

Módulo 20: Inteligência de ameaças



CyberOps Associate v1.0

Prof. Clemilson Oliveira

clemilson.oliveira@edu.sc.senai.br



Objetivos do módulo

Título do módulo: Inteligência contra ameaças

Objetivo do módulo: usar várias fontes de inteligência para localizar ameaças de segurança atuais.

Título do Tópico	Objetivo do Tópico
Fontes de informação	Descrever as fontes de informações usadas para comunicar ameaças emergentes à segurança de rede.
Serviços de inteligência de ameaças	Descrever vários serviços de inteligência de ameaças.

20.1 Fontes de informações

Comunidades de inteligência de rede sobre ameaças

- Para proteger eficazmente uma rede, os profissionais de segurança devem manter-se informados sobre as ameaças e vulnerabilidades.
- Há muitas organizações de segurança que fornecem inteligência de rede, recursos, workshops e conferências para ajudar os profissionais de segurança.
- Para permanecer eficaz, um profissional de segurança de rede deve:
 - **Mantenha-se a par das ameaças mais recentes** — Inclui a subscrição de feeds em tempo real relativos a ameaças, a análise rotineira de Web sites relacionados à segurança, o seguimento de blogues e podcasts de segurança e muito mais.
 - **Continuar a atualizar habilidades** — Inclui participar de treinamento relacionado à segurança, workshops e conferências.
- **Nota:** A segurança de rede tem uma curva de aprendizagem muito acentuada e requer um compromisso com o desenvolvimento profissional contínuo.

Comunidades de inteligência de rede de inteligência de ameaças (Cont.)

A tabela lista a organização de segurança de rede importante.

Empresa	Descrição
SysAdmin, Auditoria, Rede, Segurança (SANS)	<p>Os recursos do Instituto SANS são amplamente gratuitos mediante solicitação e incluem:</p> <ul style="list-style-type: none">• O Internet Storm Center - o popular sistema de alerta antecipado da internet• NewsBites - O resumo semanal de artigos de notícias sobre segurança informática.• @RISK - O resumo semanal de vetores de ataque recém-descobertos, vulnerabilidades com explorações ativas e explicações de como os ataques recentes funcionaram.• Alertas de segurança rápidos• Sala de Leitura - Mais de 1.200 trabalhos de pesquisa originais premiados.• O SANS também desenvolve cursos de segurança.
Mitre	<p>A Mitre Corporation mantém uma lista de Vulnerabilidades e Exposições Comuns (CVE) usada por organizações de segurança proeminentes.</p>

Fontes de Informação Comunidades de Inteligência de Rede (Cond.)

Empresa	Descrição
Fórum de equipes de resposta a incidentes e segurança (FIRST)	É uma organização de segurança que reúne uma variedade de equipes de resposta a incidentes de segurança de computador de organizações governamentais, comerciais e educacionais para promover a cooperação e coordenação no compartilhamento de informações, prevenção de incidentes e reação rápida.
SecurityNewsWire	Um portal de notícias de segurança que agrega as últimas notícias relativas a alertas, explorações e vulnerabilidades.
International Information Systems Security Certification Consortium (ISC) ²	Fornece produtos educacionais neutros e serviços de carreira a mais de 75 mil profissionais do setor em mais de 135 países.
Center for Internet Security (CIS)	É um ponto focal para prevenção, proteção, resposta e recuperação de ameaças cibernéticas para governos estaduais, locais, tribais e territoriais (SLTT) por meio do Centro de Análise e Compartilhamento de Informações Multiestaduais (MS-ISAC). O MS-ISAC oferece alertas e alertas de ameaças cibernéticas 24 horas por dia, 7 dias por semana, identificação de vulnerabilidades e mitigação e resposta a incidentes.

Relatórios de segurança cibernética daCisco sobre ameaças

- Os recursos para ajudar os profissionais de segurança a manter-se a par das ameaças mais recentes são o Relatório Anual de Segurança Cibernética da Cisco e o Relatório de Segurança Cibernética do Meio Ano.
- Esses relatórios fornecem uma atualização sobre o estado de preparação para a segurança, análise especializada das principais vulnerabilidades, fatores por trás da explosão de ataques usando adware, spam e assim por diante.
- Os analistas de segurança cibernética devem se inscrever e ler esses relatórios para saber como os atores de ameaças estão direcionando suas redes e quais ações podem ser tomadas para mitigar esses ataques.

Blogs e podcasts de segurança de inteligência contra ameaças

- Blogs e podcasts também fornecem conselhos, pesquisas e técnicas de mitigação recomendadas.
- A Cisco fornece blogs sobre tópicos relacionados à segurança de vários especialistas do setor e do Cisco Talos Group.
- Cisco Talos oferece uma série de mais de 80 podcasts que podem ser reproduzidos a partir da internet ou baixados para o seu dispositivo de escolha.

20.2 Serviços de inteligência de ameaças

Cisco Talos

- Talos é uma das maiores equipes de inteligência de ameaças comerciais do mundo e é composta por pesquisadores, analistas e engenheiros de classe mundial.
- O objetivo é ajudar a proteger usuários corporativos, dados e infraestrutura contra adversários ativos.
- A equipe coleta informações sobre ameaças ativas, existentes e emergentes e, em seguida, fornece proteção abrangente contra esses ataques e malware para seus assinantes.
- Os produtos da Cisco Security podem usar a inteligência de ameaças Talos em tempo real para fornecer soluções de segurança rápidas e eficazes.
- O Cisco Talos também fornece software, serviços, recursos e dados gratuitos e mantém os conjuntos de regras de detecção de incidentes de segurança para as ferramentas de segurança de rede Snort.org, ClamAV e SpamCop.



FireEye

- FireEye é outra empresa de segurança que oferece serviços para ajudar as empresas a proteger suas redes.
- Ele usa uma abordagem em três vertentes que combina inteligência de segurança, experiência em segurança e tecnologia.
- Ele oferece SIEM e SOAR com a Plataforma de Segurança Helix, que usa análise comportamental e detecção avançada de ameaças e é apoiada pela rede mundial de inteligência contra ameaças FireEye Mandiant.

FireEye (Cont.)

Sistema de segurança FireEye:

- O FireEye Security System bloqueia ataques em vetores de ameaças da Web e de e-mail e malware latente que reside em compartilhamentos de arquivos.
- Ele pode bloquear malware avançado que facilmente ignora as defesas tradicionais baseadas em assinaturas e compromete a maioria das redes empresariais.
- Ele aborda todos os estágios de um ciclo de vida de ataque com um mecanismo sem assinatura que utiliza análise de ataque stateful para detectar ameaças de dia zero.

Compartilhamento automático de indicadores dos serviços de inteligência

- O Automated Indicator Sharing (AIS) é um serviço gratuito oferecido pelo Departamento de Segurança Interna dos EUA (DHS).
- O AIS permite a troca em tempo real de indicadores de ameaças cibernéticas entre o Governo Federal dos EUA e o setor privado.
- O AIS cria um ecossistema quando uma ameaça é reconhecida. Mais tarde, ele é imediatamente compartilhado com a comunidade para ajudá-los a proteger suas redes contra essa ameaça em particular.

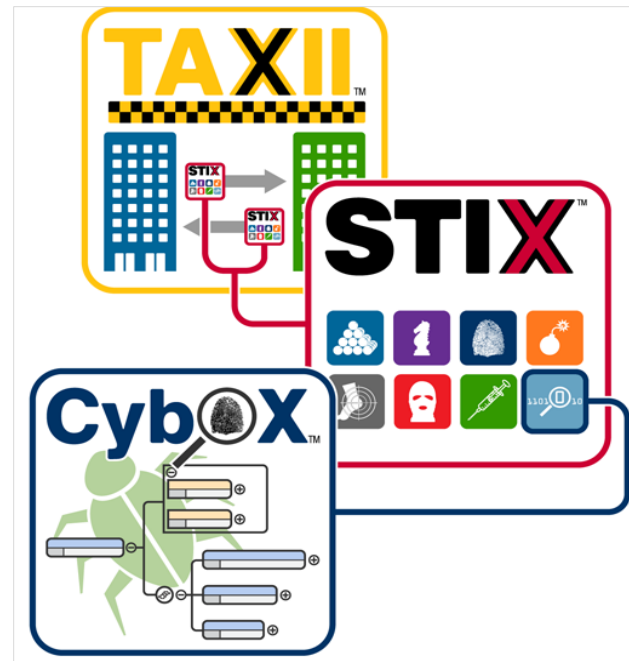
Banco de dados de vulnerabilidades e exposições comuns (CVE) do Threat Intelligence Services

- O governo dos Estados Unidos patrocinou a MITRE Corporation para criar e manter um catálogo de ameaças de segurança conhecidas chamadas Vulnerabilidades e Exposições Comuns (CVE).
- O CVE serve como um dicionário de Identificadores CVE para vulnerabilidades de segurança cibernética publicamente conhecidas.
- A MITRE Corporation define identificadores CVE exclusivos para vulnerabilidades de segurança da informação publicamente conhecidas para facilitar o compartilhamento de dados.

Serviços de inteligência de ameaças Padrões de comunicação de inteligência

Três padrões comuns de compartilhamento de informações sobre ameaças incluem o seguinte:

- **STIX (Structured Threat Information Expression)** - Este é um conjunto de especificações para troca de informações sobre ameaças cibernéticas entre organizações.
- **Trusted Automated Exchange of Indicator Information (TAXII)** — Esta é a especificação para um protocolo de camada de aplicação que permite a comunicação da CTI através de HTTPS. TAXII foi projetado para suportar STIX.
- **CyBox** - Este é um conjunto de esquema padronizado para especificar, capturar, caracterizar e comunicar eventos e propriedades de operações de rede que suporta muitas funções de segurança cibernética.



Serviços de inteligência contra ameaças padrões de comunicação de informações sobre ameaças (Condd.)

- A plataforma MISP (Malware Information Sharing Platform) é uma plataforma de código aberto para compartilhar IOCs para ameaças recém-descobertas.
- O MISP é apoiado pela União Europeia e é usado por mais de 6.000 organizações em todo o mundo.
- O MISP permite o compartilhamento automatizado de IOCs entre pessoas e máquinas usando STIX e outros formatos de exportação.

Plataformas de inteligência contra ameaças Serviços de inteligência

- Uma plataforma de inteligência contra ameaças (TIP) centraliza a coleta de dados de ameaças de várias fontes e formatos de dados.
- **Tipos de dados de inteligência de ameaças:**
 - Indicadores de compromisso (IOC)
 - Ferramentas Técnicas e Procedimentos (TTP)
 - Informações de reputação sobre destinos ou domínios da Internet
- As organizações podem contribuir com informações sobre ameaças compartilhando seus dados de intrusão pela Internet, geralmente por meio de automação.
- Honeypots são redes simuladas ou servidores projetados para atrair atacantes. As informações relacionadas ao ataque coletadas de honeypots podem ser compartilhadas com assinantes da plataforma de inteligência contra ameaças.

20.3 Resumo da inteligência de ameaças

O que aprendi neste módulo?

- Muitas organizações, como SANS, Mitre, FIRST, SecurityNewsWire, (ISC) 2 e CIS, fornecem inteligência de rede.
- Os profissionais de segurança de rede devem manter-se a par das ameaças mais recentes e continuar a atualizar as habilidades.
- Os serviços de inteligência contra ameaças permitem a troca de informações sobre ameaças, como vulnerabilidades, indicadores de comprometimento (COI) e técnicas de mitigação.
- Cisco Talos é uma das maiores equipes de inteligência de ameaças comerciais do mundo.
- FireEye é outra empresa de segurança que oferece serviços para ajudar as empresas a proteger suas redes. Ele usa uma abordagem em três vertentes que combina inteligência de segurança, experiência em segurança e tecnologia.

O que aprendi neste módulo? (Continuação)

- O Departamento de Segurança Interna dos EUA (DHS) oferece um serviço gratuito chamado Automated Indicator Sharing (AIS).
- O AIS permite a troca em tempo real de indicadores de ameaças cibernéticas entre o Governo Federal dos EUA e o setor privado.
- O governo dos Estados Unidos patrocinou a MITRE Corporation para criar e manter um catálogo de ameaças de segurança conhecidas chamadas Common Vulnerabilities and Exposure (CVE).
- Três padrões comuns de compartilhamento de informações sobre ameaças incluem STIX (Structured Threat Information Expression), Trusted Automated Exchange of Indicator Information (TAXII) e CyBox.

