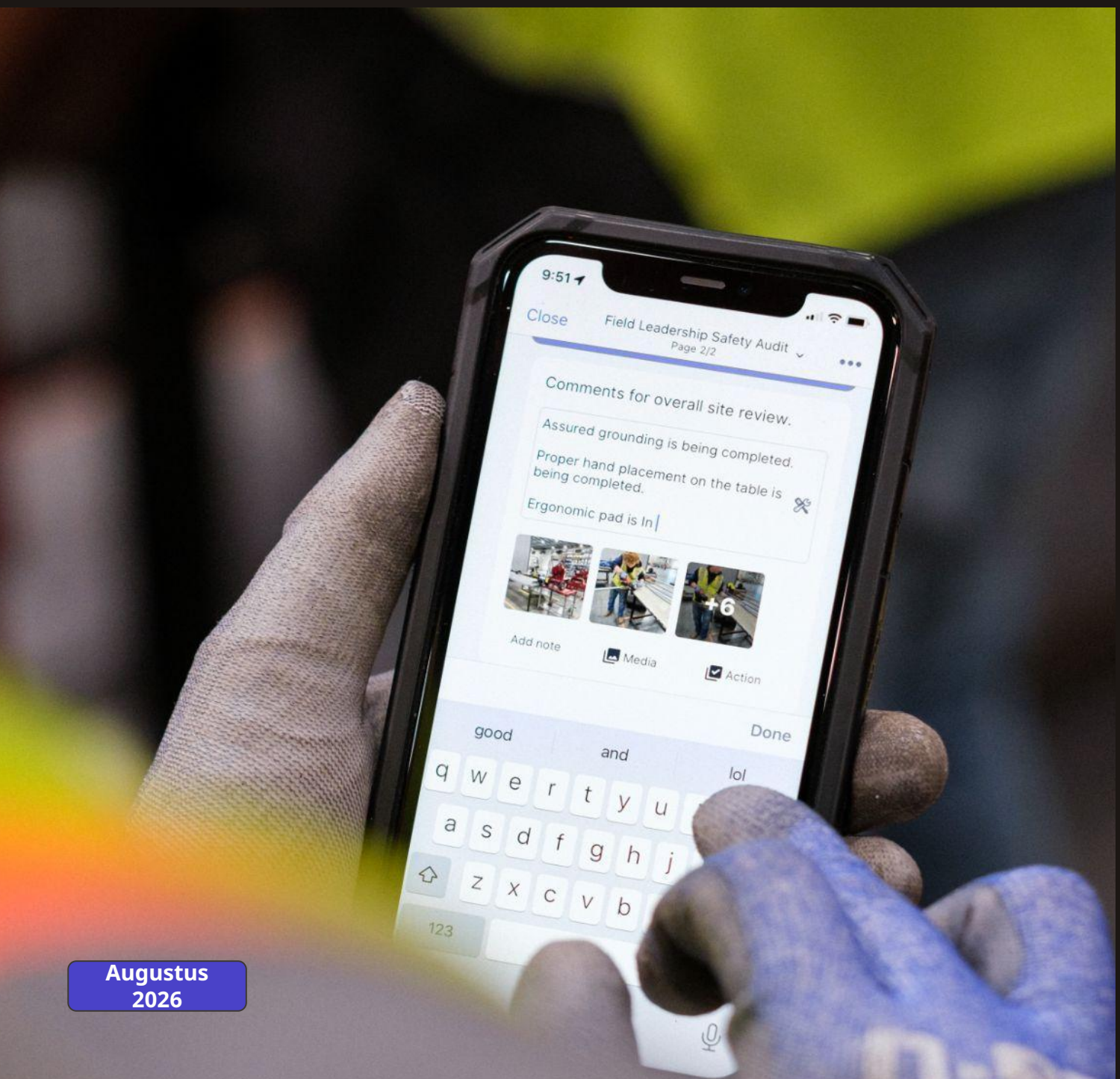
Mitti
by SafetyCulture

Veiligheidsoverzicht

Inzicht in de cyberbeveiliging van Mitti



Augustus 2026

Inhoudsopgave

> Voor Mitti hadden we iemand nodig die alle checklistgegevens invoerde zodra ze terugkwamen op kantoor, er vervolgens een Excel-analyse over uitvoerde en deze tenslotte met het team deelde. Analyse geeft ons uitgebreidere gegevens in één gebied die we kunnen delen.

Deaky Wong
Lijnonderhoudsmonteur, Cathay Pacific

Onze missie

De missie van Mitti is om bedrijven over de hele wereld te helpen veiligere en kwalitatief betere werkomgevingen te realiseren door middel van innovatieve, goedkope mobile first-producten.

We realiseren onze missie via onze Software-as-Service (SaaS) producten.

Onze producten worden gebruikt door meer dan 85.000 bedrijven wereldwijd in vele sectoren en in een verscheidenheid aan usecases.

We zijn er trots op dat Mitti wordt gezien als een wereldleider in producten die veiligheid en kwaliteit bevorderen. We weten hoe belangrijk het is om onze klanten te helpen hun dagelijkse activiteiten te verbeteren.

We zien onze benadering van cyberbeveiliging als een belangrijke pijler om onze status als leider op dit vlak te behouden. Deze inhoud vat samen hoe we cyberbeveiliging als organisatie benaderen.

Mitti is ISO 27001:2022-gecertificeerd en we volgen de Trust Services Criteria van AICPA, die onze toewijding aan de beveiliging van klanten bevestigen.

Overzicht

Cyberbeveiligingsprogramma

Mitti heeft een actief, robuust en continu verbeterend cyberbeveiligingsprogramma om ervoor te zorgen dat onze organisatie en de producten die we leveren veilig zijn. Het cyberbeveiligingsprogramma van Mitti maakt gebruik van verschillende controles op technisch en operationeel niveau om te zorgen voor een effectieve, diepgaande benadering om te beschermen tegen cyberaanvallen en om de gegevens te beveiligen die door onze Software-as-a-Service (SaaS) producten worden verwerkt.

De belangrijkste kenmerken zijn onder meer:

Een beveiligingsprogramma dat is afgestemd op de standaarden voor best practices van de sector, inclusief het gebruik van cloudplatformen die voldoen aan vertrouwde beveiligingsbenchmarks, waaronder ISO 27001 en SOC 2.

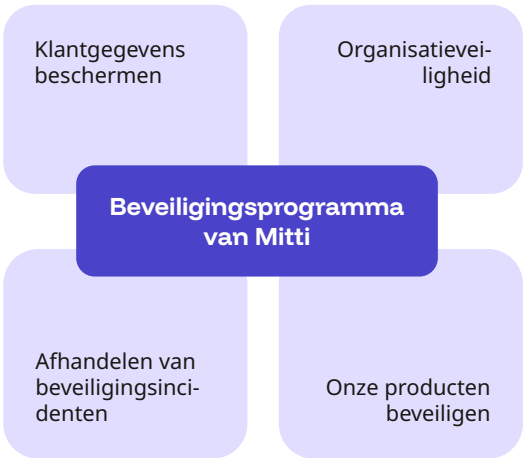
Een focus om de grondbeginselen correct te krijgen, en erkennen dat de basisprincipes van beveiliging het meest cruciaal blijven.

Dit houdt ondermeer in:

- Training van ons personeelsbestand over het belang van beveiliging.
- Beschikken over een toegewijd beveiligingsteam dat verantwoordelijk is voor het beschermen van onze organisatie tegen actuele en dreigende bedreigingen voor ons bedrijf en de gegevens die klanten ons toevertrouwen.
- Het implementeren van robuuste mechanismen om ervoor te zorgen dat de toegang tot de systemen en klantgegevens van Mitti zorgvuldig wordt gecontroleerd.
- Het versleutelen van de klantgegevens die we bewaren (zowel in overdacht als in rust).
- Ervoor zorgen dat we zo snel mogelijk patches installeren binnen onze IT-omgeving en producten om de kans dat cyberaanvallers gebruik maken van eventuele kwetsbaarheden, tot een minimum te beperken.
- Het actief monitoren en testen van onze IT-omgeving en producten op kwetsbaarheden en het met prioriteit verhelpen hiervan.
- Over een gedefinieerd proces beschikken om effectieve ondersteuning en responses te bieden in het geval van een beveiligingsincident.

Het toepassen van due diligence om ervoor te zorgen dat onze dienstproviders voldoen aan de sectorstandaarden als het gaat om beveiliging. We weten dat de beveiliging van onze partners rechtstreeks van invloed is op ons en onze klanten, dus we kiezen zeer zorgvuldig met wie we samenwerken.

De rest van dit document biedt een overzicht van de verschillende onderdelen van ons beveiligingsprogramma.



Organisatorische beveiligingspraktijken

Onze benadering van beveiliging als bedrijf is gericht op afstemming met aanbevolen best practices in erkende standaarden zoals NIST, ISO 27001 en SOC.

Beveiligingsbeheer

Mitti heeft een gedocumenteerde reeks beleidsregels, standaarden en procedures die onze benadering op het gebied van beveiliging als organisatie definiëren. Deze beleidsregels en procedures worden gedeeld met al het personeel en worden ten minste jaarlijks beoordeeld en bijgewerkt (en vaker wanneer materiële wijzigingen vereist zijn) om ervoor te zorgen dat onze benadering van beveiliging actueel blijft
.
We richten ons op het waarborgen van de verantwoordelijkheid op het gebied van beveiliging in ons hele bedrijf. Om dit te verwezenlijken hebben we een forum voor het beheer van informatiebeveiliging opgezet met belangrijke belanghebbenden uit de hele Mitti-organisatie die regelmatig bijeenkomen om beveiligingsgerelateerde zaken te beoordelen en bespreken en om beslissingen te nemen die van invloed zijn op onze benadering op het gebied van cyberbeveiliging.

Mitti is ISO 27001:2024-gecertificeerd en we volgen de Trust Services Criteria van AICPA, die onze toewijding aan de beveiliging van klanten bevestigen.

Toegangscontroles

Wij zorgen ervoor dat toegang tot systemen in onze IT-omgeving, inclusief de cloudplatformen die we gebruiken, beperkt is tot werknemers voor wie deze toegang specifiek vereist is voor hun werkzaamheden.

Voor alle beheerderstoegang is meervoudige verificatie vereist. Werknemers die toegang hebben tot onze omgeving zijn verplicht om een goedgekeurde VPN-oplossing te gebruiken.

Toegangsmachtigingen tot onze systemen worden regelmatig per werknemer beoordeeld en onmiddellijk gewijzigd. Als onderdeel van ons off-boardingproces wordt elke toegang tot systemen en diensten voor vertrekkende medewerkers ingetrokken.

Organisatorische beveiligingspraktijken

Beveiliging van derden

We beoordelen zorgvuldig de beveiligingspraktijken van derden die we inschakelen. In eerste instantie en actief om ervoor te zorgen dat hun praktijken voldoen aan sectorstandaarden en in overeenstemming zijn met ons eigen privacy- en beveiligingsbeleid en -procedures. Als een derde toegang tot onze systemen vereist, zorgen we ervoor dat die toegang specifiek wordt beperkt tot het doel waarvoor ze zijn ingeschakeld.

Aangezien Amazon Web Services (AWS) een van onze primaire providers is, werken we met ze samen op basis van het model voor gedeelde verantwoordelijkheid op het gebied van beveiliging en naleving. Zo zorgen we ervoor dat er een duidelijke definitie is van wie welke verantwoordelijkheid op zich neemt voor de beveiliging. AWS is geaccrediteerd door en voldoet aan veel van de nieuwste sectorstandaarden. Meer informatie kunt u hier vinden: .

Voor de verwerking van financiële en creditcardgegevens gebruikt Mitti meerdere partners (Zuora, eWay en Stripe) wiens beveiligingspraktijken voldoen aan de Payment Card Industry Data Security Standard (PCI-DSS).

Netwerkbeveiliging

De bedrijfsnetwerken van Mitti worden beschermd door firewalls en intrusion detection system (IDS) en intrusion prevention system (IPS) technologie aan de perimeter, geleverd door speciale netwerkbeveiligingsapparaten, zodat we kwaadaardig verkeer kunnen detecteren en ons ertegen kunnen beschermen.

Voor onze cloudgebaseerde platformen gebruiken we voornamelijk Amazon Web Services (AWS) die een meerlagige strategie bieden voor bescherming tegen aanvallen van buitenaf. Op infrastructuurniveau gebruikt AWS strategieën zoals toegangscontrole op netwerkapparaten, gegevensscheiding met behulp van firewalls en virtuele privéclouds om kwaadaardig verkeer uit te filteren en gebruik te maken van uitgebreide logging en bewaking om netwerkgebaseerde aanvallen te voorkomen. Op applicatieniveau profiteren we van s Web Application Firewall (WAF) en Distributed Denial of Service (DDoS) bescherming van Cloudflare om webgebaseerde en denial of service-aanvallen tegen onze producten te voorkomen..

We scheiden onze ontwikkel-, test- en productieomgevingen.

Organisatorische beveiligingspraktijken

Logging en monitoring

Mitti maakt gebruik van een gecentraliseerd logsysteem, dat auditgebeurtenissen voor toegang tot applicaties omvat.
Deze logs worden 90 dagen bewaard. We gebruiken ook Amazon Elastic Load Balancing (ELB) logboeken om servicetoegangsverzoeken bij te houden. Logboeken die zijn opgeslagen in AWS kunnen niet worden gewijzigd en de toegang is beperkt tot degenen voor wie dit vereist voor hun rolvereiste.

We erkennen het belang van het regelmatig controleren van logboeken om kwaadaardige gebruikersactiviteit en potentiële kwetsbaarheden met onze producten te identificeren; we hebben geautomatiseerde bewaking die ons waarschuwt voor specifieke soorten potentieel kwaadaardige gebeurtenissen binnen onze wereldwijde infrastructuur.

Beveiligingsbewustzijntraining

Al het personeel van Mitti volgt regelmatig een beveiligingsbewustzijntraining voor technische en niet-technische rollen. Aanvullend materiaal voor beveiligingstraining wordt verstrekt aan individuele werknemers waar dit verplicht is om ervoor te zorgen dat ze zijn toegerust om de specifieke uitdagingen van hun functie aan te pakken.

Patching- en kwetsbaarheidsbeheer

Het patchen van onze IT-omgeving is een van de belangrijkste maatregelen die we nemen om beveiligd te blijven tegen
een mogelijke inbreuk op de beveiliging. Om dit te realiseren:

- We gebruiken AWS System Manager om regelmatig patches voor onze cloudgebaseerde infrastructuur te implementeren.
- We maken gebruik van oplossingen voor het beheer van mobiele apparaten (MDM) om ervoor te zorgen dat belangrijke patches zo snel en efficiënt mogelijk worden geïnstalleerd.
- Onze apparaten zijn beveiligd met eindpuntbeveiligingstechnologieën om beveiligingsbedreigingen, waaronder virussen en malware-aanvallen, te detecteren en te voorkomen, en om te monitoren op kwaadwillende activiteit.
- We installeren eerst patches voor de meest kritieke kwetsbaarheden, met patches die worden geïnstalleerd in onze niet-productieomgeving voor eerste tests, waarna ze snel door de IT-omgeving wordt verspreid.

Beschermen van gegevens van klanten

Mitti neemt de beveiliging van klantgegevens uiterst serieus. We ondernemen verschillende stappen om ervoor te zorgen dat klantgegevens zorgvuldig worden beschermd.

Onze klantgegevens beschermen

Toegang tot gegevens beperken

Mitti implementeert technische en organisatiecontroles om klantgegevens te helpen beschermen tegen ongepaste toegang of ongepast gebruik door onbevoegde personen (zowel extern als intern). Klantgegevens worden alleen opgeslagen in onze productieomgeving. Toegang tot die gegevens door Mitti-werknemers is beperkt tot uitsluitend degenen voor wie toegang vereist is om hun standaartaken uit te voeren. Toegang tot klantgegevens wordt beheerd met behulp van tools voor toegangscontrole en authenticatie (inclusief het gebruik van tweefactorauthenticatie) geleverd door Amazon Web Services en onze andere cloudpartners.

Klantgegevens worden alleen gebruikt voor doeleinden die verenigbaar zijn met het leveren van de gecontracteerde diensten, zoals het oplossen van technische ondersteuningsverzoeken. Raadpleeg voor volledige details het Mitti-privacybeleid, dat hier te vinden is:

Wanneer Mitti-supportwerknemers toegang nodig hebben tot specifieke klantgegevens (voor probleemoplossing of supportdoeleinden), vereist Mitti altijd toestemming van een klant voordat deze toegang krijgen tot deze gegevens.

We slaan geen financiële gegevens van klanten op en cachen deze niet als ze worden gebruikt voor facturering via het Mitti-platform. Onze werknemers hebben geen directe toegang tot factureringsgegevens.

Fysieke toegang tot gegevens

Klantgegevens worden gehost op infrastructuur van Amazon Web Services, dat de beveiliging van hun sites handhaaft met behulp van best practice-controles in de sector, zoals uiteengezet op hun website voor beveiliging en naleving. Deze is hier te vinden: https://aws.amazon.com/architecture/security-identity-compliance/.

Op onze fysieke kantoorlocaties worden geen klantgegevens opgeslagen.

Gegevensversleuteling

Mitti heeft mechanismen geïmplementeerd om ervoor te zorgen dat de gegevens van onze klanten altijd worden beschermd.

In rust worden alle klantgegevens die in systemen zijn opgeslagen, versleuteld met behulp van AES-256, met sleutels die beheerd worden via de Key Management Service van Amazon Web Services. Alle gegevens worden veilig opgeslagen en zijn onderworpen aan het beveiligingsbeleid en -procedures van AWS.

Om gegevens tijdens overdracht te beschermen, gebruikt Mitti Transport Layer Security (TLS) en handhaaft het een minimum standaard van TLS v1.2 door middel van 128-bits versleutelingssleutels. We bieden support voor verbindingen met tot 256-bit versleutelingssleutels voor gebruik met een AES-versleuteling.

Gegevensback-ups

Van Mitti-gegevens worden dagelijks back-ups gemaakt naar ongelijksoortige oplossingen voor versleutelde gegevensopslag, geleverd door Amazon Web Services. Back-ups worden gerepliceerd naar meerdere AWS-faciliteiten en gedurende minimaal 30 dagen bewaard.

Toegang tot gegevensback-ups is beperkt tot uitsluitend die specifieke werknemers van Mitti voor wie die toegang nodig is als onderdeel van hun rolvereiste. Back-ups zijn versleuteld en worden opgeslagen als alleen-lezen.

Wissen en verwijderen van gegevens

Onze klantgegevens worden opgeslagen in, en zijn onderworpen aan, de wis- en verwijderingsprocedures van Amazon Web Services. Deze procedures omvatten een proces om beveiligde verlopen media te wissen. De gewiste media wordt vervolgens geïnspecteerd om een succesvolle vernietiging van gegevens te garanderen.

Hardware die eigendom is van Mitti en die vertrouwelijke gegevens bevat - waaronder Mitti-back-ups - is onderworpen aan de logische gegevensvernietiging volgens sectorstandaarden voordat deze wordt gerecycled.

Onze producten beveiligen

We erkennen dat voor de meerderheid van de klanten hun belangrijkste ervaring met Mitti plaatsvindt via onze producten. Beveiliging vormt een belangrijk onderdeel van de manier waarop onze producten worden ontwikkeld en werken.

Veilige softwareontwikkelingspraktijken

Als onderdeel van ons productontwikkelingsproces wordt elke code- en infrastructuurwijziging opgeslagen in een broncontrolesysteem, geversioneerd, beoordeeld en geëvalueerd op de impact voordat de wijziging in productie wordt genomen. Deze beoordeling omvat de naleving van best practices op het gebied van beveiliging. We scheiden ook onze ontwikkel-, test- en productieomgevingen en we gebruiken geen klantgegevens in onze niet-productieomgevingen.

Wijzigingsbeheer

Alle wijzigingen in de Mitti-producten worden tijdens hun ontwikkeling actief getest om ervoor te zorgen dat de impact op de eindgebruikers voorafgaand aan de implementatie wordt geëvalueerd. Belangrijke wijzigingen worden opgenomen in de productiereleasienotities.

Mitti maakt gebruik van systemen voor versiebeheer en het bijhouden van wijzigingen om wijzigingen in de codebasis of configuratie van onze infrastructuur actief te monitoren en beheren. We gebruiken geautomatiseerde processen om wijzigingen in onze omgevingen door te voeren en wijzigingen kunnen, indien nodig, ongedaan gemaakt worden. We gebruiken Amazon CloudTrail om eventuele onderliggende configuratiewijzigingen in het cloudplatform waarop onze producten werken bij te houden.

Identificatie van kwetsbaarheden en patchontwikkeling

We werken er hard aan om het aantal kwetsbaarheden in onze producten te minimaliseren. We erkennen dat het belangrijk is om proactieve stappen te ondernemen om ervoor te zorgen dat we eventuele kwetsbaarheden zo snel mogelijk aanpakken. Om dit te verwezenlijken voert Mitti jaarlijkse penetratietests uit en test en monitort het actief onze applicaties op kwetsbaarheden.
We voeren particuliere bug programma's voor het opsporen van bugs uit omdat een community van onafhankelijke beveiligingsonderzoekers die gestimuleerd wordt om onze producten actief te testen om mogelijke Issues te identificeren, de beveiliging van onze producten alleen maar versterkt.

Wanneer een kwetsbaarheid wordt geïdentificeerd (intern of extern), wordt het probleem gevolgd en geprioriteerd op basis van de mogelijke ernst en de impact op onze klanten. Voor ossues met een kritieke ernst kan dit inhouden dat onze ontwikkelaars dag en nacht doorwerken totdat het issue is verholpen.

Patches voor problemen worden ontwikkeld en vrijgegeven in de productieomgeving via een voordurend integratieproces (CI/CD) en zo snel mogelijk toegepast.

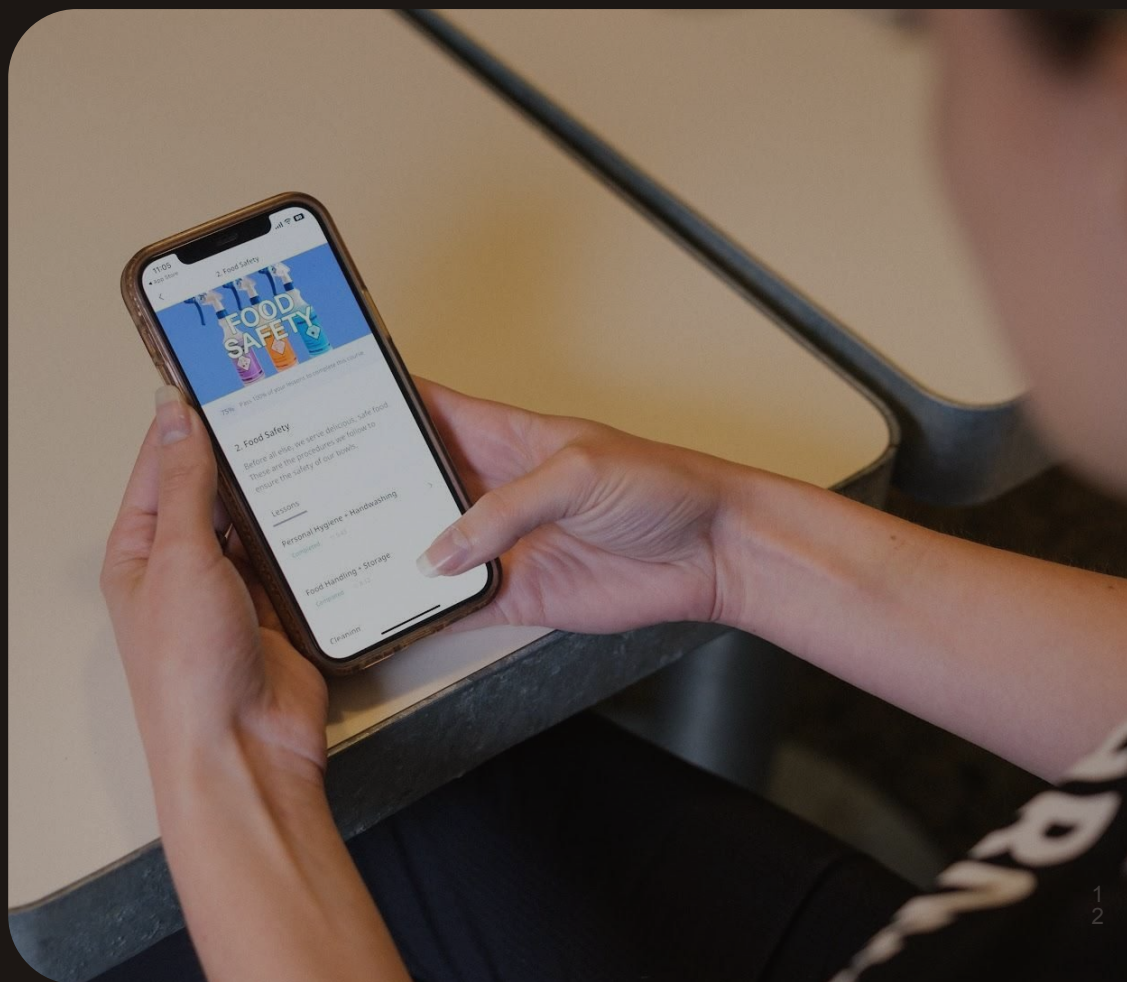
Afhandelen van beveiligingsincidenten

Hoewel we ons uiterste best doen om beveiligingsincidenten te voorkomen, erkennen we dat we ook voorbereid moeten zijn om deze incidenten aan te pakken als ze zich voordoen, om de potentiële impact op onze klanten en Mitti tot een minimum te beperken.

We hebben een reeks maatregelen getroffen, waaronder:

- Een gedocumenteerde procedure voor incidentbeheer die ons proces definieert voor het omgaan met de vertrouwelijkheid, integriteit en beschikbaarheid van onze IT-omgeving en producten.
- Beschikken over een wereldwijde organisatie om ondersteuning te bieden tijdens een incident.
- Gevestigde rampenherstelplannen en noodstrategieën die kunnen worden uitgevoerd om ons te helpen de continuïteit van de operaties tijdens een incident te handhaven. Dit omvat het gebruik van meerdere geografische beschikbaarheidszones via Amazon Web Services en de replicatie van gegevens verspreid over meerdere systemen in elke zone. Dit zorgt voor continue gegevenstoegang tijdens incidenten die de systeembeschikbaarheid beïnvloeden en biedt gegevensredundantie bij storingen van het systeem of de gegevensopslag.

Mitti waarschuwt getroffen klanten onmiddellijk over grote incidenten die van invloed zijn op de beschikbaarheid van de Mitti-diensten of -gegevens en over alle incidenten die de vertrouwelijkheid en integriteit van hun gegevens beïnvloeden.



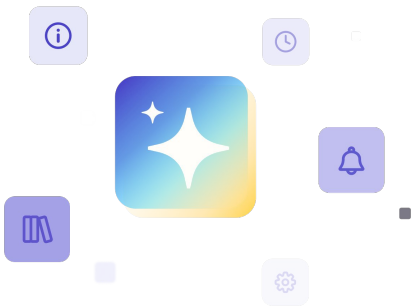
"We hebben zicht op alles wat we doen vanwege de gegevens die we vastleggen met behulp van Mitti. Als er een drempeluitzondering of een proces is dat verbeterd moet worden, hoeven we alleen maar dieper te gaan en vinden we het."

Sofia Dias
Manager voedselveiligheid en kwaliteitsborging

Marley Spoon

Mitti en AI

Mitti innoveert continu en brengt op een veilige en beveiligde manier nieuwe functies en technologieën naar onze klanten. Dit omvat functies met kunstmatige intelligentie (AI). Bij Mitti willen we transparant zijn met onze klanten over hoe we AI gebruiken om onze producten te bouwen en hoe we AI gebruiken om de ervaring van onze gebruikers te verbeteren.



Hoe Mitti AI gebruikt

Met AI kan Mitti de ontwikkeling van onze functies versnellen, handmatig werk automatiseren, tooling verbeteren en betere klantresultaten mogelijk maken.

We gebruiken zelf gehoste AI-infrastructuur en externe AI-providers.

AI-functies in Mitti

Binnen Mitti hebben we AI die gebruikers kan helpen vragen te stellen over hun gegevens, samenvattingen te genereren, inhoud te maken, te vertalen, inzichten te vinden en aanbevelingen te krijgen.

AI-providers en beveiliging

Mitti maakt gebruik van large language models (LLM's) die worden gehost door Mitti en externe organisaties zoals Anthropic, Google en AWS.

We evalueren continu LLM-providers en hun modellen om de hoogste kwaliteit ervaring aan onze gebruikers te bieden. Derden die klantgegevens verwerken, inclusief de externe AI-diensten, worden gepubliceerd op onze subverwerkerspagina. Deze is hier te vinden:

Toegang en controles

AI-functies zijn machtigingsbewust en respecteren bestaande machtigingsstructuren, zodat gebruikers alleen toegang hebben tot de inhoud waartoe ze geautoriseerd zijn. Alleen geautoriseerde gebruikers, zoals beheerders, kunnen machtigingen bijwerken en de toegang van een gebruiker tot AI-functies verlenen of verwijderen.

Klantgegevens en trainingmodellen

Klanten bepalen welke gegevens worden doorgegeven aan AI-providers en hoe ze de resultaten van AI-verwerking gebruiken.

Mitti staat niet toe dat externe diensten klantgegevens gebruiken om de modellen die we gebruiken te trainen.

Extra bronnen

Mitti is toegewijd om transparant te zijn met onze klanten over onze producten en hoe we AI gebruiken om de ervaring van onze gebruikers te verbeteren. Als u geïnteresseerd bent, vindt u hier aanvullende bronnen:

- AI in Mitti
- Uw gegevens in Mitti
- Subverwerkers van uw gegevens

Conclusie

Mitti beschouwt cyberbeveiliging als een fundamenteel onderdeel van ons bedrijf en van de diensten die we aan bedrijven over de hele wereld leveren. Hoewel de controles en maatregelen die we hebben ingevoerd veel verder gaan dan wat hier wordt behandeld, dient deze inhoud om een algemeen overzicht te geven van de veelzijdige benadering die we toepassen en onze toewijding aan beveiliging.

Als u vragen heeft over deze Inhoud of meer informatie vereist over onze benadering van support, beveiliging of privacy, neem dan contact met ons op via de onderstaande gegevens.

- **Support:** support@mitti.com
- **Privacy:** privacy@mitti.com

Om beveiligingsissues te rapporteren, kunt u contact met ons opnemen via

Meer lezen

Onze beveiligingspagina: https://www.mitti.com/nl/beveiliging

Ons privacyportaal: https://www.mitti.com/nl/juridisch/privacyportaal

Onze dienstentatuspagina: https://status.mitti.com