Lupasafe

Lupasafe-security platform

Een product van Skopos Security Labs BV

Productbeschrijving

Datum: November 2025

Versie	Datum	Wijzigingen
1.5	November 2025	Continuous phishing, Autotask integratie, custom branding
1.4	Mei 2025	Compliance rapportage & -rollen, Google integratie, rapportage
1.3	April 2025	Dmarc report, multi-tenant
1.2	Februari 2025	Single Sign-On
1.1	November 2024	E-learning
1.0	Januari 2024	Algehele opmaak

Inhoud

H1 Gehackte gegevens

Doelstelling

Lupasafe controleert gelekte gegevens om bedrijven te waarschuwen. Wij informeren medewerkers niet rechtstreeks maar doen dit via de hoofdgebruiker van het account. Onze database bevat meer dan 20 miljard records met gelekte gegevens en is opgeslagen in Limburg (Duitsland).

Proces

We zoeken actief op het dark web, torrents, PasteBin en Telegram-groepen om nieuwe datalekken te identificeren. U kunt van Lupasafe verwachten dat het de grootste beschikbare datalek bestanden vindt en verwerkt. De zoekopdracht op het dark web is gebaseerd op de domeinnaam van de klant en zijn e-mailadressen.

Gegevens

Gegevens zijn afkomstig uit twee componenten: (1) Gehackte gegevens en (2) “Have I Been Pwned”. Met “Have I Been Pwned” (HIBP) controleren we op eventuele datalekken van werknemers met behulp van uw bedrijfsdomein en e-mailadres. HIBP is gevestigd in Australië, maar bevestigt dat ze geen data opslaan (referentie). Lupasafe slaat om privacy- en veiligheidsredenen niet het volledige wachtwoord op.

Frequentie

Tests worden direct uitgevoerd nadat een domein in de portal is toegevoegd of wanneer medewerkers zijn toegevoegd, handmatig of via import. Hierna wordt de controle iedere 7 weekdagen herhaald

Resultaten

Gemiddeld vindt Lupasafe gelekte gegevens voor ongeveer een derde van de werknemers, maar voor sommige organisaries kan dit minder tot nul zijn. Het rapport bevat de wachtwoordsterkte, een gemaskeerde versie van het blootgestelde wachtwoord, de lengte ervan, de frequentie en de betrokken werknemer. Voor HIBP tonen we de naam van de lek, de soorten inbreuk op de gegevens, de HIBP-severity code en het jaar. Er worden geen PII-gegevens weergegeven. Hierdoor kunnen bedrijven getroffen werknemers op de hoogte stellen, het opnieuw instellen van wachtwoorden afdwingen en strategieën voor de reactie op datalekken evalueren.

Wet- en regelgeving

Lupasafe opereert binnen de AVG-Wet- en regelgevingen. Ons juridische team heeft een wettelijke basis geformuleerd voor Lupasafe om deze gevoelige gegevens op verantwoorde wijze te bewaren binnen de AVG-Wet- en regelgeving. In het Power BI-dashboard worden geen gegevens over persoonlijk identificeerbare informatie (PII) gepresenteerd. PII-gegevens zijn alleen zichtbaar in de portal, die beperkt is door beheerderstoegang en 2FA (voor supervisors). Lupasafe koopt geen gegevens van criminelen.

Lees meer over gelekte gegevens.

H2 Domein- en IP-scanning

Doelstelling

Lupasafe voert een reeks scans uit op domeinen en IP-adressen om kwetsbaarheden en zwakheden aan het licht te brengen en beschermt zo tegen geautomatiseerde scans die zoeken naar online kwetsbaarheden. Het platform test ook op misbruik van domeinnamen, wat mogelijk kan duiden op phishing-pogingen door kwaadwillige actoren.

Proces

De scanfunctie voert een lijst met tests uit op domeinen en IP-adressen. Domeinen staan andere tests toe dan een IP-adres. Domeinen test het platform op kwetsbaarheden in webapplicaties, e-mailbeveiliging, beveiligingsheaders en SSL-beveiliging en domeinkraken. Bij ieder domein wordt de hostprovider getoond en wordt er een screenshot gemaakt.

Op alle assets voert het platform poortscans uit op alle bijbehorende services van poort 1 tot 65535. Vervolgens worden vingerafdrukken uitgevoerd om de software en versie van de service te beoordelen. Ten slotte worden de vingerafdrukgegevens naar de risico-engine gevoerd om mogelijke kwetsbaarheden en exploits op deze service te vinden.

Om gebruikers te helpen hun online activa te identificeren, biedt het platform een DNS Lookup-functie. De DNS stelt aanvullende subdomeinen voor voor onderzoek. dit is geen volledige lijst, omdat subdomeinen verborgen kunnen zijn.

Nadat de domeinnaam is ingediend, scout en waarschuwt het platform gebruikers voor gevallen waarin domeinen die lijken op die van hen online zijn geregistreerd, die kunnen worden misbruikt voor phishing en nabootsing van identiteit. De gevoeligheid kan door de gebruiker worden ingesteld.

Gegevens

Het platform rapporteert per domeinnaam het risico in termen van DKIM, DMARC, SPF, kwetsbaarheden in webapplicaties, SSL/ TLS en security header score. Gebruikers kunnen details bekijken. Historische gegevens worden opgeslagen om vergelijkingen mogelijk te maken. Kwetsbaarheden worden volgens CVS genoemd.

Frequentie

Alle scans worden direct na het toevoegen van assets uitgevoerd. Na deze eerste actie worden er eenmaal per week domeinscans uitgevoerd omdat deze verkeer genereren. Alle scans worden wekelijks gedaan.

Resultaten

Op basis van gebruikersvoorkeuren worden er direct e-mailwaarschuwingen verzonden wanneer Lupasafe een kwetsbaarheid identificeert. Alle bevindingen kunnen in het Power BI-dashboard worden bekeken en met anderen worden gedeeld. Gedetailleerde informatie is beschikbaar op het portaal.

Wet- en regelgeving

Voor het scannen van domeinen is een gebruikersactie vereist voor toestemming. Verschillende landen hebben verschillend beleid, de gebruiker moet rechten hebben om de scans uit te voeren.

Lees meer over e-mailbeveiliging, beveiligingsheaders, websites.

H3 Bewustzijn van medewerkers / Phishing

Doelstelling

Lupasafe biedt gebruikers de mogelijkheid om gerichte en standaard phishing-tests uit te voeren op eindgebruikers. Dit kan continu of eenmalig gebeuren. Het doel is om het phishing-risico te helpen begrijpen en de eindgebruiker voor te lichten.

Proces

De gebruiker voegt medewerkers toe aan het platform en selecteert het type test: maatwerk of standaard. Het platform biedt een lijst met vooraf gedefinieerde phishing-berichten, deze worden regelmatig bijgewerkt en gecategoriseerd op onderwerp en taal. Qua phishing kan de gebruiker kiezen tussen klassiek, QR-code en smishing.

Onder aangepaste phishing kan de gebruiker zijn eigen bericht samen met een landingspagina opstellen. De gebruiker kan ook 33n doelwebsite importeren en deze gebruiken, of een aangepaste HTML-pagina voor het verzamelen van inloggegevens. Op de laatste pagina kan een educatieve video of uitlegtekst worden getoond. Elke phishing-e-mail kan worden bekeken en getest voordat deze wordt verzonden. Lupasafe geeft advies over hoe u een 100% inboxbezorging van berichten kunt bereiken. “Slachtoffers” krijgen direct na de phishing een trainingsvideo te zien in de taal van de browser. De phishing-resultaten worden opgeslagen en aan de gebruiker gepresenteerd.

De phishing kan voor een jaar geautomatiseerd worden. Beheerders kunnen via een 5-staps wizard de frequentie configureren (maandelijks, 3-maandelijks, 6-maandelijks of jaarlijks), e-mail templates selecteren, doelgroepen bepalen en een planning instellen. Het systeem voert de testen automatisch uit volgens het ingestelde schema en voegt nieuwe medewerkers automatisch toe aan volgende testronden. Na elke fase kunnen resultaten worden geanalyseerd om de security awareness binnen de organisatie te monitoren. De campagne loopt gedurende een vooraf bepaalde periode en draagt bij aan het verbeteren van de menselijke firewall tegen cyberdreigingen.

Gegevens

Gebruikers kunnen handmatig worden toegevoegd, geïmporteerd of gesynchroniseerd via de Azure Active Directory (AAD)-integratie. Voor AAD worden alleen gebruikers gesynchroniseerd die overeenkomen met het domein dat aan Lupasafe is toegevoegd. Lupasafe synchroniseert alleen actieve licenties om besmetting van de resultaten te voorkomen. Per medewerker wordt een track record bijgehouden van de basis phishing-statistieken: verzenden, lezen, aangeklikt. Dit maakt historische vergelijkingen mogelijk. Ingevulde gegevens op landingspagina's worden vanwege GDPR wetgeving en het maatwerk van de werkzaamheden niet opgeslagen.

Frequentie

Dit is afhankelijk van de gebruikersbehoeften. AAD-synchronisatie van medewerkers wordt twee keer per dag uitgevoerd.

Resultaten

Dit is afhankelijk van de configuratie van inkomende berichten, tekst van de phishing-e-mail, tijd en volume en expertise van de gebruiker. De resultaten zijn op hoog niveau zichtbaar op het Power-BI dashboard. Gedetailleerde records zijn zichtbaar in de portal zelf.

Wet- en regelgeving

De gebruiker is zelf verantwoordelijk voor het verkrijgen van goedkeuring voor een phishing-test. Lupasafe helpt bij het uitvoeren van phishing op een veilige en transparante manier. Dit zorgt voor vertrouwen bij de eindgebruiker en een leereffect. Vóór elke phishing wordt een checklist getoond met elementen als testen, toestemming van het management en transparantie. Alle verwerking van PII-gegevens volgt de AVG-wetgeving. Lupasafe gaat veilig en rechtmatig om met persoonsgegevens en zorgt ervoor dat de gegevensverzameling alleen wordt gebruikt met het doel een algemeen overzicht te geven van de veiligheidsrisico's onder medewerkers. In het Power BI-dashboard worden geen gegevens over persoonlijk identificeerbare informatie (PII) gepresenteerd. PII-gegevens zijn alleen zichtbaar in de portal, die beperkt is door beheerderstoegang en 2FA (voor supervisors).

Lees meer over Azure Active Directory, campagne op maat, rapporten, levering.

H4 Bewustzijn van medewerkers en rolbenoeming (voor compliance)

Doel

Lupasafe biedt gebruikers standaard cyberbewustzijnstraining aan eindgebruikers en medewerkers met specifieke rollen, bijvoorbeeld functionaris voor gegevensbescherming, beveiligingsfunctionaris en incidentmanager.

De trainingen zijn gericht op het onderwijzen van medewerkers over relevante onderwerpen, bijvoorbeeld:

- Wat is cybersecurity?
- Phishing en social engineering
- Wachtwoorden
- Privacy en sociale media
- Thuiswerken
- Incidentrespons
- AVG-regelgeving

Nieuwe onderwerpen worden voortdurend toegevoegd aan het programma. Het doel is om beveiligingsrisico's onder medewerkers in het algemeen te helpen begrijpen en de eindgebruiker te onderwijzen met feedback.

Proces

Leidinggevenden kunnen de e-learning modules voor het hele jaar inplannen via een Opt-In functie, en nieuwe medewerkers worden automatisch meegenomen via AAD-integratie.

Portalgebruikers kunnen medewerkers aanstellen in bepaalde rollen. Dit kan worden aangepast aan de behoeften van de organisatie. Deze aangestelde rollen worden gebruikt voor compliance rapportage.

Meer informatie over het definiëren van rollen is hier te vinden:
https://skoposlab.freshdesk.com/support/solutions/articles/47001279807-roles-in-lupasafe-for-compliance-iso27001-ens-nis2-

Gegevens

De resultaten van de bewustwordingstest worden opgeslagen en gepresenteerd aan de gebruiker in het Power-BI dashboard. Per medewerker wordt een track record bijgehouden van de basis awareness metrics: versturen, gestart, gescoord. Dit maakt historische vergelijkingen mogelijk.

Frequentie

Dit is afhankelijk van de gebruikersbehoeften. Wij raden aan om minimaal één keer per maand een korte test te sturen.

Resultaten

Alle bevindingen kunnen in het Power BI dashboard worden bekeken en met anderen worden gedeeld. Gedetailleerde informatie is beschikbaar op het portaal.

Regelgeving

Alle verwerking van PII-gegevens volgt de AVG-wetgeving. Lupasafe gaat veilig en rechtmatig om met persoonsgegevens en zorgt ervoor dat de gegevensverzameling alleen wordt gebruikt met het doel een algemeen overzicht te geven van de veiligheidsrisico's onder medewerkers. In het Power BI-dashboard worden geen gegevens over persoonlijk identificeerbare informatie (PII) gepresenteerd. PII-gegevens zijn alleen zichtbaar in de portal, die beperkt is door beheerderstoegang en 2FA (voor supervisors).

Lees meer over Azure Active Directory, medewerkers template emails.

H5 Endpoint-compliance

Doelstelling

Identificeer kwetsbare endpoints (computers, laptops, telefoons) in een organisatie. Het platform voert een analyse uit van de software en kwetsbaarheden op MacOS, Linux, Windows en de aanwezigheid van fundamenteel zwak beleid en patches op computers met Windows.

Proces

De gebruiker implementeert het endpoint handmatig of via een centrale uitrol. De implementatie kan worden gedaan via een MSI-bestand of Executable en worden uitgevoerd via Intune, groepsbeleid (GPO) of handmatige installatie. Het endpoint maakt verbinding via HTTPS via een e-mailadres of API. Na verbinding deelt het endpoint alle beschikbare applicaties, voor Windows ook het beleid en de geïnstalleerde patches (KB-bestanden). Het platform voert een risicobeoordeling uit om kwetsbare software te identificeren op basis van CVE's en beschikbare exploits. Risico's worden via e-mail en portal gerapporteerd in CVSS- en EPSS-score. Na de eerste indiening worden er twee beoordelingen uitgevoerd: een snelle risicobeoordeling van de belangrijkste kwetsbaarheden en een uitgebreide beoordeling op basis van alle bekende kwetsbaarheden.

Gegevens

Externe risicogegevens worden overgenomen van NVD, Microsoft, CISA en ExploitDB. Het portaal bewaart en toont alle endpoints, poorten en diensten, software en versies van de netwerksegmenten. Softwarekwetsbaarheden worden geclassificeerd op basis van de CVSS-score en de EPSS-score. Historische gegevens worden opgeslagen om vergelijkingen mogelijk te maken. Kwetsbaarheden worden volgens CVS genoemd. Voor elke host kunnen instellingen en activaprioriteit worden ingesteld, asset-tagging en waarschuwingsniveau worden toegepast.

Frequentie

Gemiddeld zal een actieve endpoint elke twee uur een delta van wijzigingen indienen. Na 30 dagen inactiviteit van de endpointsoftware wordt een asset in de portal op 'inactief' gezet. De timing kan worden geconfigureerd of deze functionaliteit kan worden uitgeschakeld.

Resultaten

Op basis van gebruikersvoorkeuren worden er direct e-mailwaarschuwingen verzonden wanneer Lupasafe een kwetsbaarheid identificeert. Alle bevindingen kunnen in het Power BI-dashboard worden bekeken en met anderen worden gedeeld. Gedetailleerde informatie is beschikbaar op het portaal.

Wet- en regelgeving

Er worden geen PII-gegevens verzameld, maar gebruikers kunnen besluiten activa aan werknemers te koppelen. Dit in afwachting van afspraken tussen werkgever en werknemer. Uit de gegevens kan worden afgeleid wie welke software of apps gebruikt. Vooral bij activa die geen eigendom zijn van het bedrijf moet dit zorgvuldig worden onderzocht.

Lees meer endpointen implementeren.

H6 Microsoft 365 Cloud-audit & CIS level 1 controls

Doelstelling

Geef gebruikers inzicht in verschillende belangrijke beveiligingsindicatoren van de Microsoft 365 Cloud en verbindt dit met CIS level 1 controls.

Proces

Gebruikers geven toestemming aan Lupasafe om verbinding te maken met de Microsoft 365 Cloud API. Via een alleen-lezen verbinding worden de belangrijkste beleidsregels opgeslagen in Lupasafe.

Gegevens

Lupasafe haalt gegevens uit de Microsoft 365 Cloud API via een alleen-lezen verbinding.

Frequentie

Wekelijks

Resultaten

Belangrijke beleidsregels worden geanalyseerd en weergegeven via het Power-BI-dashboard: de algehele Secure Score in percentages van 0-100%, de implementatiestatus van Admin MFA en User MFA. Inzicht in de beschikbaarheid van verouderde besturingselementen zoals IMAP en POP3.

Wet- en regelgeving

Er worden geen PII-gegevens gevraagd.

Lees meer over Microsoft 365 Cloud-audit.

H7 Netwerkscanner

Doelstelling

Regelmatig scannen van interne netwerksegmenten op hosts en services om kwetsbaarheden te helpen identificeren.

Proces

De gebruiker implementeert de netwerkscanner op een lokale computer in het doelnetwerk. De netwerkinterface moet toegang hebben tot het lokale netwerksegment en de gegevens naar de Lupasafe-server kunnen sturen. De scanner voert dagelijks een scan uit met behulp van de meegeïnstalleerde Nmap-software. De geautoriseerde scanner kan via het platform worden ingeschakeld en geconfigureerd. Na een succesvolle activering identificeert de scanner hosts in het opgegeven bereik, met uitzondering van de hosts die zijn gemarkeerd voor uitsluiting. Op alle hosts voert de scanner poortscans uit op alle bijbehorende services van poort 1 tot 65553. Vervolgens worden vingerafdrukken uitgevoerd om de software en versie van de service te beoordelen. Ten slotte wordt de volledige set aan de risico-engine doorgegeven om mogelijke kwetsbaarheden en exploits op deze service te vinden.

Gegevens

Externe risicogegevens worden afkomstig van NVD, Microsoft en CISA. Het portaal slaat alle hosts, poorten en services, software en versies van de netwerksegmenten op en toont deze. Softwarekwetsbaarheden worden geclassificeerd op basis van de CVSS-score en de EPSS-score. Historische gegevens worden opgeslagen om vergelijkingen mogelijk te maken. Kwetsbaarheden worden volgens CVS genoemd. Voor elke host kunnen instellingen en activaprioriteit worden ingesteld, asset-tagging en waarschuwingsniveau worden toegepast.

Frequentie

De scanner draait elke twee uur.

Resultaten

Op basis van gebruikersvoorkeuren worden er direct e-mailwaarschuwingen verzonden wanneer Lupasafe een kwetsbaarheid identificeert. Alle bevindingen kunnen in het Power BI-dashboard worden bekeken en met anderen worden gedeeld. Gedetailleerde informatie is beschikbaar op het portaal.

Wet- en regelgeving

De gebruiker moet toestemming hebben van de eigenaar van het netwerk om te scannen.

Lees meer over de netwerkscanner.

H8 Single Sign On (SSO)

Doelstelling

Gebruikers een veilige en eenvoudige manier bieden om toegang te krijgen tot het Lupasafe-platform zonder meerdere wachtwoorden te hoeven beheren.

Proces

De gebruiker configureert Single Sign-On via het Lupasafe-portaal. Het platform ondersteunt integratie met identiteitsproviders zoals Microsoft Entra ID (voorheen Azure AD), Google Workspace en andere SAML- of OpenID Connect-gebaseerde systemen. Zodra SSO is ingeschakeld, kunnen gebruikers zich aanmelden met hun zakelijke account. Dit vermindert de kans op wachtwoordgerelateerde beveiligingsproblemen en vereenvoudigt het toegangsbeheer. Gebruikers kunnen toegangsrechten beheren via hun bestaande identiteitsbeheerplatform, inclusief multi-factor authenticatie en groepsbeleid.

Gegevens

Lupasafe slaat geen wachtwoorden op voor SSO-gebruikers. Authenticatie en autorisatie worden afgehandeld door de identiteitsprovider. Activiteiten en inlogpogingen worden gelogd en kunnen worden ingezien via het beveiligingsdashboard in het portaal. Gebruikers kunnen sessietijdslimieten instellen en verplichte herauthenticatie afdwingen.

Frequentie

Authenticatie vindt plaats bij elke nieuwe sessie of op basis van het ingestelde beleid van de identiteitsprovider.

Resultaten

Gebruikers ervaren een snellere en veiligere aanmelding zonder wachtwoorden te beheren. Gebruikers behouden controle over de toegangsrechten en beveiliging.

Wet- en regelgeving

SSO-integraties voldoen aan de standaarden zoals SAML 2.0 en OpenID Connect. Organisaties blijven verantwoordelijk voor het correcte beheer van hun identiteitsprovider en toegangsrechten.

H9 DMARC-rapportage

Doelstelling

Organisaties voorzien van uitgebreide zichtbaarheid in e-mailauthenticatie om hun domein te beschermen tegen spoofing, de bezorgbaarheid te verbeteren en het merkvertrouwen te behouden.

Proces

Gebruikers configureren DMARC-rapportage via het Lupasafe-portaal. Na het selecteren van hun domein in de sectie "Websites & Routers" krijgen ze toegang tot het gebied "DKIM/DMARC/SPF Scan". Het platform genereert aangepaste DMARC DNS-records met unieke rapportageadressen. Gebruikers voegen deze TXT-records toe of werken deze bij bij hun domeinhostingprovider en verifiëren vervolgens de configuratie binnen Lupasafe. Zodra dit actief is, sturen mailservers wereldwijd samengevatte en forensische rapporten naar Lupasafe, dat deze gegevens verwerkt en in een overzichtelijk formaat weergeeft.

Gegevens

DMARC-rapporten bevatten authenticatieresultaten van ontvangende mailservers, inclusief SPF- en DKIM-verificatieresultaten, verzendende IP-adressen, berichtvolumes en acties (bezorgen, in quarantaine plaatsen, weigeren). Lupasafe analyseert deze rapporten, waarbij legitieme verzenders worden onderscheiden van mogelijke misbruikers. Het platform toont authenticatietrends, foutpercentages en geografische spreiding van verzendende servers. De rapporten bevatten geen werkelijke e-mailinhoud, wat de privacy waarborgt.

Frequentie

DMARC-aggregatierapporten worden meestal dagelijks of wekelijks gegenereerd door deelnemende mailservers. Lupasafe verwerkt continu binnenkomende rapporten en werkt het dashboard bij zodra er nieuwe gegevens beschikbaar zijn. Gebruikers kunnen meldingen configureren voor verdachte activiteiten of authenticatiefouten.

Resultaten

Organisaties krijgen zicht op al het e-mailverkeer dat gebruikmaakt van hun domeinnaam. Ze kunnen niet-geautoriseerde verzenders, legitieme maar verkeerd geconfigureerde systemen en mogelijke phishingpogingen identificeren. Deze informatie stelt hen in staat om hun e-mailbeveiligingsbeleid geleidelijk te versterken, van monitoring naar quarantaine en uiteindelijk naar het weigeren van ongeautoriseerde berichten, wat e-mailgebaseerde fraude drastisch vermindert.

Wet- en regelgeving

De implementatie van DMARC ondersteunt nalevingsvereisten, waaronder AVG, HIPAA en financiële regelgeving die bescherming tegen e-mailimitatie voorschrijven. De rapportagefunctie biedt een controletraject dat aantoont dat er maatregelen zijn genomen om het e-mailkanaal te beveiligen. Organisaties blijven verantwoordelijk voor het ondernemen van acties op basis van de verstrekte informatie via DMARC-rapporten.

H10 Compliance rapportage (ISO27001/NIS-2 Quality Mark 10/20)

Doelstelling

Organisaties voorzien van inzicht en bewijs van hun compliance status.

Proces

In het menu onder 'Compliance' staan verschillende compliance frameworks: NIS-2, ISO27001 en Cyber Essentials. De gebruiker kan de gegevens visueel bekijken of via Excel downloaden. Beschikbare items zijn gerelateerd aan Bijlage A van ISO27001, bijvoorbeeld 5.9 Inventarisatie van activa, 5.11 Retourneren van activa, 6.3 Informatiebeveiligingsbewustzijn en 8.1 Gebruikers endpoints.

Gegevens

Gegevens worden direct gegenereerd op basis van de nieuwste klantgegevens. De NIS-2 gegevens zijn gekoppeld op basis van de aangeleverde ISO27001 items en sluiten aan bij Quality Mark (per september 2025 - de Nederlandse standaard).

Frequentie

Op verzoek.

Resultaten

Organisaties krijgen zichtbaarheid in hun compliance status op de relevante compliance items. Ze kunnen bijvoorbeeld uitzonderingen identificeren, verkeerd geconfigureerde systemen en aangestelde rollen die bepaalde vereiste training hebben gefaald. Deze gegevens stellen hen in staat om hun compliance houding geleidelijk te versterken.

Wet- en regelgeving

Gebruikt voor ISO27001, NIS-2, ENS, etc.

H11 Lupasafe Multi-Tenant Omgeving

Doelstelling

Organisaties voorzien van een verenigd beveiligingsbeheerplatform dat monitoring en beheer van meerdere klanten of organisatorische eenheden mogelijk maakt via één dashboard, met behoud van strikte gegevensscheiding en aangepaste beveiligingsbeleid per tenant.

Proces

Beheerders krijgen toegang tot de multi-tenant omgeving via een gecentraliseerd dashboard dat belangrijke beveiligingsstatistieken weergeeft voor alle beheerde klanten. Het platform bevat een tenantselectiemenu waarmee snel kan worden geschakeld tussen klantomgevingen zonder opnieuw te hoeven inloggen.
Elke tenant behoudt gescheiden gegevens en configuraties, terwijl ze profiteren van de uniforme beheerinterface. Beheerders kunnen geaggregeerde beveiligingsstatistieken bekijken (zoals "100 Totaal aantal gebruikers over 5 klanten") of dieper ingaan op klantspecifieke gegevens ("Top 5 laagste beveiligingsscores op Microsoft Cloud").

Gegevens

De multi-tenant architectuur handhaaft gegevensscheiding tussen klanten, terwijl goedgekeurde beheerders toegang hebben tot cross-client analyses. De gegevens van elke tenant zijn logisch gescheiden met toegewijde versleuteling en toegangscontroles.
Het dashboard toont kritieke beveiligingsstatistieken, waaronder:

- Gebruikersbeheer (totaal aantal gebruikers, toegangsrechten)
- Beveiligingsincidenten (gegevenslekken, phishingstatistieken)
- Trainingsnaleving en voltooiingspercentages
- Activaregistratie en risicostatus
- E-mailbeveiligingsstatus
- Implementatiestatus van MFA
  Het dashboard maakt gebruik van numerieke indicatoren en kleurgecodeerde statusmarkeringen (rood voor risico's, groen voor conforme elementen) om de beveiligingsstatus snel te beoordelen.

Frequentie

Het multi-tenant dashboard wordt in realtime bijgewerkt naarmate beveiligingsincidenten zich voordoen in alle beheerde omgevingen. Automatische waarschuwingen informeren beheerders over kritieke problemen, ongeacht welke tenantweergave ze momenteel gebruiken.
Het schakelen tussen tenants gebeurt onmiddellijk, waardoor beheerders snel kunnen reageren op beveiligingsgebeurtenissen zonder workflowonderbreking.

Resultaten

Organisaties profiteren van:

- Gestroomlijnd beveiligingsbeheer over meerdere bedrijfseenheden of klanten
- Consistente beveiligingsbeleid met tenant-specifieke aanpassingen
- Verminderde beheerslast vergeleken met afzonderlijk beheerde instanties
- Uitgebreide zichtbaarheid over het gehele beveiligingsecosysteem
- Efficiënte toewijzing van middelen op basis van cross-tenant analyses
- Vereenvoudigd facturatie- en licentiebeheer
  De intuïtieve interface stelt beheerders in staat om trends in de gehele klantenbasis te identificeren en tegelijk tenant-specifieke problemen aan te pakken, zoals blijkt uit de gedetailleerde statistieken per beveiligingsdomein in de dashboardweergave.

Wet- en regelgeving

De multi-tenant omgeving handhaaft strikte scheiding van klantgegevens om te voldoen aan wettelijke vereisten, terwijl efficiënt beheer mogelijk blijft. Toegangscontroles zorgen ervoor dat beheerders alleen tenants kunnen bekijken en beheren waarvoor ze expliciet zijn gemachtigd.
Auditlogs registreren alle cross-tenant activiteiten voor nalevingsrapportage, en tenant-specifieke nalevingsvereisten kunnen per klant worden geconfigureerd en bewaakt.

H12 Autotask integratie

Doelstelling

Beveiligingsprofessionals en MSP's voorzien van een naadloze koppeling tussen Lupasafe beveiligingsmonitoring en Autotask PSA, waardoor kritieke beveiligingsmeldingen automatisch worden omgezet in actiegerichte tickets binnen de bestaande servicedesk-workflow.

Proces

De integratie genereert automatisch Autotask-tickets bij afwijkingen of belangrijke meldingen. Denk aan meldingen als: Cloud Policies, waarschuwt over gebruikers zonder Multi-Factor Authentication, met onderscheid tussen algemene gebruikers en admin-accounts. Network Activity, detecteert scanner assets die langer dan 6 dagen inactief zijn. DMARC Reports analyseren e-mail authenticatieproblemen en waarschuwen bij gefaalde SPF en DKIM validaties. Elke melding krijgt een prioriteitsscore (0-99) op basis van ernst en impact voor directe beoordeling door servicedesk-medewerkers.

Gegevens

De integratie verwerkt de volgende beveiligingsgegevens in Autotask-tickets:

- **MFA Beveiligingsstatus**: Aantallen en percentages van gebruikers zonder MFA-registratie (bijvoorbeeld "11 van de 18 gebruikers")
- **Asset Activiteit**: Identificatie van inactieve scanner assets met precisie tot op dagniveau
- **DMARC Statistieken**: Faalpercentages voor SPF en DKIM authenticatie per domein (bijvoorbeeld "27% SPF, 32% DKIM")
- **Prioriteitsscores**: Numerieke waarden (0-89) die urgentie kwantificeren

Alle tickets bevatten contextuele informatie die direct actionable is zonder toegang tot het Lupasafe-dashboard.

Frequentie

De integratie werkt in realtime en genereert tickets zodra beveiligingsdrempels worden overschreden. MFA-controles worden dagelijks uitgevoerd, Network Activity monitoring scant continu en genereert alerts bij 6-daagse inactiviteit, en DMARC Reports worden direct verwerkt bij nieuwe authenticatiestatistieken. De ticketfrequentie past zich dynamisch aan op basis van de beveiligingsstatus.

Resultaten

Organisaties profiteren van:

- **Proactieve beveiligingsrespons**: Automatische detectie en escalatie van beveiligingstekortkomingen
- **Verminderde reactietijd**: Directe ticketcreatie zonder handmatige dashboardcontroles
- **Verbeterde workflow-integratie**: Beveiligingstaken binnen bestaande Autotask-processen
- **Risico-gebaseerde prioritering**: Automatische scoretoekenning voor kritieke problemen eerst
- **Compliance documentatie**: Alle meldingen en acties geregistreerd voor audit-doeleinden
- **Verhoogde MFA-adoptie**: Systematische tracking leidt tot snellere implementatie
- **E-mail reputatiebehoud**: Tijdige DMARC-detectie voorkomt blacklisting

Wet- en regelgeving

De Autotask-integratie ondersteunt naleving van beveiligingsstandaarden door systematische documentatie van MFA-implementatie (vereist onder NIS2 en ISO 27001), e-mail authenticatie volgens DMARC-specificaties, en asset monitoring. Alle tickets dienen als audittrail en tonen tijdige detectie en communicatie aan. Prioriteitsscores faciliteren aantoonbare risico-gebaseerde respons, terwijl geautomatiseerde workflow waarborgt dat geen kritieke meldingen worden gemist.

.

H13 Whitelabeling and Branding

Doelstelling

MSP's en beveiligingsproviders in staat stellen om Lupasafe volledig te personaliseren met hun eigen merkidentiteit, waardoor klantcommunicatie professioneel en consistent wordt gepresenteerd onder de eigen huisstijl.

Proces

Beheerders configureren de whitelabel-omgeving via het menu 'Branding' in het dashboard. Het proces omvat drie stappen: upload van het bedrijfslogo (PNG/JPG/SVG, 300x100px, max 2MB), toevoegen van een optionele tagline, en definiëren van drie merkkleuren via HEX-codes (Primary Color voor buttons, Secondary Color voor achtergronden, Text Color voor contrast compliance). Vervolgens wordt de SMTP-server geconfigureerd voor verzending vanaf het eigen domein, inclusief host, poort (standaard 587 met TLS/SSL), authenticatiegegevens, from address en reply-to address. De live preview-functie toont realtime hoe emails en rapporten eruitzien voordat de configuratie wordt geactiveerd.

Gegevens

De branding-configuratie verwerkt:

- **Visuele Identiteit**: Bedrijfslogo, optionele tagline, en drie HEX-kleurcodes
- **SMTP Configuratie**: Server name, SMTP host, poort met encryptie, authenticatiegegevens, from address en reply-to address
- **Kleurenschema**: Primary Color, Secondary Color, en auto-berekende Text Color die voldoet aan WCAG contrast compliance
- **Status**: Active/Inactive toggle voor activering

Alle merkgegevens worden versleuteld opgeslagen en toegepast op email templates, HTML-rapportages en portal-interfaces.

Frequentie

De branding-configuratie is een eenmalige setup die permanent actief blijft. Zodra geactiveerd wordt de merkidentiteit realtime toegepast op alle uitgaande communicatie. Wijzigingen worden onmiddellijk doorgevoerd en kunnen via live preview worden gevalideerd voordat publicatie.

Resultaten

Organisaties profiteren van:

- **Volledige merkcontrole**: Alle klantcommunicatie in eigen huisstijl vergroot merkwaarde en professionaliteit
- **Verhoogd vertrouwen**: Herkenbaar domein en vertrouwde styling verbeteren open- en responsratio's
- **Consistente merkbeleving**: Uniforme toepassing over alle communicatiekanalen
- **Verbeterde deliverability**: Eigen domeinverzending faciliteert SPF/DKIM/DMARC compliance
- **Efficiëntie**: Eenmalige configuratie elimineert handmatige aanpassingen
- **Multi-tenant support**: Per klant aparte branding met centrale beheerefficiëntie

Wet- en regelgeving

De whitelabel-functionaliteit ondersteunt GDPR-transparantie door duidelijke identificatie van de verzendende partij. Automatische contrast compliance voldoet aan WCAG 2.1 toegankelijkheidsrichtlijnen. SMTP-configuratie met TLS/SSL encryptie voldoet aan beveiligingsstandaarden en faciliteert DMARC-compliance. De toggle-functie maakt terugval naar neutrale branding mogelijk bij audits. Auditlogs registreren alle configuratiewijzigingen voor compliance-rapportage.