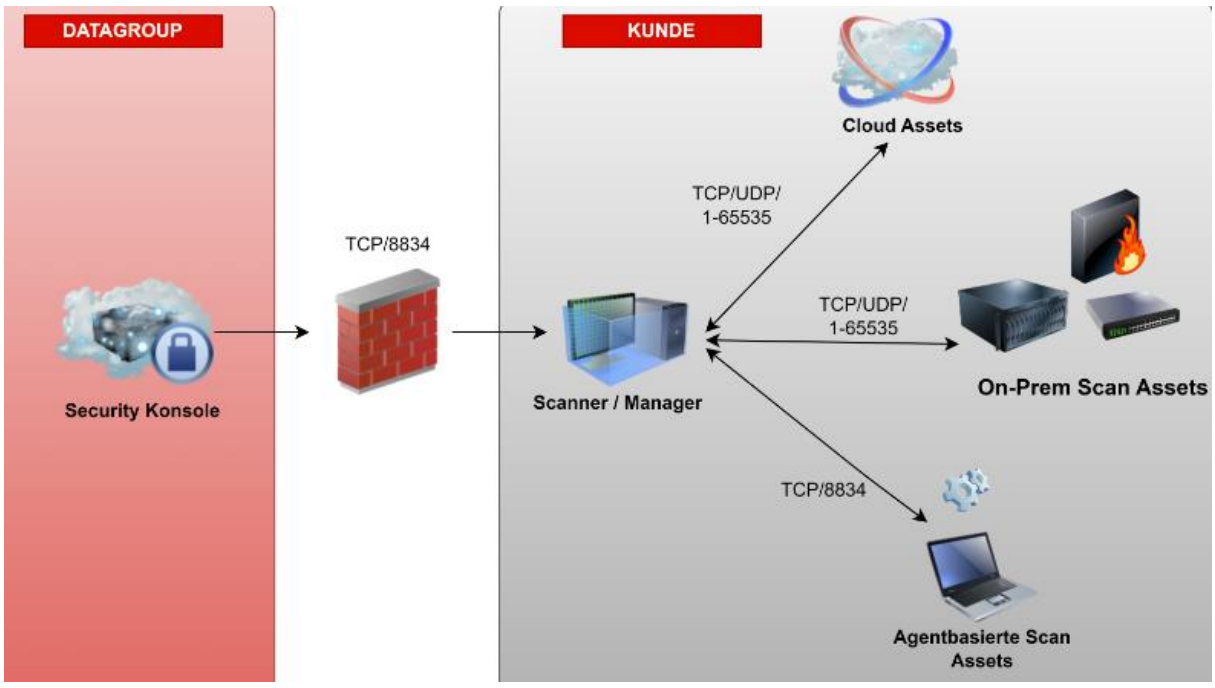
Für die Realisierung werden wir einen IPSec VPN-Tunnel zwischen Ihrem Netzwerk und unserem Netzwerk aushandeln und spannen.

Die technischen Voraussetzungen für einen IPsec-Tunnel sind wie folgt:

- IKEv1 (Internet Key Exchange Version 1) oder IKEv2.
- Eindeutige IP-Adresse, die für die Kommunikation über das Internet verwendet wird.
- IPsec-fähiges Geräte (z. B. Router, Firewalls oder VPN-Gateways).

Für die Aushandlung nutzen Sie bitte unser VPN Aushandlungsformular (Excel-Datei), welches wir an dieser Stelle verlinkt haben:

Bitte füllen Sie das VPN-Aushandlungsformular aus und bringen es vorbereitet in den Fokus-Abstimmungstermin mit. Sollten Sie inhaltliche Fragen haben, können Sie diese selbstverständlich gerne im Fokus-Workshop beantworten.



Detailfragen zum Service Darknet Scanning

Wir durchsuchen für Sie im Service Darknet Scanning einschlägige Ressourcen im Darknet nach spezifischen Inhalten, die Sie uns zur Verfügung stellen. Dies können Domaininformationen, Angaben zu zentralen Anwendern oder spezifische Schlüsselwörter sein.

16. Domains

Bitte benennen Sie die externe(n) Mail Domäne(n), welche wir im Darknet Scanning berücksichtigen sollen. Beispielsweise Ihre primäre Mail-Domain.

Antwort als Freitext

17. Very Important Persons (VIP)

Personen innerhalb Ihrer Organisation, die durch höhergestellte Privilegien ein potentiell höheren Angriffsvektor darstellen. Denkbare Beispiele sind Präsidium, Rektorrat, Kanzler/in, Dekan/en, CEO, Bereichsleiter/in, Personalsachbereiter/in, AD-Admin, Exchange-Admin usw.

Antwort als Freitext

18. Schlüsselwörter

Bitte benennen Sie organisationsspezifische Schlüsselwörter, wie beispielsweise Hochschulbezeichnungen, Forschungs- oder Projekttitel oder spezifische Hochschul-bezogene Kürzel (Prüfungensnummern).

Antwort als Freitext

Detailfragen zum Services Schwachstellen Scanning und Deep Scanning

Für die Implementierung des IT Security Services Schwachstellen Scanning (VMS) als interne Schwachstellenanalyse und für Service Deep Scanning, als sowohl interne, wie auch externe Schwachstellenanalyse benötigen wir ein besseres Verständnis über den Aufbau Ihres Netzwerks.

Hinweise zur Implementierung:

- Damit wir Ihre Systeme auf etwaige Schwachstellen scannen können, benötigen wir in Ihrem Netzwerk mindestens eine virtuelle Scanner-Appliance. **Diese stellen wir Ihnen als OVA-Template bereitstellen**.
- Die **Anzahl der Scanner-Appliances** richtet sich nach Ihrer Topologie und Segmentierung. Dies werden wir mit Ihnen in dem nachfolgenden Fokus-Workshop zum Service Schwachstellenanalyse diskutieren und festlegen.
- Im Kontext des Fokus-Workshops werden wir mit Ihnen zudem auch die **Unterschiede zwischen dem Netzwerkscan und dem agentenbasiertem Scanning** erläutern und Ihnen Empfehlungen aussprechen, auf welchen Systemen ein agentenbasiertes Scanning sinnvoll ist, Updatemechanismus der Appliances, etc.

19. Schwachstellen Scanning (VMS)

In welchen Netzwerksegmenten befinden sich ihre relevanten Server-Systeme, die für den Schwachstellenscan analysiert werden sollen.

Wir benötigen:

- *Interne IP-Subnetzbereiche die zu scannende Assets beinhalten (IPV4 und IPV6 möglich)*

Antwort als Freitext

20. Deep Scanning

In welchen Netzwerksegmenten befinden sich ihre relevanten Server-Systeme, die für den Schwachstellenscan analysiert werden sollen.

Wir benötigen:

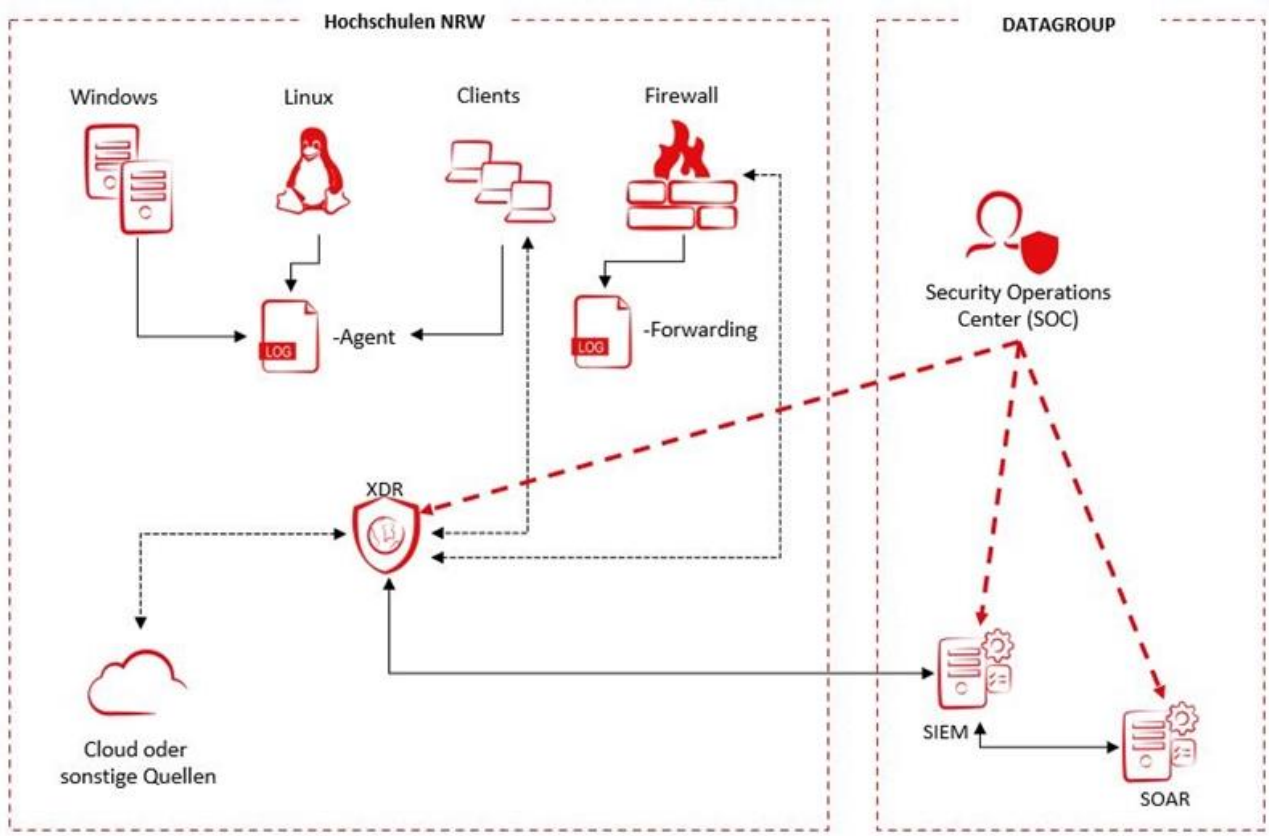
- *Externe IP-Subnetzbereiche die zu scannende Assets beinhalten (IPV4 und IPV6 möglich)*
- *Ihre öffentlichen Domains*

Antwort als Freitext

Tools mit sicherheitsrelevanten Informationen (LOG, Anomalien, Incident, XDR)

Hinweis: Der Betrieb einer Hochschul-eigenen XDR-Plattform (Extended Detection and Response) ist **optional**.

Sollten Sie bereits eine XDR-Lösung in Ihrem Hochschul-Netzwerk betrieben, ist diese Information für uns relevant. In diesem Fall würden wir ihre bestehende Lösung mit unseren Systemen koppeln und die dort aufbereiteten Daten zur weiteren Analyse nutzen.



21. XDR: Betreiben Sie in Ihrem Netzwerk bereits eine XDR-Lösung?

Verfügbare Antwortoptionen:

- Ja.
- Nein
- Einführung ist in Planung (Bitte in nachfolgender Frage weitere Hinweise zu Planungsstand, u.a. Zeit)

22. XDR: Sofern Sie eine XDR-Lösung einsetzen: Bitte teilen Sie uns mit, welche XDR-Lösung Sie einsetzen.

Antwort als Freitext

23. Netzwerk: Abfrage Firewallsysteme

Bitte benennen Sie uns Ihre relevanten Firewall-Systeme, welche wir per Log-Daten-Übermittlung **(nur Alarme)** in unsere IT Security Services integrieren dürfen.

Neben der IP sind für uns auch der Hersteller (und Modellbezeichnung) relevant. Mehrfachnennungen sind dabei möglich.

Bitte geben Sie an:
- Systemname
- Hersteller
- Modellbezeichnung
- (Optional) Beifügen Assetliste. Sofern sie eine Assetliste haben, können Sie diese an bremen.dm@datagroup.de senden.

Antwort als Freitext

24. Existieren in Ihrem Netzwerk weitere Systeme / Sensoren, deren Log-Alarme in unsere IT-Security Services integriert werden sollen?

Beispielhaft könnten das sein: interner vorhandener LOG-Server (z.B. Splunk, …), Firewall(s) (z.B. Cisco, Forcepoint, …), EDR(s) (z.B. Sophos InterceptX, FalconOne von Crowdstrike, …), DNS-Schutzschirm (z.B. Cisco Umbrella), (Netzwerk-)Anomalieerkennung (z.B. Cisco Secure Network Analytics (ehem. Cisco Stealthwatch), …), etc.

Falls ja, Bitte geben Sie an:
- Sensorbezeichnung
- IP-Adresse

Antwort als Freitext

25. Betreiben Sie in Ihrem Netzwerk bereits eine LOG Management-Lösung?

Unter LOG versteht man die kontinuierliche Erfassung, Speicherung, Verarbeitung, Synthetisierung und Analyse von Daten aus unterschiedlichen Programmen und Anwendungen. In diesem Fall würden wir ihre bestehende Lösung mit unseren Systemen koppeln und die dort vorgefilterten Security relevanten Daten zur weiteren Analyse nutzen.

Verfügbare Antwortoptionen:

- Ja.
- Nein
- Einführung ist in Planung (Bitte in nachfolgender Frage weitere Hinweise zu Planungsstand, u.a. Zeit)

26. Sofern Sie eine LOG-Management-Lösung einsetzen: Bitte teilen Sie uns weitere Details mit.

Bitte teilen Sie uns mit, welche Sensoren bzw. Log-Systeme Sie in Ihrem Netzwerk betreiben oder planen diese einzuführen. Sofern Sie eine LOG-Lösung einsetzen, teilen Sie uns bitte mit, welche Sensoren Sie einsetzen, es ist eine optional beispielhafte nicht abschließende Liste.

- interne vorhandene LOG-Server (z.B. Splunk, …)
- EDR(s) (z.B. Sophos InterceptX, FalconOne von Crowdstrike, …)
- DNS-Schutzschirm (z.B. Cisco Umbrella)
- (Netzwerk-)Anomalieerkennung (z.B. Cisco Secure Network Analytics (ehem. Cisco Stealthwatch), etc.

Antwort als Freitext

Penetration Testing (heavy)

Der Service simuliert reale Cyberangriffe, um die Widerstandsfähigkeit der IT-Infrastruktur der Hochschulen zu testen. Durch diese Simulationen werden Schwachstellen identifiziert und proaktive Sicherheitsmaßnahmen ermöglicht. Dieser Service steht Ihnen einmal im Jahr in Form einer manuellen Simulation eines Cyberangriffs pro Hochschule vertraglich zu.

Hinweise:

- *Die Simulation erfolgt nur mit Ihrem Einverständnis und einer vorherigen gegenseitigen Zeichnung eines Haftungsausschlusses.*
- *Für die Durchführung werden wir mit Ihnen im Vorfeld einen Termin koordinieren und mit entsprechender Vorlaufzeit einplanen, vgl. Frage 28.*

27. Systeme für Penetration Testing (heavy)-Simulation

Bitte machen Sie sich einmal im Vorfeld bereits Gedanken zu **maximal 10 Systemen**, welche wir für den Pen-Test berücksichtigen sollen. Je nach Systemanzahl können wir den zeitlichen Aufwand einschätzen und für die Vorplanung berücksichtigen (Systembeispiele.: System 1 – ERP (Webfrontend, Applikationen, Datenbank), System 2 - Exchange(Loadbalancer, CAS-Server, MBX-Server).

Antwort als Freitext

28. Penetration Testing (heavy): Nennung von ersten Terminvorschlägen für das Jahr 2024

Jede Hochschule hat einmal jährlich die Möglichkeit, eine manuelle Simulation von Cyberangriffen (Penetration Testing (heavy)) optional durchführen zu lassen. Bitte benennen Sie uns idealerweise **fünf mögliche Termine bzw. Zeiträume**, an denen eine Durchführung an Ihrer Hochschule grundsätzlich möglich wäre, damit wir Ihnen einen passenden Termin anbieten können.

Hinweis: Die Nennung der Terminevorschläge hilft uns bei der Terminkoordination. Im Rahmen der nachgelagerten Terminkoordination erhalten Sie von uns eine finale Terminbestätigung.
Die Dauer eines Penetration Testings kann bis zu 2 Wochen andauern.

Antwort als Freitext

Phishing Kampagnen

Gerne stellen wir Ihnen die gewünschte Lizenzanzahl zum Produkt SOPHOS Phish Threat zur Verfügung. Nach Bereitstellung können Sie die Lizenzen über ihren Zugang im SOPHOS Central-Portal aktivieren.

Hierfür benötigen Sie eine SOPHOS ID, welche Sie im sich im Bedarfsfall über folgende Webseite eigenständig anlegen können: *https://central.sophos.com/manage/login*

Weitere Informationen zum Produkt SOPHOS Phish Threat finden Sie unter:
https://www.sophos.com/de-de/products/phish-threat?utm_source=google&utm_medium=cpc&utm_campaign=mg-2023-dach-de-demg-gog-bra-convr-ema-search-exact&utm_term=sophos%20phishing&utm_content=na&cmp=7014w000001sNCPAA2&gad_source=1&gclid=CjwKCAjwl4yyBhAgEiwADSEjeHp5BKbHIj271pWBL0t7_-1HEM_taEkz4T5WZak7DwgewTJp9wlkvBoCaNsQAvD_BwE&gclsrc=aw.ds

29. Wie viele Lizenzen für SOPHOS Phish Threat benötigen Sie?

Sofern Sie an dem Phishing Kampagnen-Modul SOPHOS Phish Threat interessiert sind, teilen Sie uns bitte mit wie vielen Lizenzen Sie benötigen.

Lizenzierungsinformation:
Eine Lizenz pro E-Mail-Postfach. Hochschulangehörige ohne Studierende, Funktionspostfächer etc.

Nummerische Antwort

30. Glossar

EASM -	External Attack Surface Management
Key User	Zentrale Anwender, die berechtigt sind, bei DATAGROUP Tickets aufzumachen.
SOC	Security Operation Center
SOAR	Engl. Abkürzung für Security orchestration automation, and response. Software findet im Service Security Operation Center (SOC) DATAGROUP-seitig Anwendung.
VMS	Engl. Abkürzung für Vulnerability Management System. Zugeordneter Security Service ist Schwachstellen Scanning.