

THE DEVELOPER'S CONFERENCE

Trilha: DevSecOps

André Barreto

Hacker Ético

Mente criminosa



THE
DEVELOPER'S
CONFERENCE

Olhe para suas aplicações com os olhos de um
"criminoso"

Muito além de uma "Análise de Vulnerabilidades"

Propósito da palestra



THE
DEVELOPER'S
CONFERENCE

Mostrar que a análise humana é capaz de chegar em pontos onde processos automatizados não conseguem, mas...

Quanto mais você desenvolver uma “mente criminosa”, mais eficiente você será nessa tarefa.

Ordem de complexidade de implementação:

- Forma como a aplicação é disponibilizada
- Código
- Regras de negócio

Convido vocês a abrirem a mente, vamos pensar “fora da caixa”!

Sobre a palestra



Muito além de uma Análise de Vulnerabilidades
“não são abordadas em consultorias e análises de segurança tradicionais”

Ferramentas de análise de vulnerabilidade basicamente:

- Automatizam tarefas repetitivas;
- Analisam vulnerabilidades conhecidas mundialmente em softwares de mercado;

Mas e a sua aplicação desenvolvida para atender às suas necessidades específicas?

Analisaremos pontos que passariam em testes de vulnerabilidades e consultorias de segurança tradicionais

Scanners de rede



THE
DEVELOPER'S
CONFERENCE

Fazem varreduras na internet buscando serviços ativos que possam ser explorados e dar algum tipo de vantagem ao atacante.

Exposição de Serviços (Portas)

80/TCP (HTTP) - 100.675.471 (1°)

443/TCP (HTTPS) - 84.883.57 (2°)

22/TCP (SSH) - 19.167.244 (3°)

25/TCP (SMTP) - 5.370.241 (4°)

3389/TCP (RDP) - 3.778.311 (5°)

23/TCP (Telnet) - 2.729.175 (6°)

Segurança



THE
DEVELOPER'S
CONFERENCE



Tipos de ataque

(dentre tantas formas possíveis de qualificar)



THE
DEVELOPER'S
CONFERENCE

Tipo de Alvo:

- Aleatórios
- Direcionados

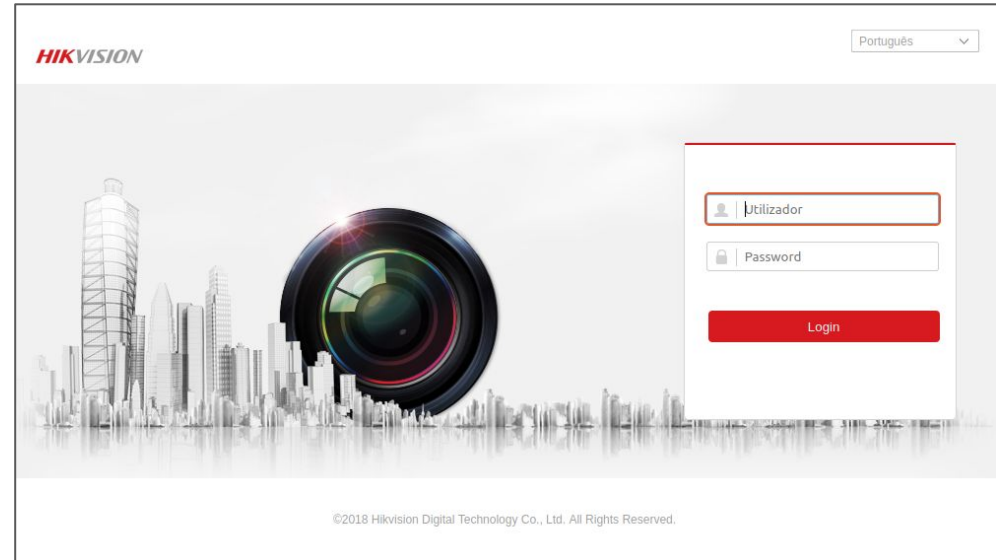
Scanner de HTTPS - Porque?



THE
DEVELOPER'S
CONFERENCE



The Intelbras login interface is displayed on a dark background with a subtle geometric pattern. At the top, the Intelbras logo is shown, including the text 'MULTI HD' and 'MHDx 1108'. Below the logo, there are three input fields: 'Usuário' (User) with a person icon, 'Senha' (Password) with a lock icon and a toggle eye icon, and 'TCP' with a dropdown arrow. A large green 'Entrar' (Enter) button is positioned below these fields. At the bottom, there is a link that says 'Esqueceu a senha?' (Forgot the password?).



The Hikvision login interface is shown on a light background. At the top left is the 'HIKVISION' logo, and at the top right is a language dropdown menu set to 'Português'. The main visual is a city skyline with a large camera lens in the foreground. On the right side, there is a white login box containing two input fields: 'Utilizador' (User) with a person icon and 'Password' with a lock icon. Below these fields is a red 'Login' button. At the bottom of the page, there is a copyright notice: '©2018 Hikvision Digital Technology Co., Ltd. All Rights Reserved.'

Scanner de HTTPS - Porque?



THE
DEVELOPER'S
CONFERENCE

SONICWALL™
Network Security Appliance

Username

Password

LOG IN

pfSense

Login to pfSense

SIGN IN

Username

Password

SIGN IN

pfSense is developed and maintained by Netgate. © ESF 2004 - 2022 View license.

RouterOS v6.48.6

You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator.

WebFig Login:

Login: Login

Password:

Winbox Telnet Graphs License Help

© mikrotik

Cisco Switch

Application: Switch Management

Username:

Password:

Language: English

Log In

© 2011-2018 Cisco Systems, Inc. All Rights Reserved.
Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Scanner de HTTPS - Porque?

Ainda pode piorar?



THE
DEVELOPER'S
CONFERENCE

vmware®

User name

Password

Log in

vmware® ESXi™

vmware®

Nome do usuário:

Senha:

☐ Usar autenticação de sessão do Windows

Logon

VMware® vCenter™ Single Sign-On

Scanner de HTTPS - Porque?

Chegamos ao fundo do poço?



THE
DEVELOPER'S
CONFERENCE

VMware ESXi 5.1
Welcome

Getting Started

If you need to access this host remotely, use the following program to install vSphere Client software. After running the installer, start the client and log in to this host.

- [Download vSphere Client](#)

To streamline your IT operations with vSphere, use the following program to install vCenter. vCenter will help you consolidate and optimize workload distribution across ESX hosts, reduce new system deployment time from weeks to seconds, monitor your virtual computing environment around the clock, avoid service disruptions due to planned hardware maintenance or unexpected failure, centralize access control, and automate system administration tasks.

- [Download VMware vCenter](#)

If you need more help, please refer to our documentation library:

- [vSphere ESXi 5.1](#)

For Administrators

vSphere Remote Command Line

The Remote Command Line allows you to use command line tools to manage vSphere from a client machine. These tools can be used in shell scripts to automate day-to-day operations.

- [Download the Virtual Appliance](#)
- [Download the Windows Installer \(exe\)](#)
- [Download the Linux Installer \(tar.gz\)](#)

Web-Based Datastore Browser

Use your web browser to find and download files (for example, virtual machine and virtual disk files).

- [Browse datastores in this host's inventory](#)

For Developers

vSphere Web Services SDK

Learn about our latest SDKs, Toolkits, and APIs for managing VMware ESX, ESXi, and VMware vCenter. Get sample code, reference documentation, participate in our Forum Discussions, and view our latest Sessions and Webinars.

- [Learn more about the Web Services SDK](#)
- [Browse objects managed by this host](#)

Copyright © 1998-2013 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries and may also be protected by international treaties. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware products may contain individual open source components, each of which has its own copyright and applicable license conditions. Please visit <http://www.vmware.com/go/opensource> for more information.

Scanner de HTTPS - Porque?

DevSec(?)Ops



THE
DEVELOPER'S
CONFERENCE

```
JSON  Raw Data  Headers
Save  Copy  Collapse All  Expand All  Filter JSON

kind:      "Status"
apiVersion: "v1"
metadata:  {}
status:    "Failure"
▼ message: "forbidden: User \"system:anonymous\" cannot get path \"/\""
reason:    "Forbidden"
details:   {}
code:      403
```

Certificate Viewer: kube-apiserver

General Details

Issued To

Common Name (CN)	kube-apiserver
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

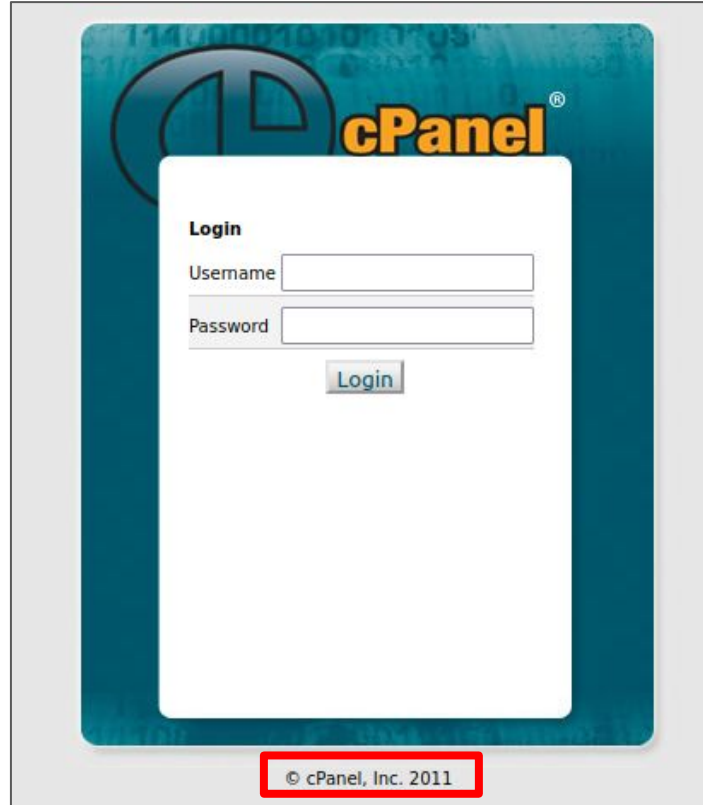
Issued By

Common Name (CN)	kubernetes
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Scanner de HTTPS - Porque?



THE
DEVELOPER'S
CONFERENCE



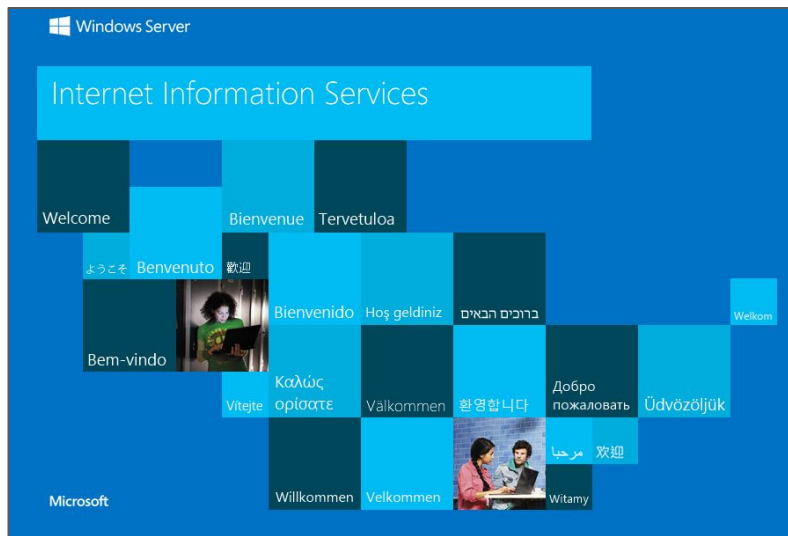
The image shows a screenshot of the cPanel login page. It features a blue background with a large, stylized 'c' logo and the word 'cPanel' in orange. In the center, there is a white login box with the following elements:

- Login** header
- Username** label followed by a text input field.
- Password** label followed by a text input field.
- A **Login** button below the password field.

At the bottom of the page, there is a red rectangular box containing the copyright notice: © cPanel, Inc. 2011.

Scanner de HTTPS - Porque?

Vamos deixar o fundo do poço?



- Sistema fora do site default
- Apresenta tela padrão do servidor web



THE
DEVELOPER'S
CONFERENCE

Apache 2 Test Page powered by CentOS

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page it means that the Apache HTTP server installed at this site is working properly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

If you are the website administrator:

You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

You are free to use the images below on Apache and CentOS Linux powered HTTP servers. Thanks for using Apache and CentOS!



About CentOS:

The Community ENTERprise Operating System (CentOS) Linux is a community-supported enterprise distribution derived from sources freely provided to the public by Red Hat. As such, CentOS Linux aims to be functionally compatible with Red Hat Enterprise Linux. The CentOS Project is the organization that builds CentOS. We mainly change packages to remove upstream vendor branding and artwork.

Scanner de HTTPS - Porque?

Vamos dar mais uma entradinha no poço?



THE
DEVELOPER'S
CONFERENCE



Scanner de HTTPS - Porque?



THE
DEVELOPER'S
CONFERENCE

Not Found

The requested URL / was not found on this server.

Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.26 with Suhosin-Patch mod_ruby/1.2.6
Ruby/1.8.6(2007-09-24) mod_ssl/2.2.8 OpenSSL/0.9.8g mod_jk/1.2.25 Server at
[REDACTED] Port 443

Forbidden

You don't have permission to access / on this server.

Apache/1.3.41 Server at [REDACTED] Port 443


Qual a chance de
vulnerabilidade?

Vamos olhar o certificado?



THE
DEVELOPER'S
CONFERENCE

Certificate



Subject Name

Common Name [REDACTED].br

Issuer Name

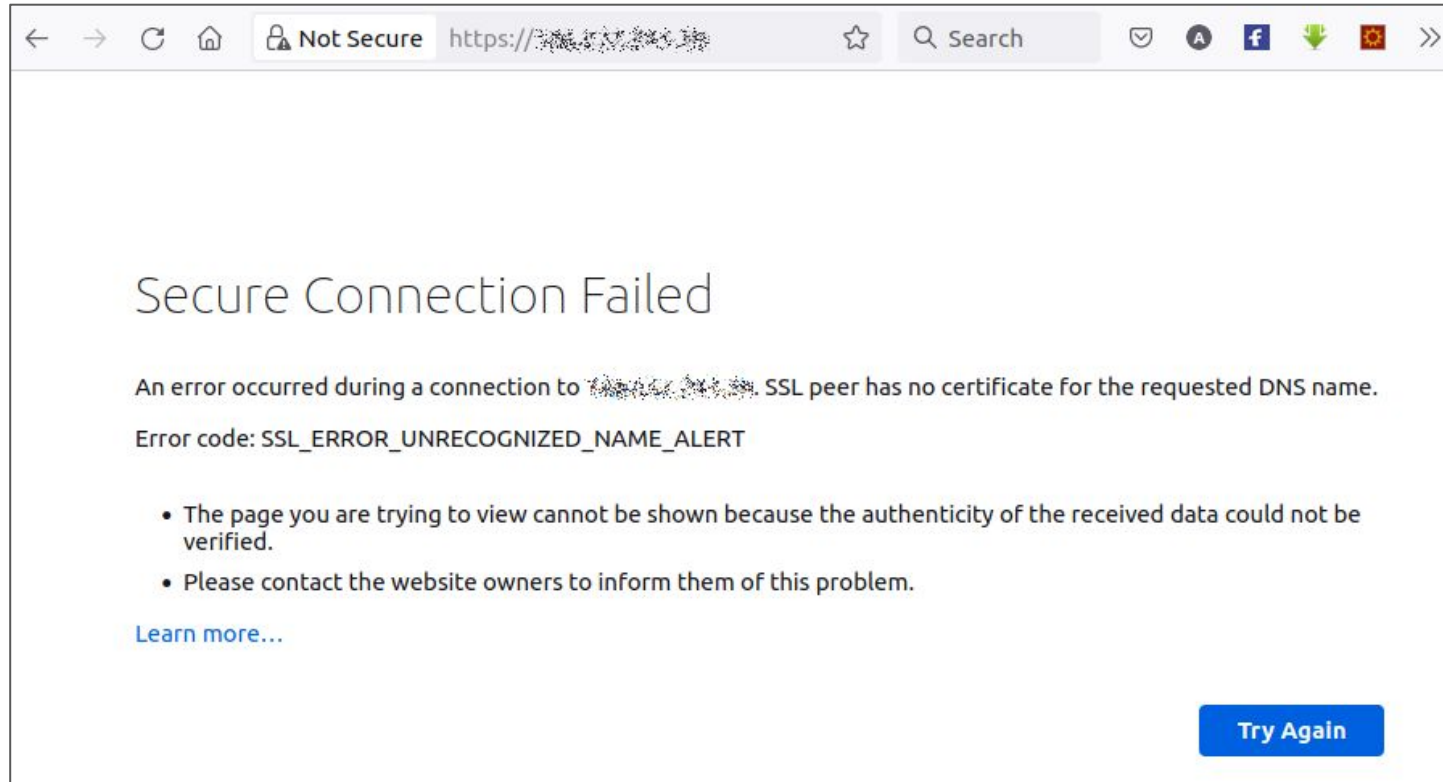
Common Name [REDACTED].br

```
PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: IIS Windows Server
|_ ssl-cert: Subject: commonName=[REDACTED].br
| Not valid before: [REDACTED]
|_ Not valid after: [REDACTED]
|_ ssl-date: 2022-05-10T02:42:01+00:00; 0s from scanner time.
|_ tls-alpn:
|_ http/1.1
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Sem certificado no site default (apenas FQDN)



THE
DEVELOPER'S
CONFERENCE



Sem certificado no site default



THE
DEVELOPER'S
CONFERENCE



Negação de serviço (DoS)



- Estabeleça limite de conexões e de requisições (throttling);
- Se possível, faça isso através de um Proxy Reverso, API Gateway ou API Manager;
- Cuidado com o tempo de resposta nas requisições de autenticação com credenciais inválidas.

Código



THE
DEVELOPER'S
CONFERENCE

- Aumentar o tempo de retorno para erros de autenticação (força bruta);
- Não apresentar comportamento diferente quando apenas a senha estiver errada e quando o usuário não existir (enumeração de usuários);
- Se existir uma opção de “Esqueci minha senha”, não apresentar comportamento diferente quando o usuário não existir (enumeração de usuários);
- Ajustar códigos de retorno HTTP.
Isso pode ser trabalhado junto ao Blue Team em sistemas de análise de acessos:
 - 400 - Identifique requisições com erros estruturais (bad request);
 - 401 - Se possível, usar nas falhas de autenticação;
 - 403 - Se possível, usar quando se tenta acessar um recurso ao qual não se tem permissão;
 - 404 - Se possível não usar dentro da aplicação, avaliar o uso do 204. Blue Team pode usar o 404 para localizar tentativas de enumeração de arquivos e diretórios.
- Se retornar 200 na falha de autenticação, então possuir diversas mensagens de erro de login, com diferentes frequências, tendo algumas com percentual bem baixo (enumeração de usuários).

Requisitos vs Vulnerabilidades



THE
DEVELOPER'S
CONFERENCE

Se “debug” é o processo de identificar e remover “bugs”, então programar é o processo de inseri-los.

- Requisitos funcionais
- Requisitos não funcionais

- Vulnerabilidades funcionais
- Vulnerabilidades não funcionais

O óbvio precisa ser dito.

O “óbvio” nem sempre é observado e muito menos seguido.

Vulnerabilidades não funcionais



THE
DEVELOPER'S
CONFERENCE

2011 - Sony (37k)
2012 - Yahoo (500k)
2020 - Catho (1,2m)
2021 - Liker (465k)

- Não armazenar a senha de forma aberta;
- Não trafegar a senha de forma aberta;
- Aumentar o tempo de retorno para erros de autenticação;
- Definir restrições de palavras de fácil associação e sequências numéricas nas senhas (tdc@123);
- Definir restrições de certas datas nas senhas (tdc@2022);
- Restringir o uso do “username” na senha (andre@2022);
- Aplicar um algoritmo de similaridade com a senha(s) anterior(es) (tdc@2021 -> tdc@2022).

Vulnerabilidades não funcionais



THE
DEVELOPER'S
CONFERENCE

- Não dar dicas se “o usuário não existe” ou “a senha está incorreta” (enumeração de usuários);
- Cuidado com mensagens de aviso para o usuário durante a autenticação (“usuário bloqueado”, “senha expirada”, etc).
Se for necessário informar algo, faça somente após validação com sucesso das credenciais;
- Avaliar a possibilidade de associar um “token ao usuário” ao invés de um “usuário ao token”.
(Reduz sessão "esquecidas" e, principalmente, evita compartilhamento de credenciais);
- Avaliar o famoso bloqueio do usuário após X tentativas de login incorretas (DoS).

Vulnerabilidades funcionais (regras de negócio)



THE
DEVELOPER'S
CONFERENCE

- Não enviar para o front-end informações que o usuário não tem permissão para ver. Não basta esconder a informação no front;
- Valide o acesso às funcionalidades no backend. Não ter a opção no “menu do front” não basta;
- Valide no backend se o usuário está consultando informações que ele deveria ter acesso. Confiar na identificação do usuário enviado pelo front não basta. O mesmo se aplica a outras identificações;
- Valide no backend se o usuário está usando recursos que pertençam a ele (cupons, moedas);
- Cuidado com “caminhos secundários” que deem acesso às informações sem as mesmas validações feitas nos “caminhos oficiais”;
- Cuidado com exposições “desnecessárias” da documentação completa dos recursos das suas APIs;
- Você **realmente** precisa saber a senha do usuário?
Avaliar a necessidade de armazenar e até de transmitir via rede a senha real do usuário, ainda que por meio criptografado.

Modelagem de Ameaças



THE
DEVELOPER'S
CONFERENCE

Representação estruturada de tudo que possa afetar a segurança de um aplicativo (ameaça).
É uma visão do aplicativo e de seu ambiente por meio de lentes de segurança.

- Identificar, organizar e analisar qualquer tipo de ameaça a um sistema;
- Tomada de decisões sobre a prevenção ou mitigação dos riscos de segurança;
- Priorizar as melhorias de segurança.

* Ameaça é um evento indesejável potencial ou real que pode ser malicioso (como um ataque DoS) ou incidental (falha de um dispositivo de armazenamento).

Matriz de risco

(Probabilidade x Impacto)



THE
DEVELOPER'S
CONFERENCE

Classificação	Valor
Baixo	1
Médio	2
Alto	3

Tabela 1: Escala de classificação de probabilidade e impacto.

1 - Muito Baixo
2 - Baixo
3 e 4 - Médio
6 - Alto (Urgente)
9 - Muito Alto (Inaceitável)

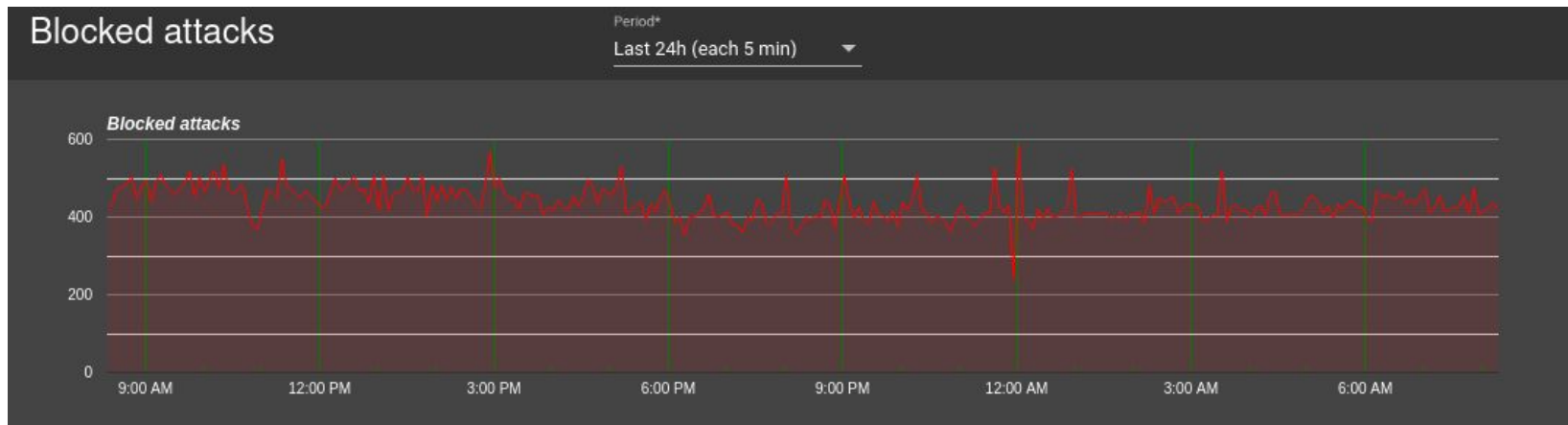
		PROBABILIDADE X IMPACTO		
PROBABILIDADE	Alto (3)	3	6	9
	Médio (2)	2	4	6
	Baixo (1)	1	2	3
		Baixo (1)	Médio (2)	Alto (3)
		IMPACTO		

Tabela 2: Matriz de probabilidade e impacto.

Recados finais



O cibercrime não dorme



Recados finais



THE
DEVELOPER'S
CONFERENCE



Mensagem final



“Se quisermos sobreviver nessa nova era de ataques cibernéticos, precisamos aprender a lidar com as novas “trancas” e “cadeados” que a evolução tecnologia nos exige.”

André Barreto

Mente criminosa: Olhe para suas aplicações com os olhos de um "criminoso"
Muito além de uma "Análise de Vulnerabilidades"

