DECLARAÇÃO de Medidas Técnicas e Organizacionais de Segurança de Dados

Histórico das revisões

Versão	Data	Editor	Alterações	Aprovado por
8,3	23/01/2023	Naveen Pillai	Incluído o certificado do Cyber Essentials na seção sobre recursos	Alan Cawse
8,4	15/03/2023	Neeraj Sharma	Adicionada a seção Fale com a Geotab e alterações aprovadas na seção Lat-Lon no Apêndice 3.	Alan Cawse
8,5	10/05/2023	Neeraj Sharma	Seções Lat-Lon atualizadas no Apêndice 3 para refletir as alterações sugeridas pelo departamento jurídico.	Alan Cawse
8,6	14/07/2023	Hari Krishnan	Atualizado o padrão de criptografia para AES-128 na seção Transmissão de dados, no Apêndice 3: Medidas de segurança do sistema Lat-Lon conforme confirmadas pela AVP, Engenharia	Alan Cawse
8,7	04/06/2024	Vani Bhatia	Informações de contato de segurança atualizadas, diagrama de arquitetura para Lat-Lon, Apêndice 1: A seção Segurança do dispositivo MyGeotab & GO foi atualizada, removido o Apêndice 2, seção “Medidas de segurança do iGestion e uReaderGPS”	Alan Cawse

Este documento foi escrito originalmente em inglês e expressa melhor as intenções das partes em inglês. Portanto, em caso de discrepância entre esta tradução e a versão em inglês, a versão em inglês prevalecerá na medida da inconsistência. A versão em inglês pode ser acessada pelo seguinte link:

https://docs.google.com/document/d/1b8F7XB86Z0h8xyD4GF3wH3vzwtdzMhKb-SmhYkz8lGs/edit#

Isenção de responsabilidade importante

Esta Declaração está sujeita a alterações e pode ser atualizada com frequência. Por si só, esta Declaração não cria obrigações ou responsabilidades vinculativas à Geotab ou aos revendedores, usuários finais da Geotab ou qualquer outra parte. Para obter mais informações sobre a finalidade deste documento, consulte a Introdução. Este documento não deve ser distribuído em nenhum formato que não seja uma versão em tempo real acessível pelo Google Docs. A versão em tempo real está sempre disponível em https://www.geotab.com/pt-br/segurança/.

Introdução

Esta Declaração de Medidas Técnicas e Organizacionais de Segurança de Dados da Geotab (conhecida como "TOMS") traz uma visão geral das medidas técnicas e organizacionais de segurança de dados implementadas pela Geotab Inc. ("Geotab" ou "nós") como nossa abordagem padrão. Por si só, esta declaração não deve criar quaisquer direitos ou prerrogativas para ninguém. Se a Geotab e seus clientes incorporarem esta declaração por referência em um contrato, então os direitos e obrigações das partes serão determinados com base nesse contrato. As medidas de segurança relacionadas a produtos Geotab específicos são descritas nas seções do Apêndice.

Uso permitido

Este documento somente pode ser usado para fins internos de clientes relacionados aos produtos e serviços específicos da Geotab. Este documento passa por atualizações frequentes. Esta declaração não pode ser copiada ou duplicada sem a permissão expressa por escrito da Geotab.

Perguntas ou feedback

Envie suas dúvidas, feedback ou qualquer outra informação pelo formulário na parte inferior da página: https://www.geotab.com/pt-br/segurança/.

Medidas e controles comuns de segurança

As medidas e os controles de segurança descritos nesta seção seguem a abordagem padrão da Geotab aplicada horizontalmente a todos os produtos e serviços da Geotab, a menos que especificamente descrito nas seções do Apêndice.

Políticas para funcionários da Geotab

A Geotab implementa medidas e políticas para garantir que todos os funcionários da empresa sejam treinados e estejam totalmente cientes de todas as políticas relacionadas à segurança e privacidade, e que somente pessoas específicas tenham acesso a áreas específicas dentro da rede e dos sistemas. Para realizar isso:

- Os funcionários da Geotab recebem credenciais muito limitadas, e apenas recebem credenciais adicionais, quando necessário, mediante análise e treinamento,
- Todas as senhas de funcionários da Geotab devem ter pelo menos 12 caracteres, conter pelo menos um número, uma letra maiúscula, um caractere não alfanumérico e não devem conter palavras/nomes de usuário comumente usados,
- Somente funcionários autorizados da Geotab podem obter acesso a áreas seguras dentro do sistema MyGeotab,
- Todas as credenciais de usuário não utilizadas ou inativas serão automaticamente desativadas após 90 dias,
- Todos os funcionários da Geotab passam por verificações de antecedentes totalmente aprovadas e sancionadas pelo governo,
- Todos os funcionários da Geotab passam por um treinamento regular de conscientização sobre segurança,
- Todos os direitos de acesso seguem o princípio de privilégio mínimo,
- Todas as solicitações de acesso devem passar por um processo de autenticação multifator para garantir que as credenciais não tenham sido comprometidas,
- Todas as solicitações de acesso são cronometradas, auditadas e registradas, e
- Um processo formal de desligamento é imediatamente seguido para qualquer pessoa desligada visando a garantir que todos os acessos, direitos, permissões e dados não estejam mais disponíveis para ela.

Todos os principais funcionários de engenharia de soluções de suporte e engenharia da Geotab estão localizados atualmente em Ontário, no Canadá. A Geotab também tem funcionários de engenharia sediados em outras partes do mundo, incluindo Colúmbia Britânica (Canadá); Nevada, Nova York (EUA); Munique, (Alemanha); Londres (Reino Unido); e Madri (Espanha).

Segregação de funções

A Geotab implementa controles internos para minimizar os riscos associados aos funcionários da empresa que acumulam privilégios excessivos dentro da rede ou do sistema. Sempre que possível, os privilégios são divididos entre vários usuários para garantir que nenhum funcionário da Geotab sozinho seja capaz de controlar completamente um processo do início ao fim. Quando essa divisão não é possível, o acesso e uso são analisados regularmente. Além disso, todas as solicitações de acesso ao servidor exigem aprovação e o acesso é concedido apenas por um período limitado. Os logs de acesso são mantidos para todos os servidores e sistemas.

Provedores de data centers e serviços de tecnologia

A Geotab armazena dados em serviços de nuvem pública atualmente operados pelo Google (Compute Engine), localizados nos EUA, Canadá, Europa e Ásia. Esses provedores de nuvem não permitem visitas de terceiros a suas dependências e somente pessoal autorizado pode ter acesso aos locais de seus próprios servidores físicos.

A Geotab pode utilizar várias regiões e adicionar data centers, conforme necessário, por motivos de desempenho, balanceamento de carga ou segurança. No entanto, eles sempre atenderão aos nossos rigorosos requisitos de segurança e redundância.

A Geotab também usa serviços de mapeamento, provedores de tecnologia sem fio e de informação (incluindo, sem limitação, provedores de segurança de rede e de controle de intrusão) para operar a plataforma de tecnologia da Geotab. Os provedores de serviços são impedidos por medidas tecnológicas, organizacionais e contratuais de

acessar ou visualizar dados pessoais de clientes.

Segurança na nuvem pública

A Geotab utiliza serviços de ponta de nuvem públicos para ajudar a cumprir seus compromissos de serviço em todo o mundo. Para tal, a Geotab estabeleceu uma parceria com o Google para utilizar a tecnologia GCP (Google Cloud Platform), que inclui Compute Engine e BigQuery, e vários data centers.

A Geotab usa o Google Compute Engine para fornecer recursos de computação para hospedagem de aplicativos e dados. Esses serviços estão de acordo com as políticas de segurança globais extremamente rigorosas e líderes mundiais do Google, o que ajuda a Geotab a manter os dados dos seus clientes seguros e protegidos. Alguns dos principais recursos dos programas de segurança do Google incluem:

- Equipe dedicada de Segurança da Informação, composta por especialistas em segurança da informação, aplicativos e rede de alto nível,
- Todos os data centers do Google apresentam um modelo de segurança em camadas, incluindo proteções como cartões de acesso eletrônico personalizados, alarmes, detecção de intrusão por feixe laser e biometria,
- Controles exclusivos de acesso a dados para ajudar a proteger a segurança das informações do cliente,
- A detecção de intrusão do Google envolve controlar rigorosamente o tamanho e a composição da superfície de ataques do Google por meio de medidas preventivas, empregando controles de detecção inteligentes nos pontos de entrada de dados e tecnologias que remediam automaticamente determinadas situações perigosas, e
- O Cloud Platform e a infraestrutura do Google são certificados para um número cada vez maior de padrões e controles de conformidade e passam por várias auditorias independentes de terceiros para testar a segurança, a privacidade e a segurança dos dados.

Clique aqui para obter mais informações sobre a segurança do Google Cloud Platform.

O relatório SSAE Tipo II SOC 2 do Google pode ser fornecido mediante solicitação, sob um acordo de confidencialidade, pela Geotab. Informações adicionais de conformidade podem ser encontradas no Site de Conformidade do Google, localizado aqui.

Controle de acesso de áreas de processamento

Os data centers do parceiro de nuvem pública da Geotab não são acessíveis por pessoas externas e não autorizadas, incluindo pessoal da Geotab. Esses data centers utilizam acesso de segurança e controles de prevenção de última geração para impedir que os equipamentos de processamento de dados (ou seja, servidores de bases de dados e de aplicativos e hardware relacionado) sejam acessados por pessoas não autorizadas.

Clique aqui para obter mais informações sobre a segurança de Data Center do Google.

Controle de acesso a sistemas de processamento de dados

A Geotab implementa medidas adequadas para impedir que seus sistemas de processamento de dados sejam usados por pessoas não autorizadas. Isso é alcançado por meio de:

- Identificação do terminal e/ou do usuário do terminal nos sistemas da Geotab,
- Encerramento de sessão automático do terminal do usuário se ele permanecer inativo, e identificação, senha e fator adicional necessários para reabri-lo,

- Desativação automática do ID de usuário quando várias senhas incorretas são inseridas, arquivo de log de eventos (monitoramento de tentativas de invasão),
- Emissão e proteção de códigos de identificação,
- Dedicação de terminais individuais e/ou usuários de terminais, características de identificação exclusivas para funções específicas, e
- Todo o acesso ao conteúdo de dados é registrado, monitorado e rastreado.

A Geotab mantém uma lista de pessoas que têm acesso aos dados dos Clientes. A Geotab concede direitos de acesso somente a um número limitado de pessoas.

Controle de Acesso para Uso de Áreas Específicas dos Sistemas de Processamento de Dados

A Geotab estabelece que as pessoas autorizadas a usar seus sistemas de processamento de dados somente podem acessar os dados dentro do escopo e na medida prevista pela respectiva permissão (autorização) de acesso, e que dados pessoais não podem ser lidos, copiados, modificados ou removidos sem autorização. Isso é alcançado por meio de:

- Políticas regulares para os funcionários e treinamento a respeito dos direitos de acesso de cada funcionário aos dados pessoais,
- Alocação de terminais individuais e/ou usuário do terminal e características de identificação exclusivas a funções específicas,
- Capacidade de monitoramento em relação a pessoas que excluem, adicionam ou modificam os dados pessoais,
- Ação disciplinar medida e efetiva contra indivíduos que acessam dados pessoais sem autorização,
- Liberação de dados somente para pessoas autorizadas,
- Controle de arquivos, destruição controlada e documentada de dados, e
- Políticas controlando a retenção de cópias de backup.

Controle de transmissão de dados

A Geotab implementa medidas adequadas para impedir que os dados dos serviços de nuvem e do dispositivo sejam lidos, copiados, alterados ou excluídos por partes não autorizadas durante sua transmissão ou durante o transporte da mídia de dados. Isso é alcançado por meio de:

- Uso de tecnologias adequadas de firewall e criptografia para proteger os gateways e pipelines através dos quais os dados circulam, e
- Monitoramento da integralidade e da exatidão da transferência de dados (verificação ponta a ponta).

Confira nos Apêndices os controles de transmissão de dados dos produtos específicos.

Monitoramento do acesso

A Geotab implementa medidas adequadas para monitorar as restrições de acesso dos administradores de sistema da Geotab e garantir que eles ajam de acordo com as instruções recebidas. Isso é alcançado por meio de:

- Nomeação individual dos administradores de sistema,
- Adoção de medidas adequadas para registrar os logs de acesso dos administradores do sistema à infraestrutura e mantê-los seguros, precisos e não modificados por pelo menos seis meses,

- Auditorias regulares das atividades dos administradores de sistema para avaliar a conformidade com as tarefas atribuídas, as instruções recebidas pelo importador e as leis aplicáveis, e
- Manutenção de uma lista atualizada com os detalhes de identificação dos administradores de sistema (ex: nome, sobrenome, função ou área organizacional) e tarefas atribuídas.

Monitoramento dos sistemas

Todos os servidores da Geotab são monitorados 24 horas por dia, 365 dias por ano, por sistemas de monitoramento totalmente redundantes e pela equipe de engenharia interna. Todos os servidores são desenvolvidos com o uso de uma compilação padrão e aprovada do Windows Server ou servidor Linux, que foi reforçada para garantir que todos os serviços redundantes ou não utilizados estejam desativados e que portas desnecessárias estejam fechadas.

Todas as atualizações e patches de software são testados em um ambiente contido e, em seguida, enviados aos servidores da Geotab mensalmente para garantir que eles estejam executando os patches, programas e aplicativos mais recentes e seguros.

Todos os servidores são gerenciados e mantidos usando agentes líderes de mercado e customizados internamente, que fornecem monitoramento de segurança e proteção contínuos, incluindo detecção/prevenção de intrusão do Host (HIDS), anti-malware (atualizado automaticamente), scan contínuo de vulnerabilidades (interno e externo) e ferramentas de Gerenciamento de Eventos de Informações de Segurança (SIEM), e monitoramento personalizado de eventos e logs.

Testes de penetração/scans de vulnerabilidades

A Geotab realiza testes externos de penetração anualmente em toda a sua rede e em todos os aplicativos e GOs da Geotab por meio de parceiros de segurança confiáveis para garantir que os sistemas permaneçam seguros e contidos.

A Geotab realiza testes sistemáticos de vulnerabilidade em todos os seus servidores de produção (verificação contínua) e em suas imagens de servidor pré-lançamento para garantir a manutenção dos processos e que nenhum possível risco de segurança ou privacidade seja criado. Quaisquer vulnerabilidades descobertas durante o processo são mitigadas e testadas novamente antes da imagem ser lançada para produção.

A Geotab tem um programa de recompensa ativo e privado para seus aplicativos MyGeotab e MyAdmin, fornecendo um ambiente sandbox dos seus aplicativos mais recentes para vários pesquisadores de segurança externos, permitindo que eles os analisem, verifiquem e tentem violá-los. Todas as vulnerabilidades descobertas são prontamente verificadas, priorizadas e tratadas em tempo hábil.

Nenhum scan de porta, teste de vulnerabilidade ou teste de penetração de terceiros pode ser feito em quaisquer serviços, servidores ou ativos da Geotab sem a aprovação expressa por escrito da Geotab e de seus parceiros de hospedagem.

Auditorias

A Geotab realiza auditorias internas regulares em suas políticas e procedimentos de segurança. Durante a auditoria, todos os funcionários da Geotab recebem treinamento de conscientização sobre segurança e sensibilidade; as políticas internas de segurança, os processos de atualização de segurança e os processos de monitoramento de servidor são revisados.

As políticas de segurança das informações são analisadas anualmente. O treinamento e o teste de conscientização

dos funcionários são realizados regularmente ao longo do ano.

Incidentes de segurança

No caso de uma violação de segurança, a equipe de engenharia da Geotab pode cortar alguns ou todos os acessos aos serviços da Geotab para mitigar quaisquer possíveis danos de intrusão. Uma vez que a ameaça tenha sido contida ou neutralizada, será realizada uma investigação criteriosa e imediata por uma equipe de alto nível da Geotab, especificamente para determinar os nomes e/ou a localização dos invasores, os métodos de violação, que tipo de dados foram expostos (se houver) e os clientes que podem ter sido afetados.

Se a Geotab determinar que os dados dos clientes foram acessados por pessoas não autorizadas, ela informará os clientes afetados imediatamente (dentro de 24 horas), conforme exigido pela lei aplicável, e trabalhará com eles para garantir que os dados sejam protegidos, movidos, removidos ou alterados.

O Programa de Resposta a Incidentes da Geotab (GRIP) foi desenvolvido de acordo com a Publicação Especial NIST 800-61 Revisão 2: Guia de Tratamento de Iincidentes de Segurança em Computador e projetado para estar alinhado às melhores práticas do mercado. A Geotab está o comprometida em melhorar e atualizar continuamente nossos recursos de Resposta a Incidentes ao incorporar lições aprendidas de respostas anteriores ocorridas tanto internamente quanto na comunidade de segurança mais ampla.

Qualquer informação ou conhecimento sobre qualquer suspeita de vulnerabilidade, violação ou tentativa de violação de segurança, ou qualquer outra informação que possa estar relacionada à Geotab e aos seus serviços, pode ser encaminhada para security@geotab.com.

Divulgação responsável

A Geotab leva muito a sério segurança e a transparência e aprecia os esforços contínuos de indivíduos ou entidades que estudam segurança e/ou vulnerabilidades de segurança (conhecidos como “Pesquisadores de Segurança”). Para melhor atender a esses Pesquisadores de segurança, a Geotab desenvolveu um programa para facilitar a comunicação de vulnerabilidades e reconhecer esses pesquisadores por seus esforços para tornar a Internet um lugar mais seguro. Esta política fornece as diretrizes da Geotab para relatar vulnerabilidades.

Para obter mais informações sobre o Programa de Divulgação de Vulnerabilidades da Geotab, acesse a página Política de divulgação responsável (em inglês) em nosso site.

Continuidade dos negócios

Os membros da gestão sênior da Geotab supervisionam o planejamento da continuidade do negócio para garantir que os serviços fundamentais possam ser continuamente entregues aos clientes.

A Geotab conduz uma análise regular de impacto no negócio para entender o cenário relevante de ameaças/riscos e priorizar o planejamento. Isso inclui ciberataques, sabotagem, interrupção de energia/utilidades, terrorismo e falha aleatória em sistemas críticos.

A Geotab implementa planos, medidas e acordos adequados para garantir a continuidade do negócio, incluindo:

- Serviços de data center em vários locais,
- Energia totalmente redundante com geradores de reserva (data centers),
- Provedores de rede de várias fontes (data centers),
- Equipamento de rede e hardware do servidor redundantes,

- Disponibilidade de opções de armazenamento de backup externo para clientes (mediante solicitação),
- Uso da tecnologia em nuvem para os negócios da Geotab (disponível em qualquer lugar),
- Sistema de monitoramento interno e redundante (monitora todos os servidores de produção, alertas de segurança e outros problemas críticos),
- Suporte de engenharia de prontidão 24 horas por dia, 7 dias por semana, 365 dias por ano para todos os serviços críticos (engenheiros e desenvolvedores), e
- Planos de recuperação de desastre por falha do servidor: permite alternar para hardware redundante.

A Geotab realiza testes mensais limitados de planos de recuperação de desastres. Para mais informações sobre o Plano para recuperação de desastres da Geotab, consulte a POLÍTICA Plano para recuperação de desastres (GRIDIRON) (em inglês).

Filiações e Assinaturas de Grupos de Interesses Especiais

A Geotab tem o compromisso de se manter atualizada e ciente de todas as vulnerabilidades e riscos conhecidos relacionados à cibersegurança e segurança da informação. Como parte desses esforços contínuos, a Geotab mantém relações diretas ou indiretas com muitas organizações, incluindo, entre outras:

- US-CERT (vulnerabilidades e alertas),
- Duo (segurança relacionada a IAM),
- SecurityMetrics (Scans de rede PCI-DSS),
- Comitê de Segurança de Sistemas Elétricos da SAE (hacks/vulnerabilidades de cibersegurança de veículos),
- NMFTA (segurança cibernética de caminhões pesados),
- Auto-ISAC (Compartilhamento e Análise de Informações de Segurança de Automóveis), e
- DOT-Volpe (segurança cibernética de caminhões pesados).

Fale com a Geotab

A Geotab trata com seriedade a segurança e o suporte ao cliente, comprometendo-se em fornecer ao cliente a melhor experiência possível. Veja os contatos apropriados na tabela a seguir, conforme a sua consulta:

Tipo de consulta	Informações de contato
Incidentes graves de segurança (24 horas por dia, 7 dias por semana)	incident@geotab.com
Enviar vulnerabilidades de segurança	Política de divulgação responsável
Suporte geral de segurança	Use o formulário no final da página: https://www.geotab.com/pt-br/segurança/
Serviços gerais de plantão da Geotab	Guia de serviços de emergência da Geotab (em inglês)
Consultas gerais	Fale conosco

Fóruns de suporte	Geotab Community

Para solicitar uma cópia em formato PDF, use o formulário no final da página: https://www.geotab.com/security/. Todas as cópias serão marcadas com uma data de expiração específica. Todos os leitores são incentivados a acessar este documento em tempo real periodicamente.

A equipe de suporte da Geotab está disponível para ajudar com qualquer dúvida ou problema. Não medimos esforços para oferecer um suporte oportuno e eficaz, sempre procurando maneiras de melhorar nossa experiência de suporte ao cliente.

Se tiver algum feedback ou sugestão de como podemos melhorar nossa segurança ou suporte ao cliente, fale conosco. Estamos sempre prontos para ouvir nossos clientes e temos o compromisso de oferecer o melhor atendimento possível.

Recursos

Veja a seguir uma lista de recursos que incluímos como documentação complementar para análise:

- POLÍTICA Nível de serviço MyGeotab (Web)
- POLÍTICA Plano para recuperação de desastres (GRIDIRON)
- Política PROGRAMA de divulgação de vulnerabilidades da Geotab [PÚBLICO]
- Site de Segurança do Google Compute Engine
- Site de Segurança da Geotab
- Certificado de certificação ISO 27001 da Geotab
- Autorização Moderada do Nível FedRAMP da Geotab
- Validação FIPS 140-2 da Geotab para o módulo de criptografia em dispositivos GO
- Certificado de garantia Cyber Essentials da Geotab

Para solucionar dúvidas gerais, acesse a página Fale conosco em nosso site. Para conferir fóruns de suporte, acesse Comunidade Geotab para encontrar respostas e conectar-se com especialistas da Geotab.

Apêndice 1: Segurança do dispositivo MyGeotab & GO

Segurança de dados do GO da Geotab

A Geotab implementa medidas adequadas para impedir que quaisquer dados sejam lidos, copiados, alterados ou excluídos por partes não autorizadas durante a transmissão ou o transporte de quaisquer dados para/a partir do GO da Geotab. Para realizar isso:

- Todas as comunicações são seguramente autenticadas antes de qualquer transmissão. Todos os dados, sejam diretamente do próprio dispositivo, de dispositivos de terceiros conectados ou do servidor Gateway, são seguramente criptografados de ponta a ponta entre o dispositivo e o servidor Gateway seguro da Geotab com o uso de um algoritmo de criptografia AES-256 padrão de mercado,
- Os processos de autenticação e criptografia utilizam chaves de criptografia individuais, aleatórias e rotativas que são alteradas regularmente,
- Todo o firmware do GO da Geotab é assinado usando o algoritmo RSA 2048 e autenticado antes de ser atualizado no dispositivo. Essa ação protege o dispositivo contra firmware malicioso ou não autorizado,
- Nenhum GPS baseado na Geotab ou dado de motor transmitido contém nomes de motoristas ou outros dados confidenciais, e
- Todos os dados enviados entre o servidor Gateway e a base de dados do MyGeotab ocorrem por meio de uma conexão TLS segura e criptografada.

! IMPORTANTE: Quaisquer dados de dispositivos de terceiros enviados através do dispositivo GO conectado serão enviados e armazenados nos servidores da Geotab.

Medidas de segurança do sistema MyGeotab

Transmissão de dados

A Geotab implementa medidas adequadas para impedir que quaisquer dados sejam lidos, copiados, alterados ou excluídos por partes não autorizadas durante a transmissão ou o transporte de quaisquer dados para e a partir do MyGeotab. Para realizar isso:

- Todos os clientes hospedados se conectam ao MyGeotab por meio de um navegador web moderno, através de HTTPS (criptografia TLS para toda a comunicação para e a partir dos servidores hospedados),
- Todas as portas e serviços TCP e UDP de entrada (exceto portas e serviços específicos exigidos pelo aplicativo MyGeotab) estão desabilitados na rede Geotab,
- Todos os dispositivos voltados para o público são protegidos por firewall conforme o padrão do setor, monitorados 24 horas por dia,
- Todos os servidores voltados para a Internet são separados dos sistemas internos da Geotab por dois firewalls, e
- Os engenheiros de suporte da Geotab se conectam via GCP IAP, com acesso controlado pelo diretório interno da Geotab.

Acesso ao sistema

A Geotab implementa medidas adequadas para impedir o acesso não autorizado ao sistema MyGeotab. Para realizar isso:

- O MyGeotab usa autenticação HTTPS (TLS) (com um nome de usuário e senha exclusivos) para autenticar usuários no sistema,
- O MyGeotab não permite o uso de senhas comuns (derivadas de uma lista ativa de muitas das senhas mais comumente usadas),
- A própria senha que um usuário usa não pode ser recuperada, pois passa por um hash de 256 bits com um salt aleatório de 128 bits, e ela nunca é armazenada ou salva no disco,
- Todas as atividades de um usuário no MyGeotab são registradas e podem ser visualizadas por qualquer usuário aprovado no log de auditoria do MyGeotab,
- Os dados do log de auditoria não podem ser alterados ou removidos,
- O sistema MyGeotab permite o gerenciamento de direitos de forma altamente flexível, para permitir acesso limitado a várias áreas dentro do sistema, para usuários específicos,
- Os dados de clientes são completamente isolados dos dados de outros clientes, ou seja, informações (dados de GPS, informações do usuário, regras de exceção, et al .) armazenadas em uma base de dados de um cliente não estão acessíveis ou disponíveis para outras bases de dados, mesmo que as duas bases de dados estejam no mesmo servidor físico, e
- Somente funcionários autorizados da Geotab podem se conectar e fazer login em todas as bases de dados hospedadas para fins de diagnóstico de problemas; tudo isso é totalmente auditado e registrado no log de auditoria.

Controle de entrada

A Geotab implementa medidas adequadas para garantir que seja possível verificar e estabelecer se e por quem dados pessoais foram inseridos ou removidos no sistema MyGeotab. Isso é alcançado por meio de:

- Uma política de autorização para a entrada de dados na memória, bem como para a leitura, alteração e exclusão de dados armazenados,
- Autenticação do pessoal autorizado,
- Medidas de proteção para a entrada de dados na memória, bem como para a leitura, alteração e exclusão de dados armazenados,
- Utilização de códigos de usuário (senhas),
- Logoff automático de IDs de usuário que não tenham sido usados por um período substancial de tempo, e
- Comprovação estabelecida dentro da organização da Geotab quanto à autorização de entrada.

Separação do processamento para propósitos diferentes

A Geotab implementa medidas adequadas para garantir que os dados coletados para propósitos diferentes possam ser processados separadamente. Para realizar isso:

- O acesso aos dados é separado por meio de segurança de aplicativos para os usuários apropriados,
- Os módulos dentro do sistema MyGeotab separam quais dados são usados para qual propósito, por exemplo, por funcionalidade e função,
- No nível da base de dados, os dados são armazenados em diferentes tabelas normalizadas, separadas por módulo ou função que eles suportam, e
- Interfaces, processos em lote e relatórios são desenvolvidos somente para propósitos e funções

específicos; dessa forma, dados coletados para propósitos específicos são processados separadamente.

Disposições gerais

É importante manter qualquer identificação ou senhas de usuários seguras e não divulgá-las a nenhuma outra pessoa ou reutilizá-las em outros sites que possam estar comprometidos. A Geotab não é responsável por senhas perdidas ou roubadas. A Geotab recomenda padrões mínimos de senha em termos de tamanho e complexidade.

Se o Cliente acreditar que houve uma violação de segurança, deverá notificar imediatamente a equipe de Incidentes graves de segurança (24 horas por dia, 7 dias por semana) pelo incident@geotab.com. Os clientes não devem criar usuários em seu sistema para pessoas nas quais não confiam totalmente e devem revogar contas de usuário de pessoas que não precisam mais acessar o sistema.

Não há instalações nem um requisito para a Geotab se conectar diretamente à rede de usuários finais em nenhuma circunstância. Todos os dados do MyGeotab são totalmente contidos e gerenciados dentro da infraestrutura do MyGeotab. O usuário final pode, por meio do Kit de Desenvolvimento de Software (SDK) do MyGeotab, baixar dados em sua própria rede, se necessário. A conexão e toda a transferência de dados para fora da rede da Geotab são feitas por HTTPS.

Os dados do MyGeotab nunca são armazenados, copiados ou transferidos por meio de dispositivos de armazenamento removíveis, a menos que haja um requisito específico do usuário final, com a aprovação dele por escrito. Todos os dados sob o controle da Geotab são estritamente monitorados e adequadamente destruídos quando não são mais necessários.

Residência dos dados do cliente

Os dados do usuário relacionados à telemática e à telemática do cliente são armazenados nas seguintes mídias:

- O dispositivo GO no veículo (o cliente pode etiquetar o dispositivo GO),
- Computador do cliente (o Cliente pode etiquetar o seu computador),
- Servidor gerenciado pela Geotab (os dados do Cliente serão separados por meio lógico e virtual),
- Os dados dos clientes europeus são armazenados nos data centers europeus da Geotab, e
- Todos os outros dados do cliente são armazenados nos data centers da Geotab no Canadá, EUA ou Ásia e estão sujeitos à localização do cliente e aos parâmetros de otimização.

Os dados do usuário relacionados a telemática e telemática do cliente podem ser excluídos com segurança por solicitação do cliente.

Sempre que o cliente da Geotab enviar solicitações formais para a remoção dos seus dados por determinados motivos, a Geotab poderá excluir esses dados de forma segura e permanente.

Disponibilidade de dados e backups

A Geotab implementa medidas adequadas para garantir que os dados pessoais estejam protegidos contra destruição acidental ou perda. Para realizar isso:

- O backup de todos os dados hospedados na plataforma MyGeotab é realizado diariamente, 365 dias por ano,
- Todos os backups são confirmados, verificados e replicados em vários locais físicos separados para armazenamento (que podem ou não estar no mesmo data center),
- Todos os dados de backup são protegidos e o acesso é limitado a funcionários da Geotab específicos e

autorizados,

- Toda a infraestrutura de backup tem redundância adequada em caso de falhas de hardware, e
- Todos os dados de backup são armazenados totalmente criptografados com o uso de tecnologias de criptografia de nível empresarial.

Retenção, correção e exclusão de dados

Retenção de dados

A Geotab reterá pelo menos dois anos de dados antes da data de limpeza. Se quiser reter seus dados por mais de dois anos, recomendamos que recupere os dados desejados com uma das ferramentas API oferecidas pela Geotab.

Correção de dados e opções de exclusão

Os clientes podem excluir e corrigir dados armazenados nos sistemas da Geotab. Mediante solicitação, a Geotab pode ajudar com exportações, exclusões e correções de dados sob um contrato de consultoria separado de acordo com taxas honorárias vigentes. Analise nossa Política de nível de serviço MyGeotab para mais informações sobre backups.

Abordagem de limpeza de dados

A Geotab implementou um cronograma de limpeza padrão nas bases de dados que exclui dados com mais de 2 anos.

Agregação e aprimoramento dos dados

A Geotab compila, armazena e usa dados agregados e informações de uso do sistema para monitorar e melhorar os produtos existentes e para a criação de novos produtos, de acordo com a Política de Análise de Dados da Geotab (em inglês). Os dados agregados usados dessa maneira não estão mais associados a um dispositivo e, como tal, não são Dados de Veículo Individual.

A Geotab não tentará desagregar os dados ou reassociá-los a um dispositivo sem o seu consentimento, ou a menos que seja legalmente obrigada a fazê-lo, ou que seja necessário para fins de segurança ou solução de problemas. Os exemplos de trabalhos que a Geotab realiza nos dados são mostrados como segue:

- Procurar por notificações do dispositivo de que o produto não está funcionando como deveria,
- Procurar por uso excessivo de dados que indiquem uma falha no design ou má instalação,
- Agregar que tipo de informação de motor está disponível para cada Marca, Modelo e Ano,
- Observar o número de desconexões de dispositivos estratificadas por provedor de celular e código postal/região,
- Observar o número total de ocorrências de frenagem brusca em uma estrada (para encontrar cruzamentos perigosos),
- Calcular o consumo médio de combustível de cada Marca, Modelo e Ano,
- Observar a velocidade média de todos os veículos em uma estrada específica (fluxo do trânsito),
- Procurar por locais onde existam possíveis buracos na estrada, e
- Como parte da melhoria dos produtos e da experiência do usuário, somente para clientes na América do Norte, a Geotab pode consultar bases de dados mantidas pela R.L. Polk & Co. (IHS) para obter informações que os usuários disponibilizaram anteriormente a respeito de sua frota e operações. Tais consultas serão

baseadas em amostras representativas de informações de VIN (porém nenhuma outra informação do cliente) fornecidas à IHS de forma segura, confidencial e restrita.

Diagrama de arquitetura

Para ver um diagrama de arquitetura de alto nível, clique aqui.

Apêndice 2: Medidas de segurança do sistema Lat-Lon

Resumo executivo

A Lat-Lon, LLC, uma empresa de responsabilidade limitada do Colorado ("Lat-Lon"), é afiliada da Geotab. A Lat-Lon fabrica dispositivos de rastreamento e monitoramento de ativos movidos a energia solar, comumente conhecidos como "STUs". Os STUs são dispositivos independentes e com carregamento automático, com opções de sensores com e sem fio. Os clientes podem não apenas rastrear seus ativos, mas também monitorar diferentes aspectos de um ativo, como detecção de impacto, temperatura, porta ou escotilha aberta/fechada e pressão, para citar alguns. As ofertas de produtos Lat-Lon também incluem um dispositivo certificado para locais perigosos (Classe I, Div 2).

Os dados de localização e sensores transmitidos pelos STUs estão disponíveis no portal da web da Lat-Lon. No portal da web, os clientes podem configurar alertas de e-mail ou mensagens de texto em tempo real, alterar configurações de dispositivos, criar usuários adicionais, criar cercas geográficas e configurar relatórios automáticos programados.

Para obter mais informações, consulte o site da Lat-Lon.

Medidas de segurança do sistema de produtos Lat-Lon

Transmissão de dados

A Lat-Lon implementa medidas adequadas para evitar que quaisquer dados sejam lidos, copiados, alterados ou excluídos por partes não autorizadas durante a transmissão ou transporte de quaisquer dados da e para a Lat-Lon. Isso é alcançado por meio de:

- Transmissão de sensor para dispositivo: Os dados são criptografados com AES-128 em bandas de radiofrequência (RF) isentas de licença,
- Transmissão de dispositivo para servidor: Os dados armazenados no hardware são criptografados por processos próprios, enquanto o hardware está em modo descanso, bem como durante a transmissão para servidores de back-end,
- Transmissão de servidor para servidor: Os dados são criptografados em trânsito por protocolo TLS 1.2, e
- Transmissão de usuário para servidor: Os dados são criptografados em trânsito por protocolo HTTPS.

Controle de acesso ao sistema

A Lat-Lon implementa medidas adequadas para impedir o acesso não autorizado ao sistema Lat-Lon. Para realizar isso:

- O acesso ao portal da web é autenticado por senha forte.

- As senhas são criadas com salts e hashes usando a classe rfc2898DeriveBytes,
- Os usuários devem alterar sua senha a cada 12 meses,
- O acesso do cliente é gerenciado pelo aplicativo Lat-Lon. Existem duas funções: Administrador e Usuário.
- Os dados do cliente são separados com base em projetos GCP. Por exemplo, os ambientes de produção, teste e desenvolvimento são separados de maneira física e lógica,
- O uso do aplicativo é monitorado pelo sistema de monitoramento Lat-Lon,
- Cada tentativa de login e alteração de senha é registrada, e
- O monitoramento e os alertas do sistema usam nosso sistema operacional de pilha Prometheus e Grafana (TIG), enquanto as métricas de aplicativos personalizados são monitoradas dia e noite, todos os dias do ano.

Controle de entrada/validação de entrada

A Lat-Lon implementa medidas adequadas para verificar e estabelecer se e por quem os dados pessoais foram introduzidos ou removidos no sistema Lat-Lon. Para realizar isso:

- Todos os dados de entrada via interface da Web são higienizados por meio de funções C# padrão para limpeza de dados, e
- Valide o cliente de entrada e o lado do servidor.

Separação/segregação do processamento para propósitos diferentes

A Lat-Lon implementa medidas adequadas para garantir que os dados coletados para diferentes fins possam ser processados separadamente. Para realizar isso:

- Desenvolvimento, garantia de qualidade (QA) e produção são totalmente segregados e restritos por controle de acesso baseado em funções.

Disposições gerais

A Lat-Lon não tem controle sobre clientes que compartilham senhas com outras pessoas; portanto, é importante manter qualquer identificação ou senhas de usuários seguras e não divulgá-las a nenhuma outra pessoa ou reutilizá-las em outros sites que possam estar comprometidos.

A Lat-Lon exige que as senhas atendam aos requisitos mínimos de tamanho e complexidade. Os usuários devem alterar sua senha a cada 12 meses. Se o Cliente acreditar que houve uma violação de segurança, deverá notificar imediatamente a equipe de Incidentes graves de segurança (24 horas por dia, 7 dias por semana) pelo incident@geotab.com. Os clientes não devem criar usuários em seu sistema para pessoas nas quais não confiam totalmente e devem revogar contas de usuário de pessoas que não precisam mais acessar o sistema.

Não há instalações nem um requisito para a Lat-Lon se conectar diretamente à rede de usuários finais em nenhuma circunstância. O usuário final pode, por meio do Guia do Usuário do Gravador Binário da Lat-Lon e do Kit de Desenvolvimento de Software (SDK) do MyGeotab, baixar dados em sua própria Proprietário rede, se necessário. A conexão e toda a transferência de dados para fora da rede da Geotab são feitas por HTTPS.

Nenhum dado é armazenado, copiado ou transferido por meio de dispositivos de armazenamento removíveis, a menos que haja um requisito específico do usuário final, com a aprovação dele por escrito. Todos os dados sob o controle da Lat-Lon ou da Geotab são estritamente monitorados e adequadamente destruídos quando não são mais

necessários.

Residência dos dados do cliente

Mídia e local de armazenamento de dados do cliente

Os dados de STU do cliente Lat-Lon e os dados correlatos inseridos pelo usuário ficam armazenados na seguinte mídia:

- O STU do ativo;
- O computador do cliente (o cliente pode identificar seu próprio computador);
- O servidor Lat-Lon (os dados do cliente serão separados por meios lógicos e virtuais); e
- Todos os dados do cliente são armazenados em servidores Lat-Lon no leste dos EUA.

Abordagem de exclusão de dados do cliente

Os dados de STU e os dados correlatos inseridos pelo usuário podem ser apagados com segurança por solicitação do cliente.

Sempre que os clientes da Lat-Lon enviam solicitações formais para remover dados de seus clientes por determinados motivos, a Lat-Lon apaga os dados dos clientes de forma segura e permanente.

Disponibilidade de dados e backups

A Lat-Lon implementa medidas adequadas para garantir que dados pessoais sejam protegidos contra destruição ou perda acidental. Para realizar isso:

- Todos os dados hospedados na plataforma Lat-Lon têm backup diário, 365 dias por ano,
- Todos os backups são confirmados, verificados e movidos para um local físico separado para armazenamento (que pode ou não estar dentro do mesmo data center),
- Todos os dados de backup são protegidos e o acesso é limitado a funcionários específicos e autorizados,
- Toda a infraestrutura de backup tem redundância adequada em caso de falhas de hardware, e
- Todos os dados de backup são armazenados totalmente criptografados com o uso de tecnologias de criptografia de nível empresarial.

Retenção, correção e exclusão de dados

Retenção de dados

Se a Lat-Lon fizer uma limpeza, reterá no mínimo 365 dias de dados antes da data de limpeza e fará todos os esforços para dar um aviso prévio aos proprietários da base de dados Lat-Lon. Se houver uma limpeza de dados e um cliente desejar reter dados por mais de um (1) ano, será sugerido ao cliente que recupere os dados desejados com uma das ferramentas API oferecidas pela Lat-Lon.

Correção de dados e opções de exclusão

Os clientes podem excluir e corrigir manualmente os dados armazenados nos sistemas da Lat-Lon pelo portal da web da Lat-Lon. Mediante solicitação, a Lat-Lon pode ajudar a exportar, excluir e corrigir dados, conforme acordo de

consultoria em separado, sujeito às taxas horárias vigentes.

Abordagem de limpeza de dados

A Lat-Lon fará todos os esforços para iniciar uma limpeza somente quando for necessário para preservar a integridade, confiabilidade e disponibilidade do portal da web da Lat-Lon. Todos os drives desativados são limpos usando ferramentas de destruição de dados padrão de mercado ou, no caso de um drive com defeito, são destruídos para garantir que nenhum dado possa ser recuperado.

Diagrama de arquitetura

Para ver um diagrama de arquitetura de alto nível, clique aqui.