REVISTA BRASILEIRA DE MECATRÔNICA
FACULDADE SENAI DE TECNOLOGIA MECATRÔNICA

SEGURANÇA CIBERNÉTICA: BOAS PRÁTICAS PARA DESENVOLVIMENTO E OPERAÇÕES DE APLICAÇÕES IOT

CYBERSECURITY: BEST PRACTICES FOR IOT APPLICATION DEVELOPMENT AND OPERATIONS

Fabio Castro Lopes[1], [i]
Daniel Barbuto Rossato[2], [ii]
Caio Vinícius Ribeiro da Silva[3], [iii]

Data de submissão: (24/10/2022) Data de aprovação: (27/07/2023)

RESUMO

Os sistemas IoT são o cerne da quarta revolução industrial, habilitando a integração de todas as coisas ao mundo digital. Porém, os ataques cibernéticos têm sido cada vez mais frequentes mostrando as vulnerabilidades destas soluções, as quais têm sido produzidas em geral, sem a devida consideração de medidas de segurança em todo o ciclo de vida do projeto, trazendo implicações materiais e intangíveis. Neste artigo são abordadas boas práticas para o desenvolvimento e operação seguros de sistemas IoT. O conceito de DevSecOps é apresentado com aplicação aos sistemas IoT, destacando a importância da arquitetura do sistema com base em plataformas de gerenciamento e monitoramento confiáveis e que ofereçam recursos para a implementação das boas práticas de prevenção e mitigação de riscos.

Palavras-chave: segurança cibernética; internet das coisas; DevSecOps; SIEM; plataforma IoT.

ABSTRACT

IoT systems are at the heart of the fourth industrial revolution, enabling the integration of all things into the digital world. However, cyber-attacks have been increasingly frequently showing the vulnerabilities of these solutions, which have been produced in general, without due consideration of security measures throughout the project life cycle, bringing material and intangible implications. This article covers best practices for the safe development and operation of IoT systems. The concept of DevSecOps is presented with application to IoT systems, highlighting the importance of reliable system architecture based on management and monitoring platforms that offer resources for the implementation of best risk prevention and mitigation practices.

Keywords: cybersecurity; internet of things; DevSecOps; SIEM; IoT platform.

[1] Especialista em Internet das Coisas pela Faculdade SENAI São Paulo. E-mail: fabioclopes07@gmail.com
[2] Professor da Faculdade SENAI São Paulo. E-mail: daniel.rossato@sp.senai.br
[3] Professor da Faculdade SENAI São Paulo. E-mail: caio.silva@sp.senai.br

1 INTRODUÇÃO

A Internet das Coisas (IoT) se refere ao processo de conectar objetos físicos do dia a dia à Internet, podendo ser um sensor, que coleta informações sobre o objeto e as transmite, ou um atuador, que recebe comandos para tomar uma ação no objeto; ou ambos. Sistemas IoT estão sendo adotados em diferentes verticais por toda a sociedade: carros autônomos, casas conectadas, indústrias agrícolas e financeiras, cidades inteligentes, hospitais e centros de saúde (RED HAT, 2019).

A revolução da Internet das Coisas (IoT) marcou o início de uma nova era de transferência de dados. A cada dia, novos dispositivos são adicionados a todos os tipos de infraestruturas de rede, transferindo quantidades gigantescas de dados para frente e para trás. Segundo a *International Data Corporation* (IDC), espera-se que o número de dispositivos IoT cresça para 80 bilhões de dispositivos conectados em 2025, praticamente superando em dez vezes a população humana (VELOCITY BUSINESS SOLUTIONS, 2018).

Ainda de acordo com a IDC (CONVERGENCIA DIGITAL, 2022), os gastos mundiais com tecnologia em IoT atingirão mais de um trilhão de dólares nos próximos anos. Outras estimativas apontam impactos de quatro a onze trilhões de dólares em setores da economia como: indústria, cidades, saúde, varejo, transporte, casas e escritórios (SCHWAB, 2018). Isso significa que os desenvolvedores terão muito o que programar. Muitos de nós atualmente já estamos cercados por dispositivos IoT, como por exemplo: o *smartspeaker* Alexa, que reporta informações e monitora o ambiente; o *smartwatch* que monitora eventos do corpo, como sono, frequência cardíaca, momentos de exercício e de sedentarismo, entre outras informações e envia os dados para uma aplicação alocada em uma nuvem pública. Temos também câmeras IP, babás eletrônicas, medidores de energia, carros, entre outros. Com a presença cada vez maior destes dispositivos torna-se necessário compreender os cenários em que estão se desenvolvendo e operando essas aplicações.

Já é um fato conhecido que os dispositivos IoT representam um ponto de acesso vulnerável e atraente para ser explorado por hackers e outros atores mal-intencionados, dado a existência de 17 bilhões de dispositivos IoT atualmente no mundo (STATISTA, 2022), a sua localização distribuída (ao invés de concentrada em data centers), e o uso de bibliotecas de softwares *open source* com diversas vulnerabilidades. Muitas destas vulnerabilidades estão identificadas com seu código CVE (*Common Vulnerabilites and Exposures*), cujo catálogo pode ser encontrado no site *cve.org* criado a partir do trabalho de Mann e Cristey (1999).

Portanto, medidas de segurança cibernética para redução de riscos são fundamentais, e dentre elas a iniciativa de DevSecOps (MACBRIDE, 2023). No primeiro semestre de 2021, foram mais de 1,5 bilhões de ataques ante os 639 milhões de ataques, nos seis meses de 2020, ou seja, um crescimento de mais de 100%. A maioria dos ataques (58%) usou o protocolo Telnet e explorou diversas vulnerabilidades para provocar ataques DDoS, minerar criptomoedas ou roubar dados confidenciais. Desde o início da pandemia o número de ciberataques cresceu mais 600%, com danos estimados de aproximadamente 6 trilhões de dólares em 2021 (PAUL, 2021).

A falta de padrões de fabricação adequados, os investimentos sendo cortados para manter os preços baixos às custas da segurança e as dificuldades em criptografar adequadamente os dispositivos IoT contribuem para tornar esses pontos de acesso um ponto fraco conhecido em todas as estratégias de ataque cibernético.

A aplicação de tecnologias e boas práticas de segurança geram custos no projeto, porém podem trazer estabilidade nas operações e retorno de investimento aplicado. Pois, além dos custos infligidos materialmente pelas ameaças de segurança, a imagem e reputação da empresa são ativos intangíveis e valiosos que podem ser afetados.

Apesar de ser um tema relevante, há poucas referências a respeito de boas práticas de segurança em sistemas IoT. Podemos citar um estudo de caso em que Momenzadeh et. al (2020) evidenciam a importância destas práticas, e também o trabalho de Barrera, Bellmann e Van Oorschot (2023) em que buscam catalogar e sistematizar diversas práticas que aparecem de forma isolada na literatura, como por exemplo apresentadas por Payne e Abegaz (2017). Russel e Van Duren (2016) mostram diversas tecnologias de segurança aplicáveis a sistemas IoT, mostrando possíveis soluções a serem adotadas com as boas práticas. Existem ainda propostas de plataformas para desenvolvimento seguro de sistemas IoT como em Samaila et. al (2020) em que é apresentada uma estrutura de segurança denominada IoT-HarPSecA que oferece três recursos de funcionalidade: elicitação de requisitos de segurança, diretrizes de práticas recomendadas de segurança para desenvolvimento seguro e um recurso que recomenda Algoritmos Criptográficos *LightWeight* (LWCAs) específicos para implementações de software e hardware.

Portanto, o objetivo deste artigo é apresentar boas práticas para o desenvolvimento, gerenciamento e monitoração de sistemas IoT, seja em ambientes *on-premises* ou em nuvem, independente do segmento de aplicação.

Neste sentido, é apresentado o conceito de DevSecOps, que permite incluir a segurança diretamente nos fluxos de desenvolvimento e implantação CI/CD (*continuous integration and continuous delivery/deployment*), minimizando as vulnerabilidades.

Diversas plataformas de gerenciamento para sistemas IoT permitem a implantação de segurança. Em especial, a plataforma Cisco IoT FND é comentada com suas particularidades incluindo análises, operações, administração e funcionalidades. Esta plataforma se destaca por possuir diversas medidas de segurança que permitem a implantação de boas práticas.

A arquitetura de uma solução IoT aplicando estas práticas de segurança é apresentada com base na experiência do autor na implementação para uma empresa de grande porte.

Por fim, é abordada a questão do monitoramento contínuo, um grande aliado de toda a infraestrutura de IoT, trazendo métricas, indicadores, manutenção preventiva e até mesmo agregando valor ao produto.

2 METODOLOGIA DEVSECOPS

DevSecOps é um conjunto de princípios e práticas que fornecem entrega mais rápida de recursos de software seguros, melhorando a colaboração e a comunicação entre equipes de desenvolvimento de software, operações de TI e equipe de segurança dentro de uma organização, bem como com adquirentes, fornecedores e outras partes interessadas no ciclo de vida de um sistema de software (YASAR, 2021).

O conceito de DevSecOps foi criado a partir do DevOps. DevOps é uma combinação de desenvolvimento e operações de uma aplicação de forma automatizada. Neste conceito tem-se a participação conjunta de engenheiros de desenvolvimento e operações em todo o ciclo de vida da aplicação, desde o design e o desenvolvimento até à produção e manutenção. Para isso, é desenhado um fluxo de desenvolvimento e implantação CI/CD (*continuous integration and continuous delivery/deployment*), que é automatizado por meio de ferramentas como Jenkins, Buddy, GitLab, Azure Devops, AWS CodePipeline, entre outros.

O DevSecOps é a inclusão de conceitos de segurança dentro do fluxo de DevOps, com o intuito de proteger o software, infraestrutura, aplicativos e dados, oferecendo suporte ao desenvolvimento de um código estável e seguro, conforme mostra a figura 1.

Figura 1 – Diagrama DevSecOps

Fonte: ZETTLER, 2021.

Segue uma breve descrição das etapas da metodologia DevSecOps mostradas na figura 1, as quais devem ser consideradas para haver o desenvolvimento e operação da solução IoT de forma integrada com a segurança, conforme Zettler (2021).

2.1 *Plan* (planejar)

A fase de planejamento é a fase menos automatizada do DevSecOps e envolve colaboração, discussão, revisão e estratégia de análise de segurança. As equipes devem realizar uma análise de segurança e criar um plano que descreva onde, como e quando os testes de segurança serão realizados. Podem ser usadas ferramentas como: IriusRisk, Tenable Nessus.

2.2 *Code* (código)

As ferramentas DevSecOps para a fase de codificação ajudam os desenvolvedores a escrever códigos mais seguros. Práticas de segurança importantes para a fase de codificação incluem análise de código estático, revisões de código e ganchos de pré-confirmação. Algums ferramentas úteis são: Git, Azure DevOpsServer, AWS CodeCommit, Mercurial, CVS.

2.3 *Build* (compilação)

A fase de compilação começa quando os desenvolvedores confirmam o código no repositório de origem. As ferramentas de compilação de DevSecOps se concentram na análise automatizada de segurança em relação ao artefato de saída do *build*. Práticas de segurança

importantes incluem análise de componentes de software, teste de software de aplicativo estático (SAST) e testes de unidade. As ferramentas podem ser conectadas a um pipeline de CI/CD existente para automatizar esses testes.

O SAST (*Static Application Security Testing*) é uma ferramenta de segurança de aplicativos (AppSec) que verifica os códigos-fonte (binário ou na linguagem) e por isso é considerado uma ferramenta de teste de caixa branca, analisando um aplicativo "de dentro para fora", identificando a causa principal das vulnerabilidades e ajudando a corrigir as falhas de segurança subjacentes. Assim, não espera o sistema entrar em execução para fazer a verificação.

O SAST reduz os riscos de segurança em aplicativos, fornecendo feedback imediato aos desenvolvedores sobre problemas introduzidos no código durante o desenvolvimento. Ele ajuda a aculturar os desenvolvedores sobre segurança enquanto trabalham, fornecendo-lhes acesso em tempo real às recomendações e navegação de linha de código, o que permite descobrir vulnerabilidades mais rapidamente e viabiliza a auditoria colaborativa. Isso permite que os desenvolvedores criem mais códigos que sejam menos vulneráveis a comprometimentos, proporcionando um aplicativo mais seguro.

2.4 *Test* (teste)

A fase de teste é acionada depois que um artefato de compilação é criado e implementado com sucesso em ambientes de *staging* ou teste. A execução de um conjunto de testes abrangente leva um tempo considerável. Essa fase deve falhar rapidamente para que as tarefas de teste mais caras sejam deixadas para o fim.

A fase de teste usa ferramentas de teste dinâmico de segurança de aplicativos (DAST) para detectar fluxos de aplicativos em tempo real, como autenticação de usuário, autorização, SQL *injection* e *endpoints* relacionados à API. O DAST focado em segurança analisa um aplicativo em relação a uma lista de problemas de alta gravidade conhecidos.

O DAST (*Dynamic Application Security Testing*) é o processo de análise de um aplicativo da web que usa o *front end* para encontrar vulnerabilidades por meio de ataques simulados. Esse tipo de abordagem avalia o aplicativo "de fora para dentro", atacando-o como um usuário mal-intencionado faria. Depois que um scanner DAST realiza esses ataques, ele procura resultados que não fazem parte do conjunto esperado e identifica as vulnerabilidades de segurança.

São vantagens do DAST: ser independente de aplicativo; a identificação, de imediato, de vulnerabilidades que podem ser exploradas; não requer acesso ao código-fonte. São desvantagens do DAST: não ser possível encontrar a localização exata de uma vulnerabilidade no código; exigir conhecimento de segurança para interpretar os relatórios; provável morosidade nos testes.

2.5 *Release* (liberação)

Na fase de lançamento do ciclo DevSecOps, o código do aplicativo e o executável já devem ter sido testados a fundo. O foco desta fase é proteger a infraestrutura do ambiente de execução examinando valores de configuração do ambiente, como controle de acesso do usuário, acesso a firewall de rede e gerenciamento de dados secretos.

2.6 *Deploy* (implementação)

Se as fases anteriores forem aprovadas, é hora de implementar o artefato de *build* na produção. As áreas de segurança abordadas na fase de implementação são aquelas que só acontecem com o sistema de produção ao vivo. Por exemplo, as diferenças na configuração entre o ambiente de produção e os ambientes de *staging* e desenvolvimento anteriores devem ser analisadas a fundo. Os certificados TLS e DRM de produção devem ser validados e revisados para renovação futura.

2.7 *Monitor/Respond* (segurança contínua)

Depois que um aplicativo é implementado e estabilizado em um ambiente de produção ao vivo, outras medidas de segurança são necessárias. As empresas precisam monitorar e observar o aplicativo ao vivo em busca de ataques ou vazamentos com verificações de segurança automatizadas e ciclos de monitoramento de segurança.

3 PLATAFORMA DE GERENCIAMENTO CISCO IOT FND

Para realizar o gerenciamento das soluções IoT muitas plataformas tem sido desenvolvidas fornecendo ferramentas de conectividade, como Broker MQTT, protocolos OPC-UA, REST-HTTP, suporte a redes WiFi, LoraWAN, SigFox, NB-IoT e Z-Wave, gerenciamento e configuração de rede banco de dados relacional e não-relacional para armazenamento de dados, processamento e análise dos dados, gerenciamento e atualização dos dispositivos IoT, monitoramento e visualização de dados e eventos, visão da infraestrutura, *endpoints* e dispositivos conectados, entre outros.

Os sistemas IoT estão em constante evolução, de forma que cada vez mais funcionalidades são agregadas e atualizações são realizadas ao longo do tempo. Isso significa dizer que projetos de Internet das Coisas devem ser expandidos ou sofrerem grandes mudanças sem nenhuma intervenção nos dispositivos em campo, flexibilizando negócios e operações com o menor impacto possível. Esta é a principal razão da utilização de plataformas IoT em projetos de grande porte de Internet das Coisas.

Estas plataformas, portanto, trazem maior segurança, robustez e competitividade na administração do negócio por meio de controle, automação, atualização, relatórios, e melhoria contínua, gerando valor agregado ao produto. Em geral, as plataformas podem atender diversos segmentos de aplicação de sistemas IoT: indústria, agronegócio, cidades, veículos, entre outros.

Podemos destacar as principais plataformas do mercado atualmente:

a) Thingspeak (*thingspeak.com*), da Mathworks, que possibilita integração com os recursos do Matlab;
b) Konker (*konkerlabs.com*);
c) Tago (*tago.io*);
d) Dojot (*dojot.com.br*), criada pelo CPqD em parceria com outras instituições brasileiras;
e) AWS IoT, conjunto de funcionalidades na nuvem AWS para sistemas IoT;
f) Azure IoT, conjunto de funcionalidades na nuvem Azure para sistemas IoT.

Entretanto, quando se trata do gerenciamento da rede principalmente em sistemas de automação de energia, destaca-se a plataforma da Cisco IoT *Field Network Director* (FND), que

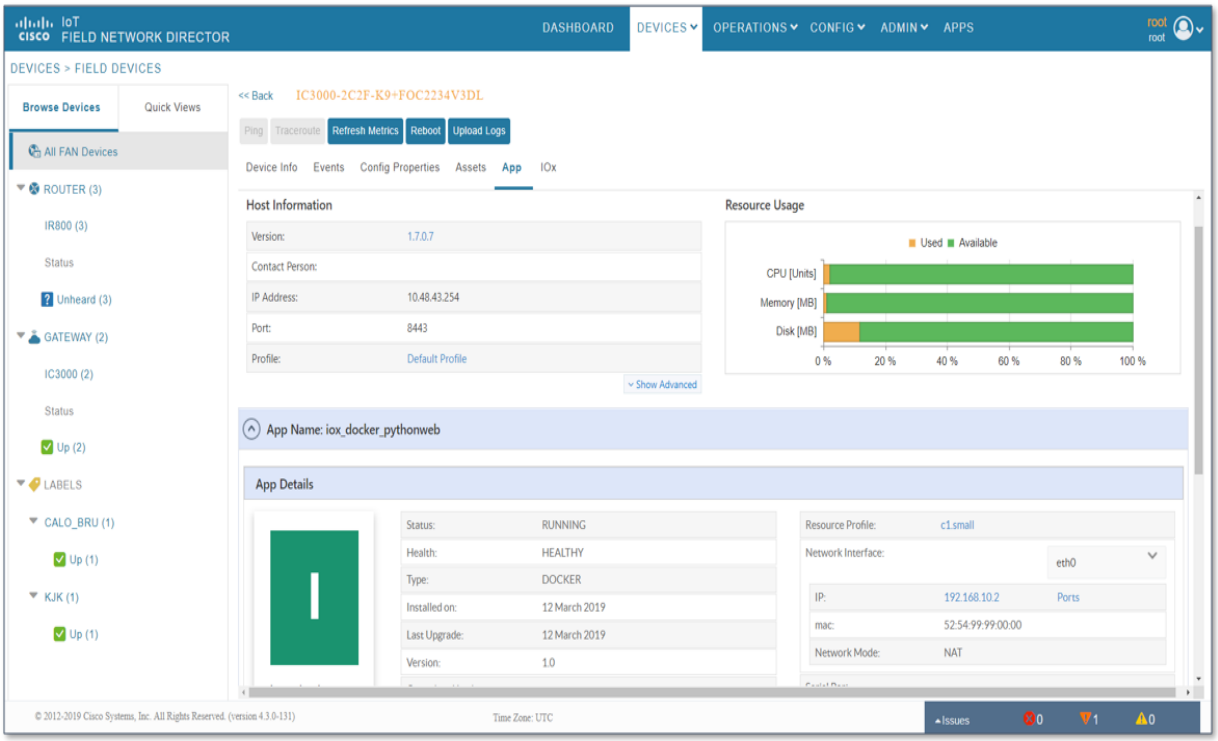
atualmente encontra-se na versão 4.9 e anteriormente era chamada de *Connected Grid Network Management System* (CG-NMS).

O Cisco IoT FND é responsável pelo gerenciamento e monitoração de toda infraestrutura de rede em uma solução IoT de grande escala. É uma plataforma de software que auxilia na separação entre a gestão da rede de comunicação e as aplicações operacionais tais como: infraestrutura de medição avançada (AMI), automação de distribuição (DA) e gerenciamento da distribuição de energia (DMS), automação da restauração de energia interrompida (OMS), gerenciamento de dados do medidor (MDM) (CISCO, 2022). Temos como exemplo de aplicação no Brasil, o Smart Light implementado pela concessionária BHIP em parceria com a empresa Itron que possui capacidade de controlar semáforos, iluminação pública, chancela de pedágios, entre outros elementos (ITRON, 2022).

Nestas aplicações, o Cisco IoT FND é o responsável pela administração de toda infraestrutura lógica e física, gerenciando os equipamentos: *switchs*, roteadores, servidores, *firewalls* e os dispositivos IoT, que pode ser um sensor de radar, ponte, pedágios até mesmo um celular, desde que cumpra os pré-requisitos para fazer parte da solução.

As ferramentas de gerenciamento de configuração são um ingrediente fundamental para a segurança, pois dão visibilidade da configuração estática de uma infraestrutura dinâmica. Assim, a configuração do sistema pode ser auditada e revisada. Na figura 2 podemos observar a tela de interface com o usuário para configuração e monitoramento dos dispositivos de campo IoT.

Figura 2 - GUI Overview



Fonte: Elaborado pelo autor, 2023.

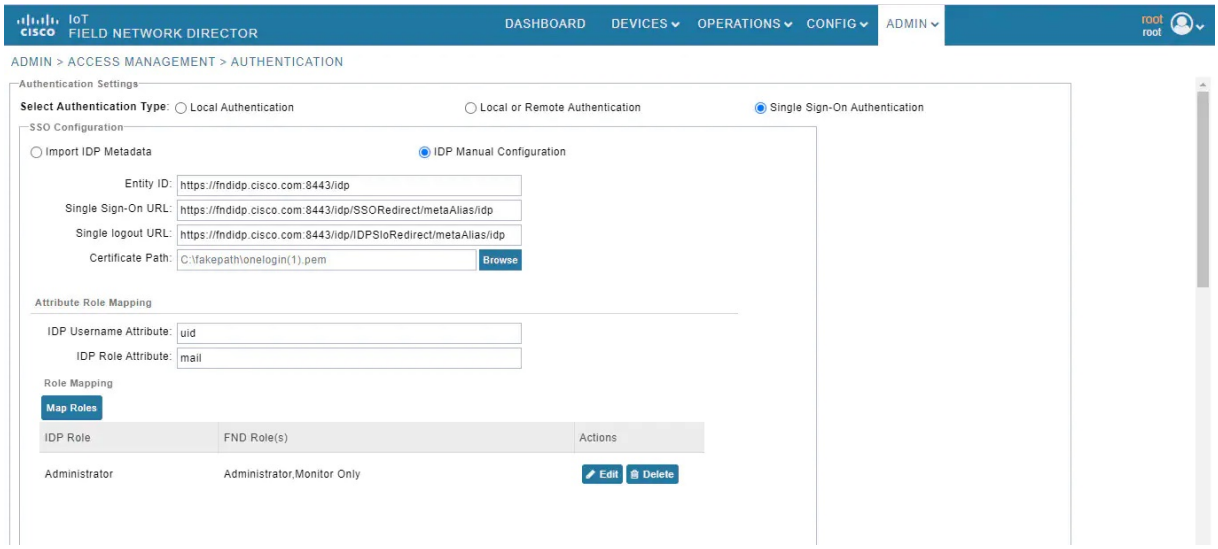
Os recursos proporcionados por esta plataforma incluem a segurança da rede com: gerenciamento de identidade e controle de acesso; defesa de thread (defesa em camadas que se integre a *firewall*, VPN, prevenção de intrusões e serviços de segurança de conteúdo para detectar, prevenir e mitigar ameaças); segurança do data center (proteção da integridade de

aplicativos e dados, proteção das comunicações entre processos de negócios e aplicativos e proteção da conectividade com recursos externos); conformidade de utilitários (para satisfazer requisitos regulatórios e de conformidade, como NERC-CIP, com serviços de avaliação, design e implantação); monitoramento e gerenciamento de segurança (monitoramento contínuo de eventos cibernéticos) (CISCO, 2022).

O sistema possui opções de *audit trail*, um nome mais popular seria logs de acessos dos usuários que utilizam a plataforma, data, hora, usuário, IP, qual tipo de operação e outros detalhes.

A plataforma Cisco IoT FND possui diversas opções para gerenciar os usuários e os tipos de acessos aos ambientes, desde integração com AD (*active directory*), acesso com SSO SAML, LDAP, podendo adicionar, habilitar, editar, resetar senhas, visualizar, permissões, deletar e desabilitar, todas essas operações fazem parte da plataforma. A figura 3 mostra a tela de configuração de acesso.

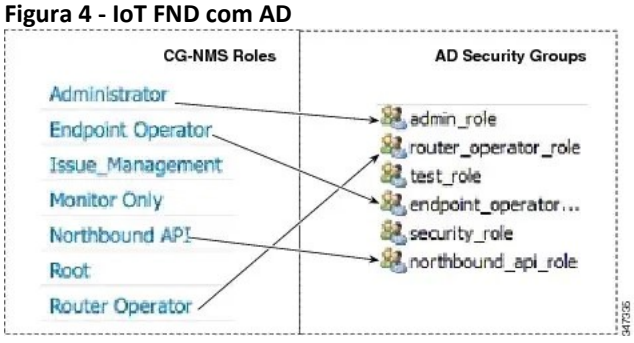
Figura 3 - SSO IoT FND



Fonte: Elaborado pelo autor, 2023.

Com intuito de melhor administração para os usuários, podem ser criados grupos conforme sua função, segue na figura 4, um exemplo para o AD.

Figura 4 - IoT FND com AD



Fonte: CISCO, 2022.

Para que os dispositivos possam ser totalmente gerenciados pelo FND, a plataforma possui uma integração com os servidores Windows Server PKI RSA, esses certificados são

essenciais para garantir a segurança no tráfego de informações e acesso aos equipamentos conectados ao FND.

Uma das particularidades do IoT FND é a capacidade de receber eventos de todo o ambiente, ele armazena os eventos no seu banco de dados e envia mensagens para um servidor Syslog na qual podemos fazer interação com ferramentas de terceiros como Graylog, ELK, Splunk entre outros que são sólidos no mercado.

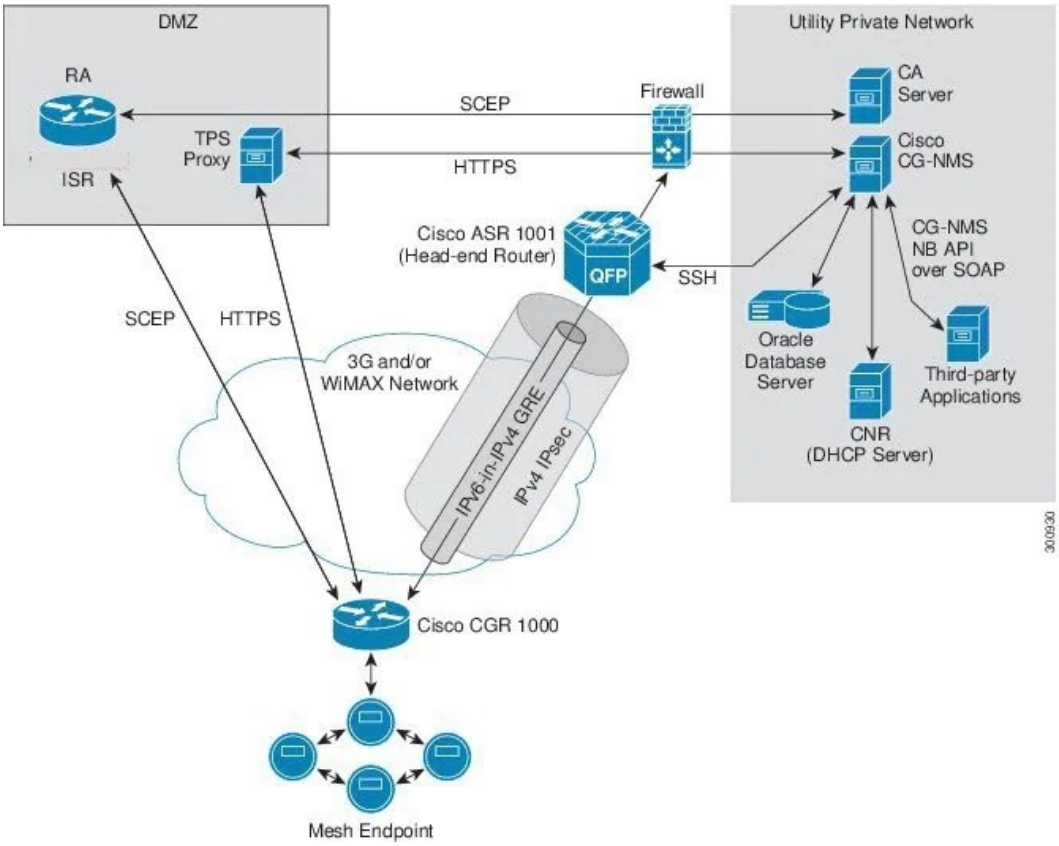
O IoT FND ainda possui outros recursos como retenção de dados, gerenciamento de registros (logs), provisionamento de dispositivos com IPv6, configurações do servidor Web, temporização de atualização para protocolo UDP entre outras particularidades.

A figura 5 mostra a arquitetura de rede para soluções que utilizam o Cisco IoT FND. Nesta arquitetura, temos a rede *mesh* dos *endpoints* (dispositivos IoT), a rede DMZ (rede pública da empresa) e a rede privada da empresa. A conexão entre estas redes pode ser feita por tecnologias de rede pública celular 3G/4G/5G ou rede privada WiMAX ou ainda fibra óptica Ethernet para garantir o acesso a grandes distâncias.

Os principais componentes da solução IoT FND são (CISCO, 2022):

a) *IoT FND Application Server* (servidor de aplicações IoT FND): local principal da implementação do IoT FND. Roda em um servidor Linux Red Hat (RHEL) e permite que administradores controlem diferentes aspectos da implementação do IoT FND usando interface de usuário gráfica em navegador Web. Para obter alta disponibilidade, são utilizados dois ou mais servidores IoT FND conectados a um *load balancer*.
b) *NMS Database* (base de dados do sistema de gerenciamento da rede): este banco de dados Oracle armazena todas as informações gerenciadas pela solução IoT FND, incluindo todas as métricas recebidas dos dispositivos IoT (ME - *mesh endpoints*) e todas as propriedades dos equipamentos como imagens de *firmware, templates* de configuração, logs, eventos, e assim por diante.
c) *Software Security Module* (SSM): solução de baixo custo como alternativa ao *Hardware Security Module* (HSM); é usado para assinar as mensagens CSMP enviadas aos medidores e dispositivos IR500 (roteador industrial da Cisco para conexão de dispositivos IoT via serial ou Ethernet/IP para rede WPAN *mesh* em RF 915 MHz).
d) TPS *Proxy*: permite que os roteadores se comuniquem com o IoT FND quando forem inicializados pela primeira vez em campo. Depois que o IoT FND provisiona os túneis entre os roteadores e o HER (ASRs), os roteadores se comunicam diretamente com o IoT FND.

Figura 5 – Arquitetura típica Cisco IoT FND



Fonte: CISCO, 2022.

Nesta arquitetura, um *firewall* é utilizado para separar a rede pública da companhia (DMZ) e sua rede privada. Dentro da rede privada temos o servidor Cisco IoT FND (Cisco CG-NMS), o servidor do banco de dados Oracle, o servidor DHCP, o Cisco IoT FND *North Bound* API e o servidor Autoridade Certificadora (CA). O servidor *proxy* de provisionamento de túnel (TPS *proxy*) e o servidor Autoridade de Registro (RA) devem estar localizadas na rede DMZ.

Quando o roteador Cisco CGR da série 1000 se torna ativo na rede, ele registra seu certificado com o RA empregando o protocolo *Simple Certificate Enrollment Protocol* (SCEP). O RA (ou ISR na arquitetura de implementação *Zero Touch*) funciona como um *proxy* da CA, obtendo o certificado para o rotador CGR. O Cisco CGR então envia uma requisição de provisionamento de túnel por HTTPS para o *proxy* TPS que por sua vez, direciona a solicitação para o IoT FND. O Cisco IoT FND coleta todas as informações necessárias para configurar um túnel entre o Cisco CGR e o roteador *Head-end* ASR 1001.

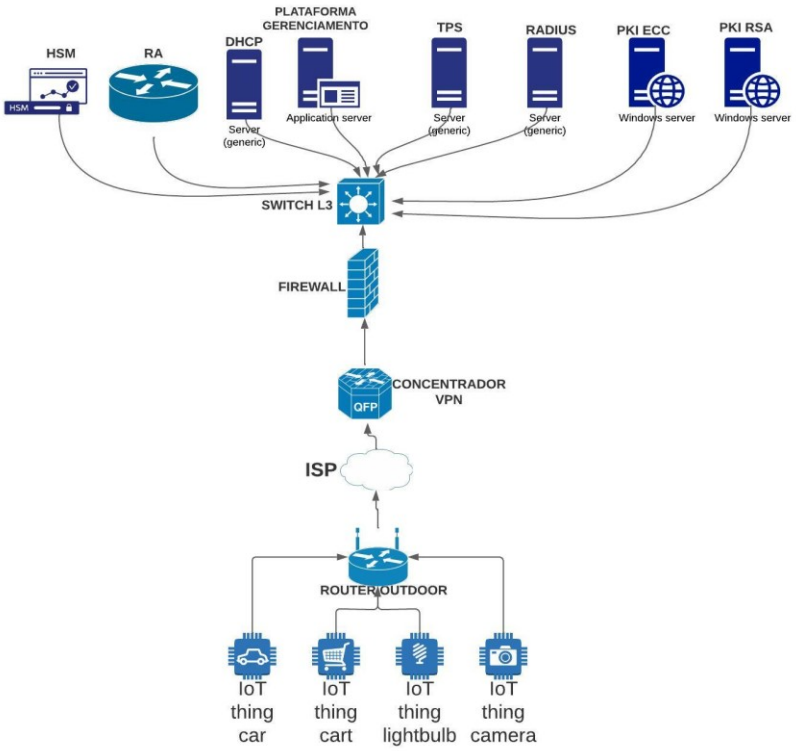
4 EXEMPLO DE UMA PLATAFORMA DE GERENCIAMENTO

Nesta seção, será descrita a arquitetura de um sistema IoT com boas práticas de segurança, implementado em uma empresa de grande porte. A solução pode ser implantada em *cloud* ou até mesmo *on-premises*, como todo projeto vai depender do investimento e o objetivo a ser alcançado.

Nesta solução robusta, foram utilizados: SO Linux e Windows, *firewall*, roteadores (concentrador de VPN), HSM (criptografia de dados), roteadores para IoT (outdoor),

dispositivos *endpoints* IoT. O modelo de infraestrutura física implementada pode ser visualizado na figura 6 e será descrito a seguir.

Figura 6 – Arquitetura de uma aplicação IoT



Fonte: Elaborado pelo autor, 2023.

Hardware Security Module (HSM) é um dispositivo físico que fornece segurança extra para dados confidenciais. Esse tipo de dispositivo é usado para fornecer chaves criptográficas para funções críticas, como criptografia, descriptografia e autenticação para uso de aplicativos, identidades e bancos de dados.

Registration Authority (RA) é uma autoridade em uma rede que verifica as solicitações do usuário para um certificado digital e informa à autoridade de certificação (CA) para emiti-lo.

Dynamic Host Configuration Protocol (DHCP) possibilita a alocação dinâmica de endereços mudando a configuração do dispositivo para *pools* de endereços globais no nível do servidor. O DHCP é baseado em um modelo cliente/servidor. O software cliente é executado no dispositivo e o software do servidor é executado no servidor DHCP.

A plataforma de gerenciamento é normalmente responsável por fazer toda administração dos dispositivos IoT conectados, promovendo monitoração, atualização em massa, gerando relatórios e análise do ambiente.

Tunnel Provisioning Server (TPS) é um *proxy* entre a plataforma de gerenciamento e os roteadores, permite que os roteadores se comuniquem com a Plataforma de Gerenciamento quando forem inicializados pela primeira vez em campo. Depois que a Plataforma de Gerenciamento provisiona os túneis entre os roteadores e os Concentradores de VPN, os roteadores se comunicam diretamente com o Plataforma de Gerenciamento.

Remote Authentication Dial-In User Service (RADIUS) é um protocolo de rede que protege uma rede habilitando a autenticação centralizada e a autorização de usuários de discagem. Muitos aplicativos ainda dependem do protocolo RADIUS para autenticar usuários (RICKETTS et al., 2022).

PKI ECC – Autoridade Certificadora (CA), responsável pela emissão de certificados que serão implantados nos dispositivos IoT, o padrão internacional é o X.509 baseados em PKI (*Public Key Infraestructure*).

PKI RSA - Autoridade Certificadora (CA), responsável pela emissão de certificados que serão utilizados para acessos remotos nos roteadores, gerando a chaves ".pem" que podem variar entre 80 até 256 bits baseado em PKI (*Public Key Infraestructure*).

Switch L3 é um comutador de rede que atua na camada 2 e 3 do modelo OSI, ou seja, possui as funcionalidades de *switch* e roteador combinados no mesmo chassi, o que permite que dispositivos conectados na mesma sub rede ou VLAN troquem informações com maior velocidade. Nesta infraestrutura *on-premises* é importante manter para melhor administração da rede.

Firewall é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança. Nesta infra ele é o responsável pela proteção e liberação das portas de comunicação de todo ambiente, garantindo que uma comunicação segura.

Concentrador de VPN é um dispositivo de rede que cria e ajuda a gerenciar várias conexões VPN remotamente. Ele estabelece vários túneis VPN criptografados ao mesmo tempo e fornece uma conexão segura e criptografada entre diferentes nós VPN.

Internet Service Provider (ISP) é qualquer entidade que oferece serviços de acesso, participação ou utilização da internet.

Router Outdoor (roteador de campo): são roteadores modulares e robustos nas quais as concessionárias e outros clientes industriais podem construir uma infraestrutura de comunicação altamente segura, confiável e escalável. Os produtos são certificados para atender a padrões ambientais rigorosos. Eles suportam uma variedade de interfaces de comunicação, como Ethernet, Serial, Celular e malha de radiofrequência (RF) 902-928 Mhz.

Dispositivos IoT: são dispositivos que conectam objetos físicos do dia a dia à Internet, incluindo objetos domésticos comuns, como lâmpadas, dispositivos médicos e acessórios, dispositivos *smart* e até mesmo cidades inteligentes.

Após a infraestrutura implantada e configurada com os pré-requisitos de segurança, incluindo os certificados, o processo de validação da segurança no fluxo de comunicação será explicado passo-a-passo a seguir. A plataforma de gerenciamento é importante no provisionamento dos roteadores outdoors e no gerenciamento dos dispositivos. Configurações específicas não serão apresentadas, pois cada fabricante possui seus segredos e particularidades.

Passo 1 – a configuração do roteador precisa estar com detalhes de túnel VPN e certificado RSA validado. No momento que o roteador é ligado, ele faz um *broadcasting* através da sua rota *default*, na qual a operadora (cabeada, 4G, 5G) encaminha o pacote para o concentrador de VPN pedindo autorização.

Passo 2 – o concentrador de VPN possui as configurações padrões e possui a lista de equipamentos que podem fazer parte daquela rede. O *firewall* está configurado para fazer

todo o bloqueio e liberação das portas de comunicação dentro de toda infra, ele é o responsável pela separação da rede pública da operadora e sua rede privada.

Passo 3 - o túnel VPN IPsec será estabilizado no momento que o certificado do roteador for autorizado pela PKI RSA (autoridade certificadora) através do *Registration Authority* (RA) permitindo que ele possa trafegar dados pelo túnel VPN.

Passo 4 – após o túnel VPN estabilizado para que a plataforma de gerenciamento possa identificar o roteador, um outro passo de segurança é validado. O protocolo HTTPS precisa ser ativado e validado pelo dispositivo TPS, que faz o papel de *proxy* para tráfego de protocolos HTPPS. Isso permite que a plataforma de gerenciamento possa fazer configurações via interface gráfica, sem a necessidade de CLI, permitindo configurações em massa.

Passo 5 – com o roteador operacional identificado, validado com seus certificados, ele entra em operação para identificar os dispositivos conectados nele através da interface RF, fazendo com que todos os dispositivos possam fazer parte da rede IoT. O servidor Radius é o responsável para que a plataforma possa fazer acesso aos roteadores via SSH diretamente pela aplicação

Passo 6 – para que um dispositivo IoT possa entrar na rede (ambiente IoT), é importante identificar qual tipo de comunicação será usada: WIFI ou WPAN. Os dispositivos precisam estar programados e configurados para “escutar” a interface WPAN. O roteador mais próximo vai identificar o dispositivo. Devido a uma configuração, é preciso colocar uma rota *default* na qual o pedido de entrada na rede seja enviado para a plataforma de gerenciamento.

Passo 7 – o pedido será validado porque o mesmo certificado gerado no PKI ECC está inserido no dispositivo e com isso é feito uma validação pelo servidor PKI ECC. Os certificados são carimbados e passa ser assinado pelo HSM garantindo mais um ponto de segurança no ambiente.

Passo 8 – A interface WPAN do roteador possui uma configuração para fornecer um IP através do DHCP externo. Por ser uma tecnologia muito ampla, o servidor DHCP disponibiliza um IPV6 fazendo uma soma da faixa de IP WPAN mais a configuração implantada no DHCP.

Passo 9 – Com o dispositivo validado, ele começa fazer parte da rede e por estar dentro da mesma faixa de IP e estar utilizando o protocolo UDP, a rede *mesh* neste caso é montada. Isso traz muitos benefícios porque alguns dispositivos não alcançam a interface do roteador, o maior benefício é utilizar os demais dispositivos como salto para alcançar a rede.

Passo 10 – Todo ambiente já pode ser monitorado e gerenciado. Usando os sistemas de gerenciamento, pode-se acompanhar o comportamento dos equipamentos, atualizar os firmwares, trocar nomes, mudar rotas entre outras características, isso tudo pode ser feito em massa.

5 MONITORAMENTO CONTÍNUO

O monitoramento contínuo é uma prática importante no ciclo de DevSecOps auxiliando na economia de recursos, manutenção preventiva, desenvolvimento de produtos, análise de riscos e na distinção real dos problemas que podem ocorrer nos ambientes.

Podemos citar uma das ameaças que merece atenção e pode ser mitigada com o uso do monitoramento contínuo. Atualmente, 99,9% do tráfego para os *honeypots* é automatizado, porém isto é um cenário terrivelmente perigoso, já que a maioria dos exércitos de *bots* e *malwares* modernos são programados para atacar em escala. Portanto, medidas

para rastreamento e estratégias de monitoramento de logs detalhados devem ser empregados.

Sabemos que podemos fortalecer a segurança da IoT com uma estratégia sábia de gerenciamento de logs. Então, como podemos aproveitar esses logs de eventos para melhorar a segurança cibernética desses pontos de acesso, muitas vezes extremamente vulneráveis, aos nossos sistemas?

À medida que os dispositivos IoT se comunicam entre si e com as redes do sistema, inúmeros arquivos de log são gerados em tempo real de forma constante. Uma grande quantidade de dados e eventos podem ser monitorados e supervisionados tanto para fins de solução de problemas quanto como parte de estratégias preventivas. É impossível acompanhar todas as atividades diferentes de uma infinidade de dispositivos IoT, pois muitos processos de monitoramento não são dimensionados para lidar com seu grande volume. Deve-se ter uma solução de gerenciamento de log rápida e escalável, e evitar um sistema de log inchado que possa atrapalhar o controle adequado da rede.

O SIEM é uma solução de gerenciamento de informações (SIM) e de gerenciamento de eventos (SEM) de segurança. Ele coleta dados de log de eventos de várias fontes, identifica irregularidades conforme padrões de métricas para cada equipamento, ambiente ou item com análise em tempo real e toma as medidas apropriadas.

No mercado existe diversas ferramentas, a maioria são pagas e muitas possuem um amplo repertório de recursos, como o Datadog, Dynatrace, Zabbix, Graylog, Elk e Splunk.

Podemos destacar no uso destas ferramentas, a centralização de todos os logs de acesso, permitindo que os gerentes de TI mantenham todos os dispositivos vulneráveis sob seu controle. A ingestão automática de logs de auditoria em um repositório centralizado permite que as organizações identifiquem possíveis violações de segurança ou uso indevido interno de informações assim que elas ocorrerem. O registro moderno está evoluindo para novos formatos de registro mais estruturados.

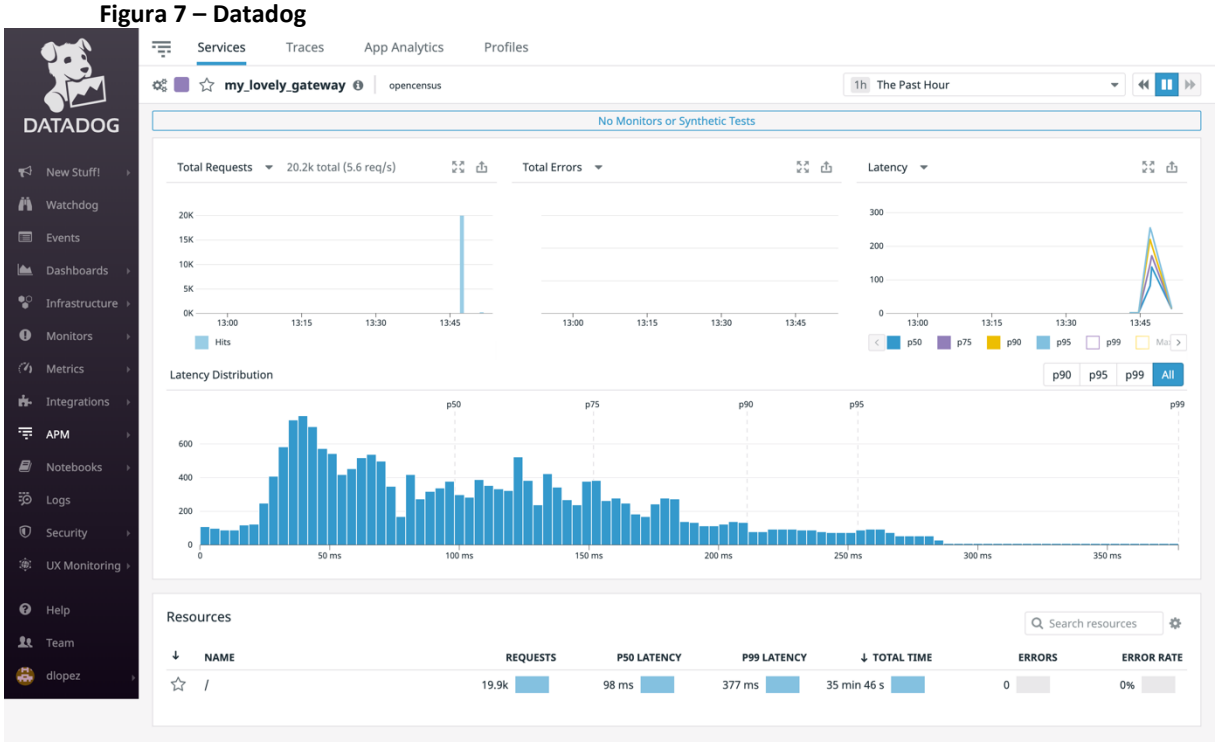
As novas ferramentas de gerenciamento são capazes de lidar com dados muito mais complexos do que apenas texto simples. A análise de logs de auditoria e dispositivo é um requisito padrão para avaliar danos ao sistema, melhorar a segurança da IoT e estabelecer protocolos de reação e mitigação ágeis.

Além disso, os logs de eventos podem ser usados para trabalhos forenses cibernéticos – as trilhas de auditoria são as evidências que serão investigadas para reconstruir a “história” de um problema recente. Todos os dispositivos conectados compartilham muitas informações entre si para que, quando ocorrer uma invasão, um rastro seja deixado para trás.

Além de apenas analisar os acessos de entrada comprometidos, o registro de eventos centralizado nos permite conectar os pontos e encontrar correlações entre eventos que, de outra forma, podem parecer não relacionados. Se as coisas derem errado, não importa o que aconteça, e a invasão já aconteceu, pelo menos coletar informações pertinentes dos logs pode ajudar a evitar resultados semelhantes no futuro (CARSTENSEN, 2019).

Datadog e Dynatrace são duas grandes plataformas de monitoração do mercado. Atualmente são conhecidas como ferramentas de *Observability*, podendo monitorar qualquer tipo de *device* em uma rede por eventos ou por SNMP, tudo vai de acordo com custo do projeto. As ferramentas de monitoração são grandes aliados de todo ambiente seja ele simples ou robusto, trazendo resultados de métricas, performance, análise de riscos entre outros dados de acordo com a tecnologia aplicada. A figura 7 mostra a tela do Datadog.

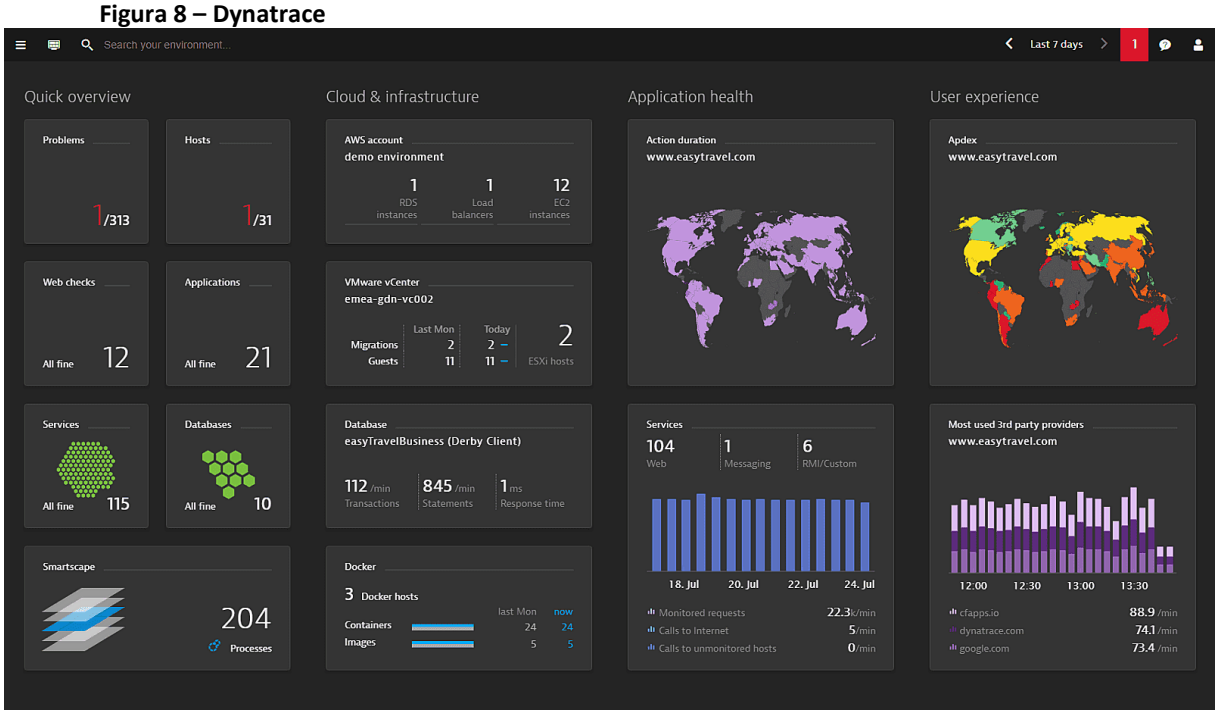
Figura 7 – Datadog



Fonte: ALTMAN, 2021.

A figura 8 mostra o *dashboard* do Dynatrace. Nele, podem ser configurados painéis para monitorar o status em tempo real, facilitando a identificação de anomalias e análise de tendências nos dados.

Figura 8 – Dynatrace



Fonte: ZAHRER, 2018.

Caso o projeto possua orçamento curto, podemos agilizar com plataformas de *open source* como Zabbix, Graylog entre outras no mercado de *Observability*.

O Zabbix pode fazer a monitoração via SNMP dependendo da sua solução. O Zabbix possui um *dashboard* que pode trazer os eventos do seu ambiente gerando alertas para *troubleshooting* (figura 9).

Figura 9 – Zabbix

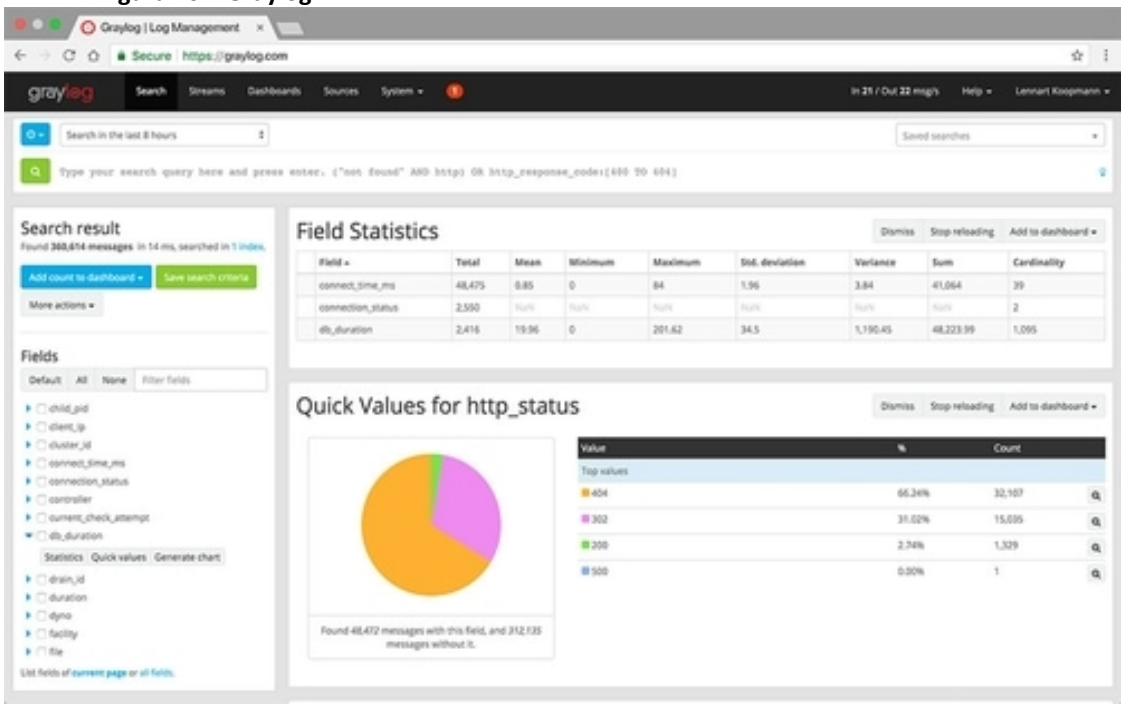
Fonte: ZABBIX, 2022.

Mas se a solução não possui protocolos SNMP e trabalha com outros protocolos ou até mesmo somente eventos, uma plataforma gratuita que também pode ser customizada para que o seu ambiente não fique descoberto é o Graylog (figura 10).

O Graylog é uma ferramenta gratuita para Gerenciamento de Logs e o SIEM fácil, rápida, acessível e eficaz. Já foi implantada em mais de 50.000 instalações em todo o mundo, É uma solução premiada criada para velocidade e escala na captura, armazenamento e análise em tempo real de *terabytes* de dados de máquina (GRAYLOG, 2022a).

Configurando o Graylog na recepção de logs, dependendo da gravidade do evento podemos fazer uma integração diretamente com o Zabbix para que ele possa gerar um alerta e informar os responsáveis pelo ambiente que está sendo monitorado.

Figura 10 – Graylog



Fonte: GRAYLOG, 2022b.

6 RESULTADOS E DISCUSSÕES

A segurança é considerada um objetivo negativo, ou seja, não existe uma forma de dizer que o objetivo foi alcançado, mas que certas ameaças e riscos foram mitigados. Porém, outras vulnerabilidades sejam em relação a tecnologias, pessoas ou procedimentos podem surgir e se tornarem novos riscos.

Neste sentido, as boas práticas apresentadas aqui, incluindo a utilização dos conceitos de DevSecOps, plataformas de nuvem IoT, como a Cisco IoT FND e softwares de monitoramento SIEM mostram que esses riscos podem ser diminuídos, oferecendo: consciência de segurança no desenvolvimento do sistema IoT, testes do código-fonte e da implementação, tecnologias de controle de acesso aos dispositivos IoT e seus dados, monitoramento contínuo para detecção rápida de falhas de segurança e tomadas de decisão para recuperação diante de possíveis ameaças e incidentes.

Todas estas práticas foram implementadas em uma empresa de grande porte, conforme a arquitetura apresentada, mostrando robustez na segurança cibernética do sistema IoT.

7 CONCLUSÃO

Muitas soluções estão disponíveis no mercado para gerar maior segurança cibernética aos sistemas IoT, utilizando os conceitos do ciclo DevSecOps, incluindo plataformas de desenvolvimento, gerenciamento, monitoração e muito mais recursos que podem ser investidos para agregar valor à solução.

Em cada projeto, cada solução, cada segmento, é importante utilizar as boas práticas para desenvolvimento voltado para segurança, compreender melhor qual público e objetivo alcançado. Existem várias soluções *open source*, sejam em gerenciamento quanto ao

monitoramento, porém o custo zero praticamente é inexistente, porque gastos são necessários para armazenar dados, infraestrutura lógica e física, e mão de obra especializadas no entendimento de IoT.

Além disso, destaca-se que soluções de baixo custo pode acarretar altos custos em segurança principalmente quando envolver dados sensíveis, tráfego de dados com valores. E está claro que as empresas que vendem as soluções fechadas como a Cisco, Huawei entre outros, garantem mais qualidade e suporte, trazendo credibilidade na venda de projetos.

Portanto, destaca-se a importância da escolha e configuração de arquitetura e plataformas IoT e SIEM que ofereçam o suporte das boas práticas contempladas no DevSecOps para o desenvolvimento e operação de aplicações IoT com segurança e confiabilidade na coleta, armazenamento, análise de dados e disponibilização dos resultados.

REFERÊNCIAS

ALTMAN, Natalie. **Introducing Network Device Monitoring**. 2021. Disponível em: https://www.datadoghq.com/blog/network-device-monitoring/. Acesso em: 29 ago. 2022.

BARRERA, D.; BELLMAN, C.; VAN OORSCHOT, P. Security Best Practices: A Critical Analysis Using IoT as a Case Study. **ACM Transactions on Privacy and Security**, v. 26, n. 2, p. 13:1-13:30, 13 mar. 2023.

CARSTENSEN, Nick. **Improving IoT security with log management.** 2019. Disponível em: https://www.graylog.org/post/improving-iot-security-with-log-management. Acesso em: 29 ago. 2022.

CISCO. **Cisco IoT Field Network Director User Guide, Release 4.9.0**. 2022. Disponível em: https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/iot_fnd/guide/4_9/b-iot-fnd-user-guide-49/m-overview-of-cisco-iot-field-network-director.html. Acesso em: 29 ago. 2022.

CONVERGENCIA DIGITAL. **Transformação digital:** investimentos chegam a US$ 1,8 trilhão em 2022. 2022. Disponível em: https://www.convergenciadigital.com.br/Negocios/Transformacao-digital%3A-investimentos-chegam-a-US%24-1%2C8-trilhao-em-2022-60317.html. Acesso em: 30 jul. 2022.

GRAYLOG. **Graylog Open Source**. 2022a. Disponível em: https://www.graylog.org/products/open-source. Acesso em: 29 ago. 2022.

GRAYLOG. **About Graylog.** 2022b. Disponível em: https://www.graylog.org/about. Acesso em: 29 ago. 2022.

ITRON. **Intelligent streetlights**. 2022. Disponível em: https://www.itron.com/br/solutions/what-we-enable/smart-cities/intelligent-streetlights. Acesso em: 26 ago. 2022.

MACBRIDE, Elizabeth. **The dark web's criminal minds see Internet of Things as next big hacking prize.** 2023. Disponível em: https://www.cnbc.com/2023/01/09/the-dark-webs-criminal-minds-see-iot-as-the-next-big-hacking-prize.html. Acesso em: 23 maio. 2023.

MANN, D. E.; CHRISTEY, S. M. Towards a Common Enumeration of Vulnerabilities. **Proceedings of the 2nd Workshop on Research with Security Vulnerability Databases**. West Lafayette Indiana: CERIAS, 1999.

MOMENZADEH, B. et al. Best Practices Would Make Things Better in the IoT. **IEEE Security & Privacy**, v. 18, n. 4, p. 38–47, jul. 2020.

PAUL, David. 2021. IoT devices see more than 1.5bn cyberattacks so far this year. **DIGIT**, 13 set. 2021. Disponível em: https://www.digit.fyi/iot-security-kaspersky-research-attacks/. Acesso em: 23 maio. 2023

PAYNE, B. R.; ABEGAZ, T. T. Securing the Internet of Things: Best Practices for Deploying IoT Devices. Em: DAIMI, K. (Ed.). **Computer and Network Security Essentials**. Cham: Springer International Publishing, 2018. p. 493–506.

RED HAT. **O que é IoT? Internet das Coisas**. 2019. Disponível em: https://www.redhat.com/pt-br/topics/internet-of-things/what-is-iot. Acesso em: 26 ago. 2022.

RICKETTS, Janice et al. **Autenticação RADIUS com o Azure Active Directory**. 2022. Disponível em: https://docs.microsoft.com/pt-br/azure/active-directory/fundamentals/auth-radius. Acesso em: 26 ago. 2022.

RUSSELL, B.; DUREN, D. V. **Practical Internet of Things Security**. Birmingham: Packt Publishing Ltd, 2016.

SAMAILA, M. G. et al. IoT-HarPSecA: A Framework and Roadmap for Secure Design and Development of Devices and Applications in the IoT Space. **IEEE Access**, v. 8, p. 16462–16494, 2020.

SCHWAB, Klaus. **Aplicando a quarta revolução industrial**. São Paulo: Edipro, 2018.

VELOCITY BUSINESS SOLUTIONS. **IDC: 80 billion connected devices in 2025 for generating 180 trillion GB of Data and IoT opportunities**. 2018. Disponível em: https://www.vebuso.com/2018/02/idc-80-billion-connected-devices-2025-generating-180-trillion-gb-data-iot-opportunities/. Acesso em: 30 jul. 2022.

YASAR, Hasan. **Moving from DevOps to DevSecOps**. 2021. Disponível em: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=734098. Acesso em: 23 maio. 2023.

ZABBIX. **Zabbix features overview**. 2022. Disponível em: https://www.zabbix.com/br/features. Acesso em: 29 ago. 2022.

ZAHRER, Peter. **Organize your dashboards more effectively**. 2018. Disponível em: https://www.dynatrace.com/news/blog/organize-your-dashboards-more-effectively/. Acesso em: 29 ago. 2022.

ZETTLER, K. **Ferramentas de DevSecOps**. 2021. Disponível em: https://www.atlassian.com/br/devops/devops-tools/devsecops-tools. Acesso em: 23 ago. 2022.

SOBRE OS AUTORES

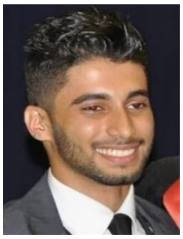
[i] **FABIO CASTRO LOPES**

Tecnólogo em Telecomunicações pela Unicid (2007) e especialista em Internet das Coisas (IoT) pela Faculdade SENAI São Paulo (2022). Mais de 15 anos de experiência na área de data centers, tecnologia de redes, sistemas operacionais, segurança e monitoração. Atualmente é consultor de tecnologia na área de projetos da empresa DXC. (https://orcid.org/0009-0007-6088-9752)

[ii] **DANIEL BARBUTO ROSSATO**

Doutor em Engenharia Eletrônica e Computação pelo ITA, Mestre em Engenharia Elétrica pela USP, Bacharel em Engenharia Elétrica pela USP. Medalha de bronze em Mecatrônica pela Worldskills. Possui experiência em projetos e manutenção de sistemas de automação industrial e como analista de TI. Atualmente, é professor na Faculdade SENAI São Paulo – Campus Mariano Ferraz, atuando em IoT e sistemas de controle. (https://orcid.org/0000-0003-1654-3424)

[iii] **CAIO VINÍCIUS RIBEIRO DA SILVA**



Possui pós-graduação em Automação Industrial pela Faculdade SENAI Mecatrônica (2017), pós-graduação em Inovação e Competitividade Industrial pela Faculdade SENAI “Theobaldo de Nigris”(2021) e graduação em Eletrônica Industrial pela Faculdade SENAI Anchieta(2012). Atualmente, é docente e coordenador de estágios na Faculdade SENAI São Paulo – Campus Mariano Ferraz, atuando em IoT e Tecnologia da Informação. (https://orcid.org/0000-0002-9421-2471)