Spam melden, falsch klassifiziert, virtuelle E-Mail-Nachrichten

Inhalt

Einleitung

In diesem Dokument werden Spam-, falsch klassifizierte, virtuelle oder zusätzliche E-Mails zur Unterstützung oder Prüfung an Cisco weitergeleitet.

Arten von E-Mail-Nachrichten

Spam-, Spam- und Marketing-E-Mail-Nachrichten sind:

- *Spam*: Unrelevante oder unangemessene E-Mail-Nachrichten an einen Empfänger.
- *Ham*: Eine E-Mail-Nachricht, die kein Spam ist. Oder "non-spam", "good mail".
- *Marketing*: Marketing einer kommerziellen E-Mail-Nachricht direkt

Cisco akzeptiert Einsendungen für E-Mails, die falsch klassifiziert wurden:

- Falsch-negativ (Spam-Mailversand)
- falsch positiv (oder "Ham")
- Falsch negative Marketingbotschaften
- Fehlalarme Marketingbotschaften
- Phishing-Nachrichten, Phishing-positive Nachrichten
- Virusverdächtige, virenpositive Meldungen

Warum E-Mails an Cisco melden?

Versäumte oder falsch gekennzeichnete E-Mail-Nachrichten, die Cisco zur Verfügung gestellt werden, beinhalten die Inhaltsbestätigung, die allgemeine Wirksamkeit und die zugehörigen Regeln und Bewertungen. Sobald Sie eine E-Mail an Cisco gesendet haben, können Sie über das E-Mail-Status-Portal weitere Observables und eingebettete Anhänge anzeigen.

E-Mail-Statusportal

Mit einer gültigen CCO-ID können Sie sich bei https://talosintelligence.com/tickets/email_submissions anmelden. Über das E-Mail-Status-Portal können Sie den Status Ihrer E-Mail-Einsendungen an Cisco anzeigen. Cisco empfiehlt, Spam/Phishing-E-Mails zu versenden, die aktuelle Erkennungsinhalte und Ham, unerwünschte E-Mails, die falsch herausgefiltert wurden, umgangen haben, um die Gesamtwirksamkeit zu erhöhen. Das E-Mail-Status-Portal bietet eine Möglichkeit, den Status dieser Anträge zu verfolgen. Sie können Ihre Eingaben überwachen, und Domänenadministratoren oder Domänenanzeigen können alle Eingaben aus Ihrer Domäne(n) überwachen.

> **Hinweis**: Das veraltete E-Mail-Einreichungs- und Nachverfolgungsportal (ESTP) wurde mit Stand vom 1. September 2020 durch das E-Mail-Statusportal ersetzt, das auf Talosintelligence.com gehostet wurde.

So melden Sie E-Mail-Nachrichten an Cisco

Unterstützte Methoden sind:

1. Cisco Secure Email Submission Add-In
   Unterstützt Outlook (Windows, Mac und Web)
2. Cisco Email Security-Plug-in Unterstützt Outlook (nur Windows)
3. Direkte E-Mail-Übermittlung vom Endbenutzer

Cisco Secure Email Submission Add-In

Das Cisco Secure Email Submission Add-In unterstützt Microsoft Outlook für Windows, Mac und Web. Weitere Informationen finden Sie unter "Supported Configurations for Cisco Secure Email Encryption Service Add-In and Cisco Secure Email Submission Add-In" in der Kompatibilitätsmatrix für Cisco Secure Email Encryption Service, um die Kompatibilität mit Ihrer Outlook-Version sicherzustellen.

Weitere Informationen zum Herunterladen und Installieren finden Sie in der Cisco Secure Email Submission Add-In-Dokumentation.

Cisco Email Security-Plug-in

Das Cisco Email Security-Plug-in unterstützt nur Microsoft Outlook unter Windows. Weitere Informationen finden Sie unter "Supported Configurations for Cisco Email Reporting Plug-in" in der Kompatibilitätsmatrix für Cisco Secure Email Encryption Service, um die Kompatibilität mit Ihrer Outlook-Version sicherzustellen.

> **Anmerkung:** Ältere Versionen des Plug-ins heißen "IronPort Email Security-Plug-in" oder "Encryption-Plug-in für Outlook". Diese Version des Plugins enthielt sowohl Reporting als auch Encryption zusammen. 2017 trennte Cisco die Services und veröffentlichte zwei neue Versionen des Plug-ins "Email Reporting Plugin for Outlook" und "Email Encryption Plugin for Outlook". Diese waren mit einer Version 1.0.0.x verfügbar.

Direkte E-Mail-Übermittlung

Befolgen Sie die Anweisungen für Ihren E-Mail-Client, um die E-Mail als MIME-codierte Anlage (RFC 822 Multipurpose Internet Mail Extension) anzufügen. Wenn eines der Beispiele nicht Ihren E-Mail-Client widerspiegelt, lesen Sie bitte direkt das E-Mail-Client-Benutzerhandbuch oder den Produktsupport und bestätigen Sie, dass der E-Mail-Client "Forwarding as Attachment" (Weiterleiten als Anhang) unterstützt.

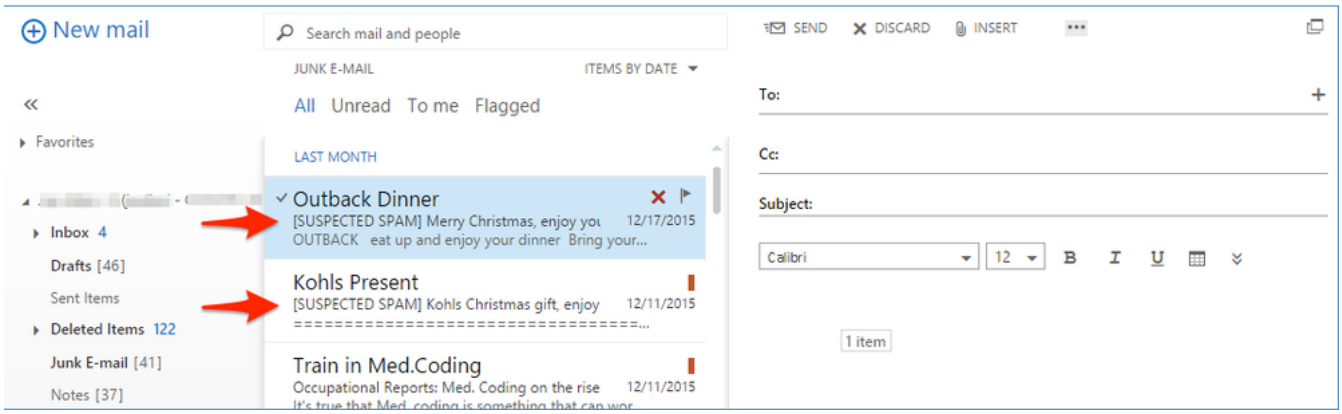
Senden Sie E-Mails an die entsprechende E-Mail-Adresse:

spam@access.ironport.com	Der Endbenutzer berücksichtigt den E-Mail-Spam oder die Betreffzeile enthält [SUSPECTED SPAM].
ham@access.ironport.com	Der Endbenutzer betrachtet die E-Mail NICHT als Spam. Die Betreffzeile enthält [SUSPECTED SPAM], oder die Betreffzeile enthält zusätzliche Tags.
ads@access.ironport.com	Der Endbenutzer betrachtet die E-Mail-Nachricht als Marketinginhalte oder als Graus oder die Betreffzeile umfasst [MARKETING], [SOCIAL NETWORK] oder [BULK].
not_ads@access.ironport.com	Der Endbenutzer betrachtet die E-Mail NICHT als Marketing oder Graymail, oder die Betreffzeile enthält [MARKETING], [SOCIAL NETWORK] oder [BULK].
phish@access.ironport.com	Die E-Mail-Nachricht scheint ein Phishing-E-Mail zu sein (der darauf ausgelegt ist, Benutzernamen, Kennwörter, Kreditkarteninformationen oder andere persönlich identifizierbare Informationen zu erfassen), oder die E-Mail enthält Malware-Anhänge

virus@access.ironport.com	(ebenfalls zur Erfassung von Benutzernamen oder Kennwörtern). Der Betreffzeile wir [SUSPECTED SPAM], [Possible $Threat_category Fraud] oder Ähnliches vorangeste Der Endbenutzer betrachtet die E-Mail-Nachricht oder einen Anhang als viral oder die Betreffzeile enthält [WARNUNG: VIRUS ERKANNT].

Nicht alle Betreffzeilen enthalten zusätzlichen Text und Tags. Informationen zu Ihren Einstellungen finden Sie in Ihrer Konfiguration des Cisco Secure Email Gateway oder Cloud Gateway für Anti-Spam-, Anti-Virus-, Graymail- und Outbreak-Filter, oder wenden Sie sich bei Bedenken an Ihren E-Mail-Administrator.

Beispiel für getaggte Betreffzeilen:



Warnung: Leiten Sie Ihre E-Mail-Nachricht nicht als Vorlage weiter. Diese Aktion behält nicht die Reihenfolge der Mail-Routing-Header bei und entfernt die erforderlichen E-Mail-Routing-Header, die für die Zuweisung der Quelle der E-Mail erforderlich sind. Stellen Sie stattdessen sicher, dass Sie die E-Mail immer über die Option "Weiterleiten als Anhang" versenden.

Sie können eine E-Mail direkt an folgende Adresse senden:

- Microsoft Outlook
- Microsoft Outlook Web App, Microsoft Office 365
- Microsoft Outlook 2011 und Microsoft Outlook 2016 für Mac (OS X, MacOS)
- Mail (OS X, MacOS)
- Mozilla Thunderbird
- Mobile Plattformen (iPhone, Android oder andere)

Microsoft Outlook

- Die bevorzugte Einsendemethode von Microsoft Outlook ist die Verwendung des Cisco

Secure Email Submission Add-Ins.

- Senden Sie bei unerwünschten E-Mails wie Spam, Viren und Phishing-E-Mails Nachrichten an Cisco.
- Die Schaltfläche Kein Spam kann legitime E-Mail-Nachrichten, die als Spam markiert sind, schnell neu klassifizieren.

Anmerkung: Bitte befolgen Sie die nächsten Anweisungen, wenn Sie das Cisco Email Security-Plug-in nicht installieren können oder es vorziehen.

Microsoft Outlook Web App, Microsoft Office 365

1. Öffnen Sie Ihr Postfach in Microsoft Outlook Web App.
2. Wählen Sie die Nachricht aus, die Sie senden möchten.
3. Klicken Sie oben links auf "Neue Mail".
4. Ziehen Sie die Nachricht, und legen Sie sie als Anlage zur neuen Nachricht ab.
5. Senden Sie die E-Mail-Nachricht an die in diesem Dokument angegebene Adresse.

Microsoft Outlook 2011 und Microsoft Outlook 2016 für Mac (OS X, MacOS)

1. Wählen Sie die Nachricht im Nachrichtenbereich aus.
2. Klicken Sie auf die Schaltfläche Anhang.
3. Leiten Sie die Nachricht an die in diesem Dokument angegebene Adresse weiter.

Mail (OS X, MacOS)

1. Klicken Sie mit der rechten Maustaste auf die E-Mail-Nachricht selbst, und wählen Sie **Weiterleiten als Anhang aus**.
2. Leiten Sie die E-Mail an die in diesem Dokument angegebene Adresse weiter.

Mozilla Thunderbird

1. Klicken Sie mit der rechten Maustaste auf die E-Mail-Nachricht selbst, und wählen Sie **Weiterleiten als > Anhang aus**.
2. Leiten Sie die E-Mail an die in diesem Dokument angegebene Adresse weiter.

Anmerkung: MailSentry IronPort Spam Reporter ist ein Drittanbieter-Plugin für Mozilla Thunderbird, das die gleiche Aktion wie beschrieben ausführt, aber eine "Spam/Ham"-Schaltfläche bereitstellt. **MailSentry IronPort Spam Reporter ist kein von Cisco unterstütztes Plugin.**

Mobile Plattformen (iPhone, Android oder andere)

- Wenn Ihre Mobilplattform keine Möglichkeit hat, die ursprüngliche E-Mail als Anhang weiterzuleiten, senden Sie sie bitte, sobald Sie Zugriff auf eine der anderen Methoden haben.

Überprüfen von Einsendungen an Cisco

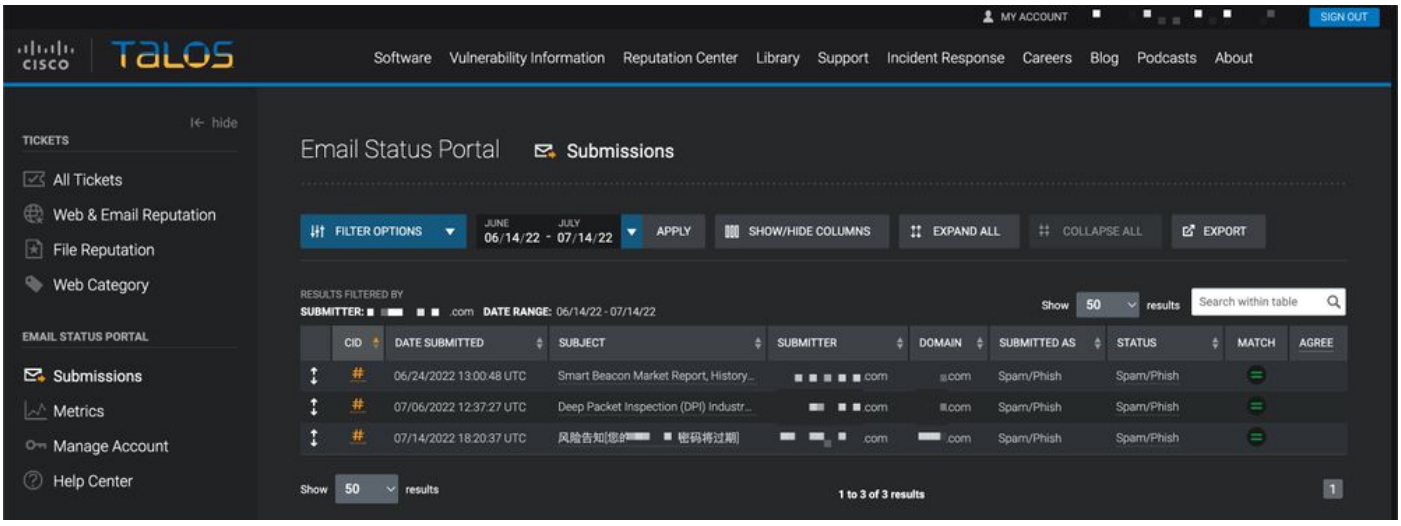
Direkte E-Mail-Übermittlung

Cisco sendet keine Bestätigungs-E-Mail oder Empfangsbestätigung für E-Mail-Einsendungen. Stattdessen können Sie Ihre Beiträge über das E-Mail-Status-Portal unter Talosintelligence.com einsehen.

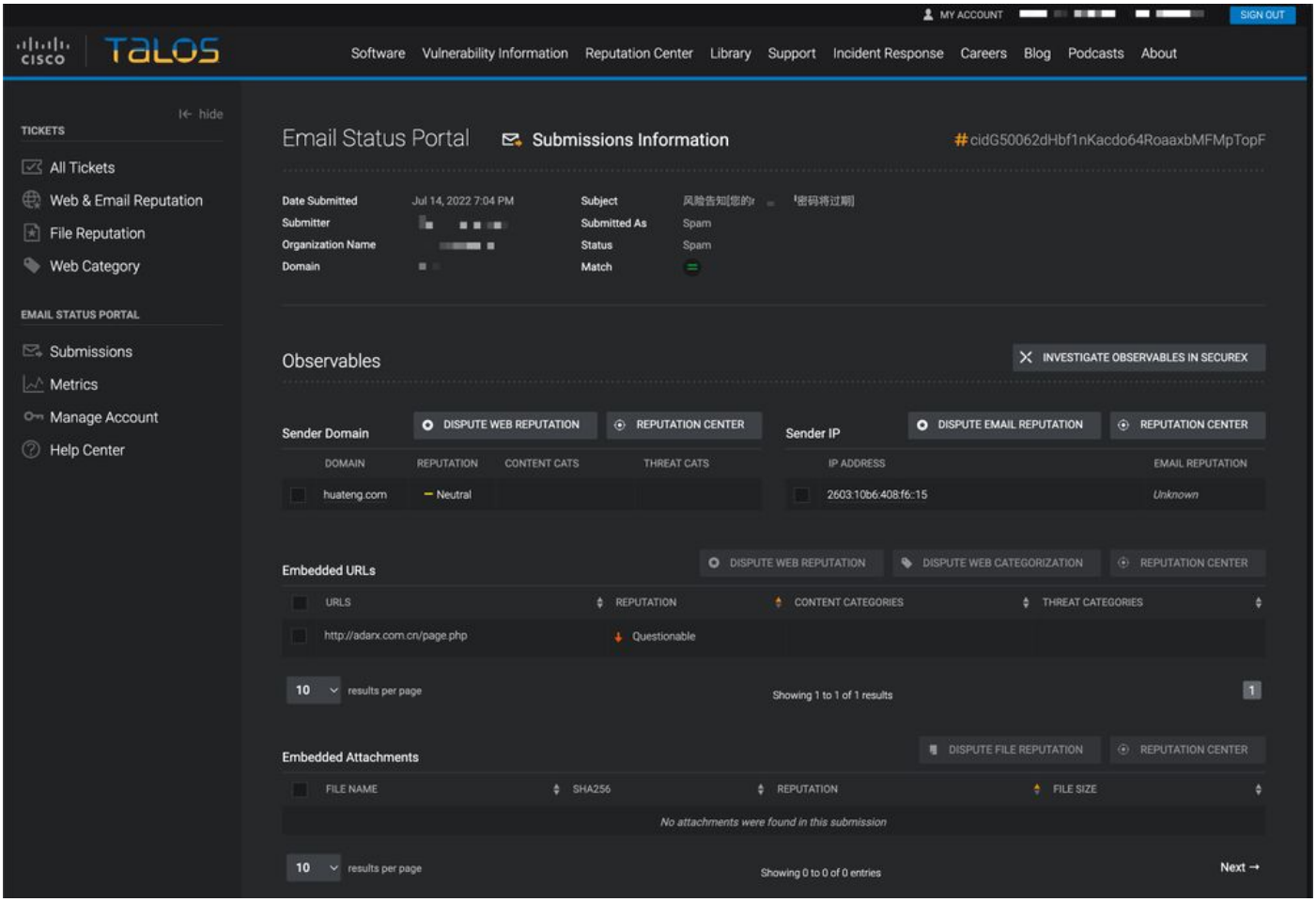
E-Mail-Statusportal

Validieren Sie Ihre Eingaben im E-Mail-Status-Portal. Nach der Anmeldung erhalten Sie eine Liste aller Ihrer Eingaben innerhalb des angegebenen Datums-/Zeitbereichs.

Beispiel:



Wenn Sie auf die eindeutige CID "#" klicken, werden weitere Details zur gemeldeten E-Mail angezeigt.



Ihnen werden Absenderdomäne, Absender-IP, eingebettete URLs und eingebettete Anhänge angezeigt, die der gemeldeten E-Mail zugeordnet sind. Sie können weitere Maßnahmen mit **Webreputation bei Streitfällen**, **E-Mail-Reputation** und **Dateireputation bei Streitfällen** ergreifen.

Jede verschachtelte Informationszeile zeigt maximal fünf Beobachtungsdaten eingebetteter URLs und eingebetteter Anhänge. Wenn eine E-Mail-Vorlage mehr Beobachtungsdateien enthält, kann ein Benutzer auf die Seite "Go to Email Submission Detail" (Details zur E-Mail-Einsendung anzeigen) klicken, um eine vollständige Liste der extrahierten Beobachtungsdateien anzuzeigen.

Sie können weitere Reputationsdetails einer einzelnen beobachtbaren Person aufrufen und dann auf die Schaltfläche 'Reputation Center' klicken.

Sie können auch mehrere Observables über SecureX untersuchen. Dieses Dashboard kombiniert Reputationsdaten aus der gesamten Suite von Cisco Secure-Produkten, basierend auf Ihrem Cisco Produktportfolio. Sie können bis zu 20 Beobachtungen aus einem einzigen Beitrag auswählen, um in SecureX gleichzeitig mit der Schaltfläche "Investigate Observables in SecureX" zu untersuchen.

Benutzer können einen einzigen Reputationsstreit (Web, E-Mail oder Datei) einreichen oder mehrere Streitigkeiten für einen oder mehrere der bei einer Einreichung beobachteten Streitfälle auslösen. URLs und Domänen können auch Web-Kategorisierungsstreitigkeiten gegen sie einreichen lassen.

Weitere Informationen zum E-Mail-Status-Portal finden Sie unter https://talosintelligence.com/tickets/email_submissions/help

Zusätzliche Informationen

Dokumentation für Cisco Secure Email Gateway

- Versionshinweise
- Benutzerhandbuch
- CLI-Referenzhandbuch
- API-Programmieranleitungen für Cisco Secure Email Gateway
- Open Source im Cisco Secure Email Gateway
- Installationsanleitung zur Cisco Content Security Virtual Appliance(einschl. Virtual Cloud Gateway)

Secure Email Cloud Gateway-Dokumentation

- Versionshinweise
- Benutzerhandbuch

Dokumentation für Cisco Secure Email und Web Manager

- Versionshinweise und Kompatibilitätsmatrix
- Benutzerhandbuch
- API-Programmieranleitungen für Cisco Secure Email und Web Manager
- Installationsanleitung für Cisco Content Security Virtual Appliance(einschl. Virtual Email und Web Manager)

Cisco Secure Product Documentation

- Namensarchitektur des Cisco Secure Portfolios