Industria 4.0: Segurança em Redes de comunicação industrial e a implementação de sistema de detecção de intrusão.

Tiago Sutil Gabriel (tgabriel@klabin.com.br) , Murilo Oliveira Leme (muriloleme@utfpr.edu.br)

Resumo: Sistemas de automação industrial são o coração produtivo de muitas industrias, e nos últimos tempos muitas delas tem sofrido com o aumento de ataques cibernéticos industriais. Com isso diversas empresas de tecnologia estão desenvolvendo produtos e soluções que possibilitam as indústrias mitigar o risco de ataque ou proporcionar uma resposta rápida afim de evitar prejuízos financeiros. Dentre as soluções fornecidas atualmente no mercado estão os sistemas de detecção de intrusão (IDS), que tem como suas principais funções mapear o fluxo de dados que trafegam dentro das redes de automação (variáveis, valores e tempo de processo) e estabelecer um padrão, e também realizar o inventario dos ativos de rede e com isso propiciando uma análise sobre sistemas operacionais, firmwares, hardwares e suas vulnerabilidades. Este artigo apresenta uma visão sobre *cyber* segurança e as principais funcionalidades que um sistema de detecção de intrusão possui.
Palavras chave: Automação, Sistema, Intrusão.

Industry 4.0: Security in Industrial Communication Networks and Implementation of Intrusion Detection System.

Abstract: Industrial automation systems are the productive heart of many industries, and in recent times, many of them have suffered with the growth of industrial cyber-attacks. As a result, many technology companies are developing products and solutions that allows industries to mitigate the risk of attack or provide a fast response to avoid financial loss. Solutions currently available on the market include intrusion detection systems (IDS), whose main functions are to map the flow of data that travels within the automation networks (variables, values and process time) and to establish a standard, It also conducts an inventory of network assets and thus provides an analysis of operating systems, firmware, hardware and their vulnerabilities. This article provides an insight into cyber security and the key features that an intrusion detection system has.
Key-words: Automation, System, Intrusion.

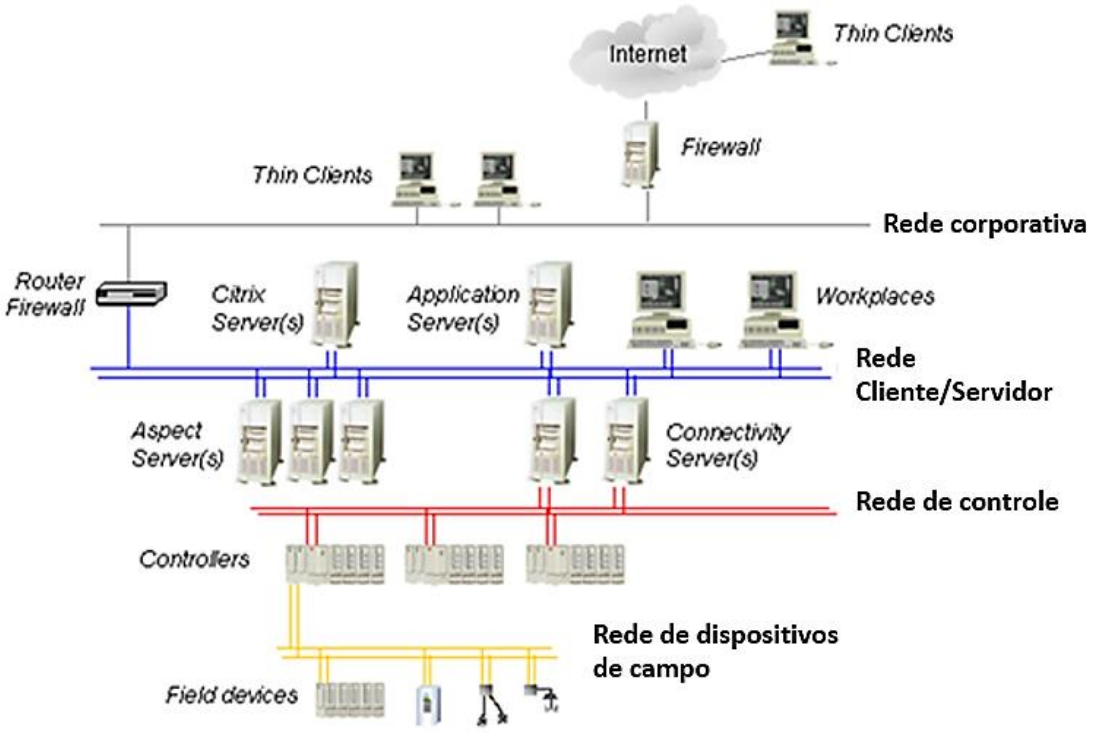
1. Introdução

Nas industrias da década de 1960 os controladores lógicos programáveis (CLP) apareceram com o objetivo de substituir os painéis de controle a relé, que necessitavam de uma atenção especial, visto que os reles eram mecânicos e, portanto, suscetíveis ao desgaste, com alto gasto de energia e eventuais produção de faíscas, e trouxeram consigo a grade vantagem de serem reprogramáveis, ou seja, não era mais necessário a substituição de vários cabos, que muitas vezes acabavam inviabilizando modificações de processo. Com o sucesso nas aplicações dos controladores lógicos programáveis, a demanda por novas funções e maior capacidade aumentou consideravelmente, e com isso os equipamentos evoluíram e cresceram em poder de processamento, número de entradas e saídas, e novas funções. Entretanto, estes controladores ainda usavam lógica discreta, ou seja, apenas dados digitais eram processados, isso limitava qualquer aquisição de dados analógicos de processo (Pressão,

vazão, nível e temperatura) bem como enviar um sinal analógico para um elemento de controle de processo, como bombas e válvulas de controle. O advento do microprocessador permitiu uma diminuição nos custos e tamanho dos CLPs, possibilitou que firmwares sejam escritos em várias linguagens, o que contribui para ciclos de programas mais rápidos, sistemas de entrada e saída mais compactos, interfaces especiais que permitem que aparelhos sejam conectados diretamente no CLP, outros grandes avanços do desenvolvimento de CLPs foram a capacidade de realizar funções que indiquem suas próprias falhas, bem como as falhas de máquina ou do processo, também o aumento do poder de processamento, confiabilidade e o surgimento das primeiras redes locais para comunicação entre CLPs e entre CLPs e computadores (Silveira;Lima; 2013).

Nos últimos anos as indústrias estão tendendo a cada vez mais automatizar os processos e diminuir a interação entre pessoas e máquinas, visando ganhos financeiros e de segurança.

Para atender essas necessidades as redes industriais de automação estão em constante evolução. Os sistemas de automação atuais são muito grandes e complexos, com isso podemos dividi-los em 3 camadas básicas: Nível de cliente servidor, controle e dispositivos (ABB, 2019).



Fonte: ABB (2009)

Figura 1- Topologia básica de automação

A camada de controle e cliente servidor é tipicamente uma rede Ethernet, e com isso possuem os mesmos problemas de *Cyber* segurança de uma rede de TI corporativa ou mesmo de uma rede residencial de computadores, ou seja, as redes industriais estão suscetíveis *a invasões externas, ataques de DoS (Denial of Service) e todos os tipos de* Malware. *Cyber* segurança pode ser definida como a prática que protege computadores, servidores, dispositivos móveis, sistemas eletrônicos, redes e dados de ataques maliciosos. Também é chamada de segurança de tecnologia da informação ou segurança de informações eletrônicas. O termo é muito

abrangente e se aplica a tudo o que se refere a segurança de computadores, recuperação de desastres e conscientização do usuário final (Kasperky, 2019).

Esta relação cada vez mais próxima entre as redes corporativas das empresas e as redes de controle e de chão de fábrica, tipicamente chamadas de redes industriais, responsáveis pela automação dos processos, tem levado a uma preocupação cada vez maior com a segurança cibernética.

2. Segurança cibernética em redes industriais.

Nos últimos anos a quantidade de ataques cibernéticos industriais tem aumentado exponencialmente e as perdas geradas para as indústrias são gigantescas. A Tabela 1 apresenta os principais ataques cibernéticos ocorridos em indústrias entre os anos de 2012 até 2019 e os danos causados que foram registrados por uma das maiores empresas provedoras de soluções de segurança no mundo.

Ano	Organização	Problema	Custo (US$)	Impacto
2019	Norsk Hydro	Lockergoga Ramsomware	40mi	Substituição de equipamentos e perda de produção
2019	Duke Energy	Compliance Violation	10mi	Financeiro e reputação
2018	Saudi Petrochem	Triton	Não informado	Não informado
2018	UK NHS	Wanna Cry	92mi	Equipamentos
2017	Merck	NotPetya	870mi	Custos de recuperação de produção
2017	FedEx	NotPetya	400mi	Custos de recuperação de produção
2017	Maersk	NotPetya	300mi	Custos de recuperação de produção
2017	Mondelez	NotPetya	188mi	Custos de recuperação de produção
2016	Ukrenergo	Insdustroyer	Interrupção	Mais de 225.000 casas sem energia
2012	Saudi Aramco	Shamoon	1bi	Substituição de equipamentos

Fonte: Nozomi Networks (2019)

Tabela 1 - Principais ataques cibernéticos

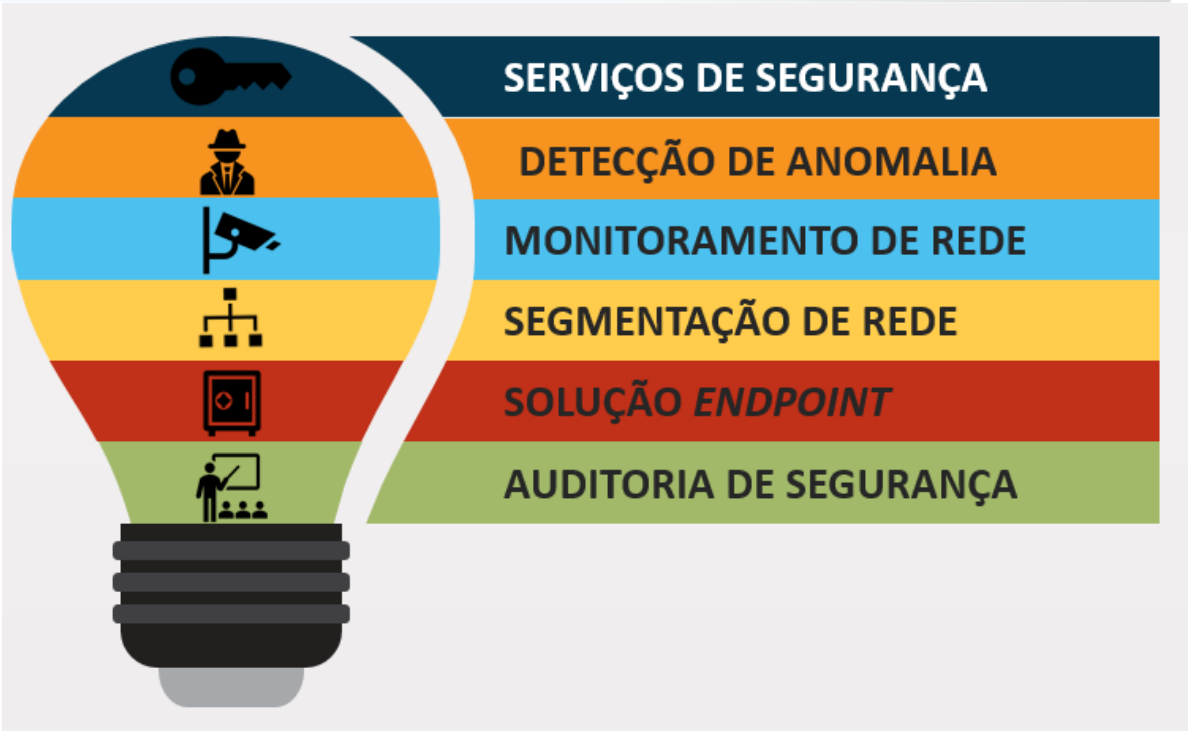
Ainda em relação a segurança cibernética, temos na Tabela 2 parte do relatório semanal (semana 19 de Agosto de 2019) de vulnerabilidades encontradas pelo departamento de segurança cibernética do governo americano. Nesta tabela é apresentado o nome do produto ao qual foi detectado a falha de segurança, a descrição da falha, a data de publicação e a pontuação CVSS (Sistema de pontuação de vulnerabilidade), que representa o nível de gravidade da vulnerabilidade encontrada.

Produto	Descrição	Publicação	Pontuação CVSS
bestwebsoft -- visitors_online	*Plugin* de visitantes online antes do 0.4 para *WordPress* possui possibilidade de inserção de comandos SQL.	16/08/2019	7.5
codepeople -- booking_calendar_contact_form	O plugin *booking* calendário antes da versão 1.0.24 para WordPress possui possibilidade de inserção de comandos SQL.	21/08/2019	7.5
duplicate_post_project -- duplicate_post	O *Plugin duplicate-post* plugin antes da versão 2.6 para *WordPress* possui possibilidade de inserção de comandos SQL.	21/08/2019	7.5
olimometer_project -- olimometer	O *plugin olimometer* antes da versão 2.57 para *WordPress* possui possibilidade de inserção de comandos SQL.	16/08/2019	7.5
soflyy -- wp_all_import	O *plugin wp-all-import* antes da versão 3.2.5 para *WordPress* possui possibilidade de inserção de comandos SQL	20/08/2019	7.5
wp_front_end_profile_project -- wp_front_end_profile	*O plugin wp-front-end-profile* antes da versão 0.2.2 para *WordPress* tem a possibilidade de escalada de privilégios.	21/08/2019	7.5
wpbusinessintelligence -- wp_business_intelligence	O *plugin wp-business-intelligence-lite* antes da versão 1.6.3 para *WordPress* possui possibilidade de inserção de comandos SQL.	16/08/2019	7.5

Fonte: Cybersecurity and Infrastructure Security Agency (CISA) (2019)

Tabela 2- parte do relatório semanal de vulnerabilidades

Para se proteger destes ataques, as indústrias estão buscando no mercado soluções de *cyber* segurança para proteção dos ambientes de automação. A Figura 3 apresenta uma sugestão de passos que uma indústria que possui uma grande rede de automação pode seguir afim de estar protegida contra ataques cibernéticos.



Fonte: Klabin (2019)

Figura 2 - Passos para *Cyber* segurança

Como início da trajetória de uma indústria em *cyber* segurança para redes de automação industrial é extremamente indicado a contratação de uma empresa especializada em segurança para a realização de uma auditoria total dos sistemas de automação instalados. Esta auditoria permite que as pessoas responsáveis pela segurança cibernética possam obter visibilidade e o status atual das redes, equipamentos, processos e cultura dos funcionários. Ao final da auditoria a empresa contratada deve fazer a entrega de um plano de segurança cibernética.

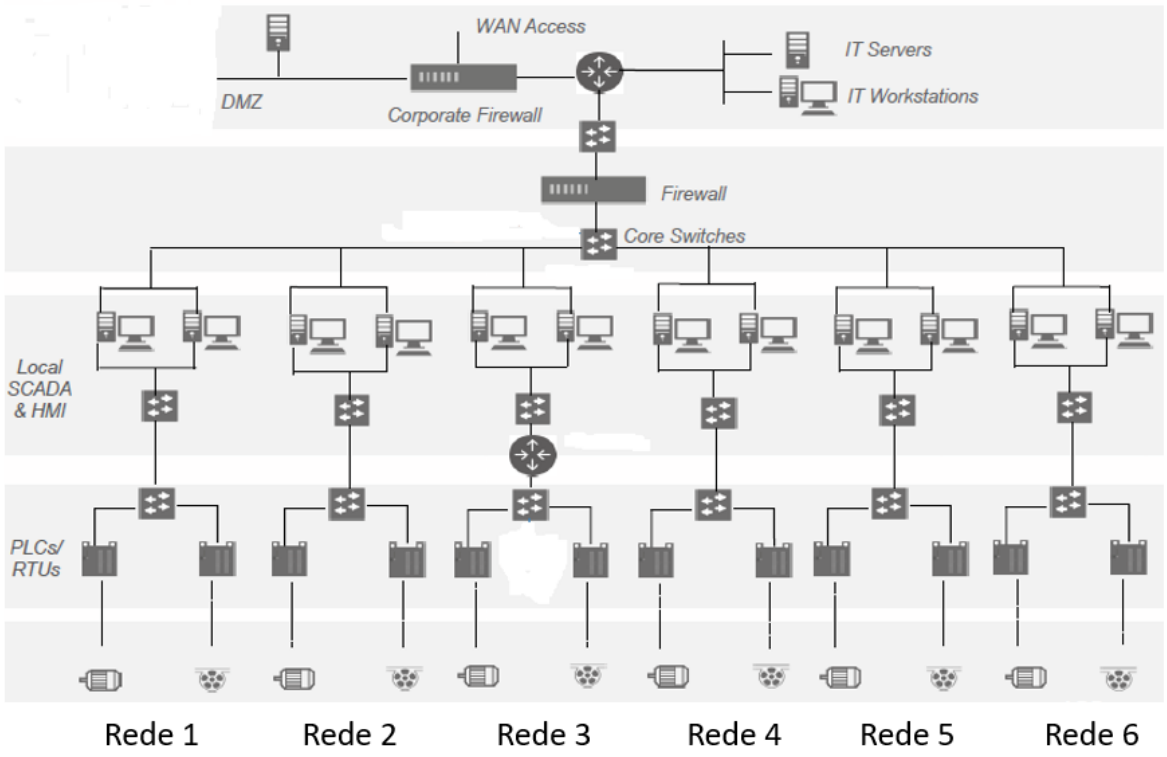
O segundo passo da trajetória é a aquisição de uma boa solução em *endpoint security* que além de realizar a função de uma antivírus também inclui recursos como gerenciamento de permissões de instalação e de acessos a aplicativos, controle de acesso à rede e à Internet, gerenciamento contra perda de dados, controle de aplicação , controle de conexão de dispositivos (USB, CD/DVD, Floppy, etc.), proteção de sistemas operacionais legados (Windows XP, 2003, etc) e levantamento do inventário de hardware conectado à rede da organização.
Para a solução de *endpoint security* existem várias empresas no mercado qualificadas, a Figura 4 apresenta um quadro criado pela consultoria Gartner apresentando um comparativo entres as principais empresas e quais estão se destacando no ano de 2019.

Fonte: Gartner *EndPoint* Protection *Plataform*s (2019)

Figura 3 - Principais empresas para solução Endpoint security

O terceiro passo da trajetória de segurança cibernética é definir uma adequada segmentação de rede, isso tem como principal objetivo o bloqueio de comunicações impróprias ou maliciosas entre redes. Isso é crucial para garantir que o acesso à rede seja mantido e com alto nível de proteção, garantindo a integridade dos dados e propriedade intelectual das companhias, limitando, por exemplo, a disseminação de um *malware* por toda a rede.

A adoção de uma abordagem adequada de segregação de recursos de rede permite aos profissionais estabelecer políticas que habilitem somente aos funcionários responsáveis o acesso a certas informações e aplicações, servidores e recursos de rede específicos. A aplicação da segmentação de rede adequada pode tornar muito mais difícil para um invasor localizar e obter acesso a informações valiosas de toda a empresa. Em muitos casos, quando um ataque está em andamento, a segmentação pode ser utilizada para fornecer controles dinâmicos na contenção da invasão, limitando possíveis danos e auxiliando na identificação do ataque através de alertas de acesso indevido. A figura 5 apresenta um modelo ideal de segmentação de redes de automação dentro de uma indústria que possui diversos fabricantes de equipamentos de automação e processo.



Fonte: Nozomi *Networks – Proof of concept* (2019)

Figura 4 - Topologia de segmentação de redes de automação

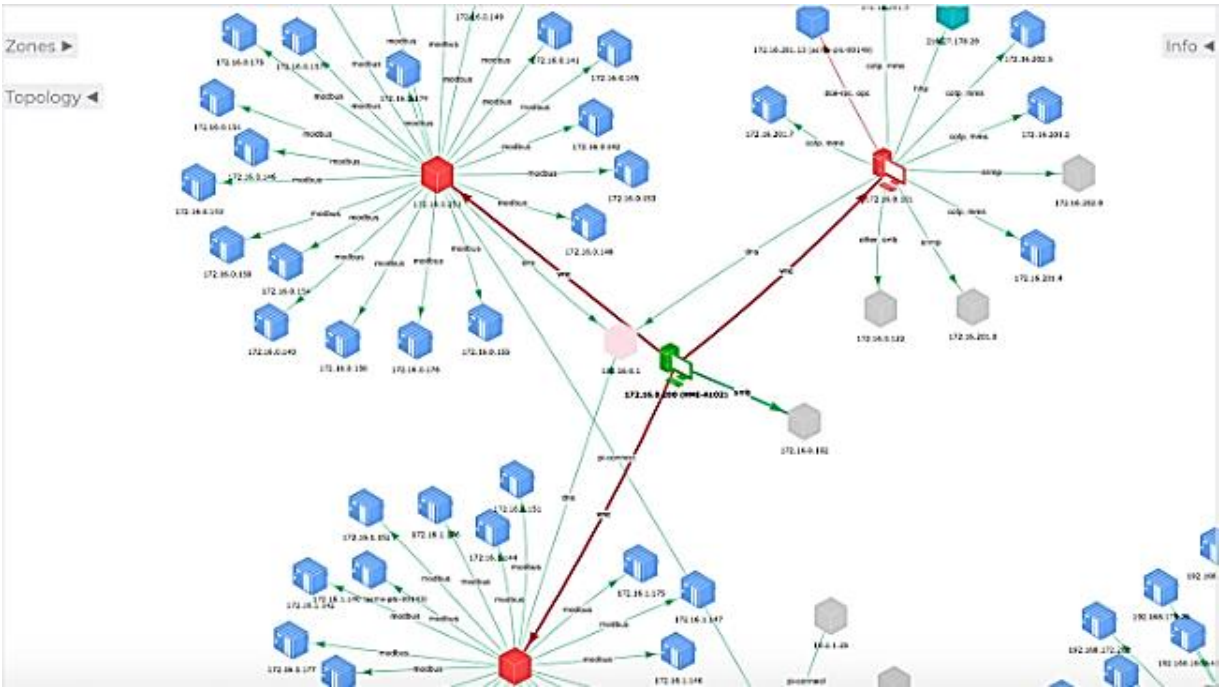
O quarto e quinto passo da trajetória de *Cyber* segurança serão abordados em um item especifico neste artigo pois trata se da solução completa de um sistema de detecção de intrusão.

O Sexto e último passo da Trajetória acontece após todos os itens previamente apontados estiverem aplicados, ele trata-se da contratação de uma empresa especializada em *cyber* segurança para realizar o monitoramento continuo das redes de automação, ela irá atuar em casos de emergências e trabalhar preventivamente evitando a ocorrência de incidentes.

3. Implementação de sistemas de detecção de intrusão.

Os itens 4 e 5 da trajetória em *cyber* segurança aponta 3 itens que agrupados resumem uma solução de detecção de intrusão em um sistema de automação industrial. O item monitoramento da rede e visibilidade é uma funcionalidade onde o sistema de detecção de intrusão quando instalado nas redes de automação irá primeiramente mapear todos os dispositivos nelas contidos (servidores, switches, computadores, controladores, roteadores e etc) e irá obter dados como: nome do dispositivo, tipo, serial *number*, versão de firmware, endereço IP, endereço MAC . A partir dos dados de dispositivos coletados a ferramenta irá disponibilizar para o usuário do sistema um mapeamento da base instalada dos dispositivos por segmento de rede de automação.

A figura 6 apresenta graficamente um mapeamento de rede realizado por um sistema de identificação de intrusão onde estão apresentados graficamente os dispositivos pertencentes a cada rede a cada rede e o fluxo de dados entres os mesmos.



Fonte: Nozomi *Networks – Proof of concept* (2019)

Figura 5 - Tela de mapeamento de dispositivos em uma rede

Com o levantamento de todos os dispositivos contidos nas redes de automação e suas características, o sistema de detecção de intrusão também é capaz de apontar problemas e vulnerabilidades levando em consideração sistemas operacionais, firmwares, versões de aplicativos e pacotes de atualizações. Na grande maioria dos casos, a base comparativa para conclusões quanto a segurança de utilização de um determinado software e as vulnerabilidades ligadas a ele é o repositório de gerenciamento de vulnerabilidade do governo americano. A figura 7 traz um exemplo do de uma tela onde cada dispositivo é avaliado e classificado quanto a sua vulnerabilidade.

ASSET	TYPE	OS/FIRMWARE	COUNT	SCORE DISTRIBUTION	SCORE GROUPS
10.8.96.222	computer	Windows 10	1134		156 547 431
10.8.48.197	computer	Windows 10	553		132 317 104
10.8.97.6	computer	Windows 10	553		132 317 104
10.8.48.149	computer	Windows 10	553		132 317 104
00:1b:1b:ba:45:1f	switch	Firmware: V05.01.00	2		2

Fonte: Nozomi *Networks* (2019)

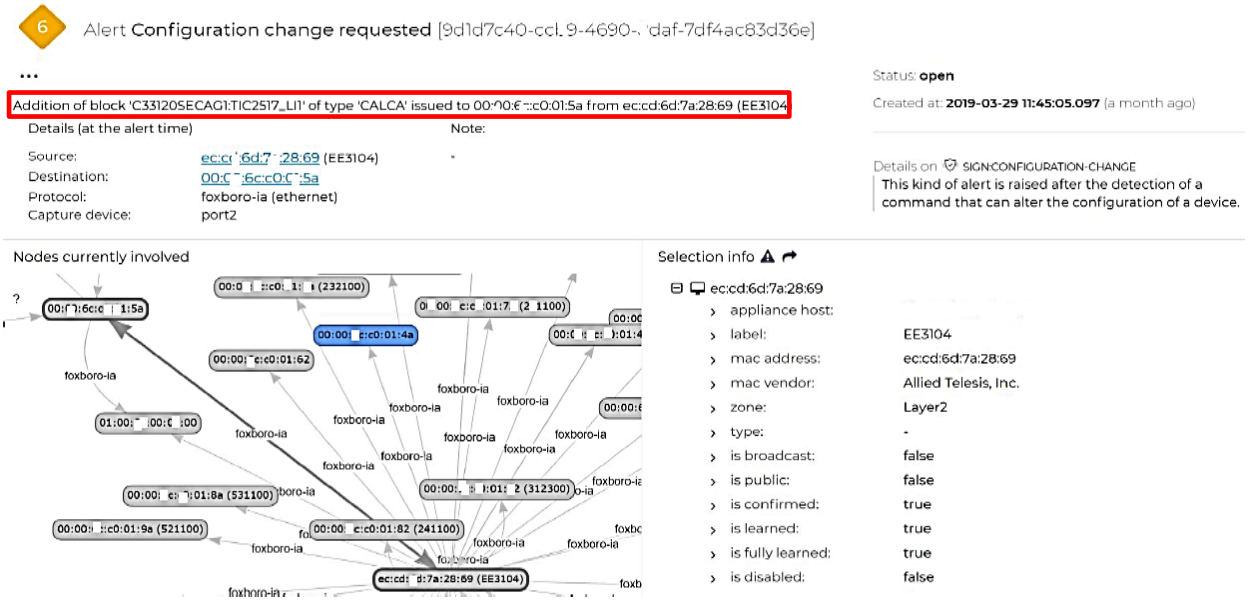
Figura 6 - Tela de classificação de dispositivo quanto a sua vulnerabilidade

Após a realização do mapeamento e a classificação dos ativos contidos na rede, o sistema irá por um tempo determinado (dependente do tamanho da rede) monitorar o trafego de dados entre esses dispositivos, levando em consideração quais dispositivos se comunicam entre si e por quais redes, protocolos de rede, *throughput*, funções, sub funções, portas utilizadas e

tempo de trafego. Esse tempo de monitoramento serve para o sistema de detecção de intrusão de construir um padrão de comportamento dentro de cada segmento de rede de automação da empresa.

Após finalizado o tempo de aprendizado do sistema de detecção de intrusão quanto ao comportamento das redes de automação e realizado a eliminação de alguns problemas identificados durante a fase monitoramento inicial que normalmente são: pontos de acesso a redes não conhecidos pela equipe responsável pelas rede de automação, softwares não autorizados instalados em máquinas, uso inadequado de ativos da rede de automação, computadores totalmente desprotegidos e redes não totalmente segmentadas, inicia se o monitoramento ativo das redes.

Com o monitoramento ativo das redes iniciado o sistema de detecção de intrusão é capaz de identificar qualquer comportamento estranho ou fora do padrão já estabelecido dos ativos contidos na rede de automação. Quando o sistema detecta um evento não esperado ele emite um alerta apresentando informações relativas a natureza do evento, ativos que geraram o alerta e data e hora da ocorrência. Em destaque em vermelho na figura 8 é apresentado um exemplo de alerta gerado por um sistema de detecção de intrusão, nele foi detectado a alteração na configuração de blocos em um dos controladores presente na rede de automação industrial.



Fonte: Nozomi *Networks – Proof of concept* (2019)

Figura 7 - Alerta de comportamento não esperado em rede de automação

.

A informação do alerta gerado pelo sistema possibilita com que a equipe responsável pelas redes de automação possa analisar e definir ações para correções. Alguns fabricantes de sistemas IDS também oferecem a proteção ativa quanto a ataques cibernéticos, ou seja, o sistema detecta o problema e toma uma ação imediata, este modo de operação mesmo ainda não sendo muito utilizado é muito importante pois possibilita a desconexão ou isolamento de um segmento de rede impedindo assim proliferação de *malwares* (programas maliciosos que visam causar danos, roubar o alterar informações em um computador ou rede de computadores) ou restrição de acesso de possíveis atacantes externos.

4. Conclusão

Os usuários de redes domésticas e redes de TI corporativa a muito tempo já convivem com os riscos de segurança a eles associados, e com isso já existem diversos meios extremamente eficazes de proteção. Com o advento da indústria 4.0, que trouxe para as indústrias a conexão e a troca de dados como a chave do sucesso, as redes de automação antes consideradas isoladas das redes corporativas passaram a trocar uma enorme quantidade de dados com clientes externos. Para os sistemas de automação industrial é relativamente nova esta preocupação, muitas empresas começaram a pouco tempo a busca por informações e soluções para *cyber* segurança, um dos grandes empecilhos para as empresas principalmente as brasileiras é o alto custo para adequação da base instalada para atender as demandas de segurança e os altos valores dos produtos oferecidos no mercado. Para as empresas que conseguem investir em soluções os sistemas de detecção de intrusão apresentam um grande ganho pois possibilitam um excelente controle sobre a base instalada de equipamentos nas redes de automação e propiciam para a equipe responsável pelas redes um monitoramento ativo, gerando alertas e avisos quanto as possíveis ameaças possibilitando que realizem ações que caso não executadas poderiam gerar grandes perdas para a empresa, porem apenas as instalações de softwares e sistemas de proteção não garantem que uma empresa estará totalmente segura, o comportamento humano é uma peça chave no processo, as simples ações de manter painéis de servidores fechados e chaveados, evitar a inserção de dispositivos de mídia em equipamentos das rede de automação e a utilização de senhas em estações de operação e engenharia já ajudam bastante a evitar problemas de *cyber* segurança.

Referências

Cybersecurity and infrastructure security agency (CISA). Disponível em <http://www.us-cert.gov/ics> Acesso em: 03 set. 2019.

KASPERSKY. Disponível em <https://www.kaspersky.com.br/resource-center> Acesso em: 22 set. 2019.

Lugli,A.B.; Santos M.M.D. Redes industriais: **Evolução, motivação e funcionamento**. InTech, Minas Gerais 2011.

Nozomi Networks. Nozomi ***Networks solution Brief***. 2019

Nozomi Networks. ***Proof of concept***. 2019

Richter, C. **Curso de automação industrial**. Porto Alegre 2001.

Sestito, G. **Uso de Ethernet em automação industrial, São Carlos Novembro 2011**.Trabalho de conclusão de curso – Universidade de São Paulo.

Silveira,L.;Lima,W. **Um breve histórico conceitual da Automação Industrial e Redes para Automação Industrial**, UFRN, Lagoa Nova - 2013

Klabin. **Apresentação de soluções em cyber segurança**. 2019

Weekly summaries of new vulnerabilities. Disponível em <https://www.us-cert.gov/ncas/bulletins > Acesso em: 03 set. 2019.