

# Café com Network

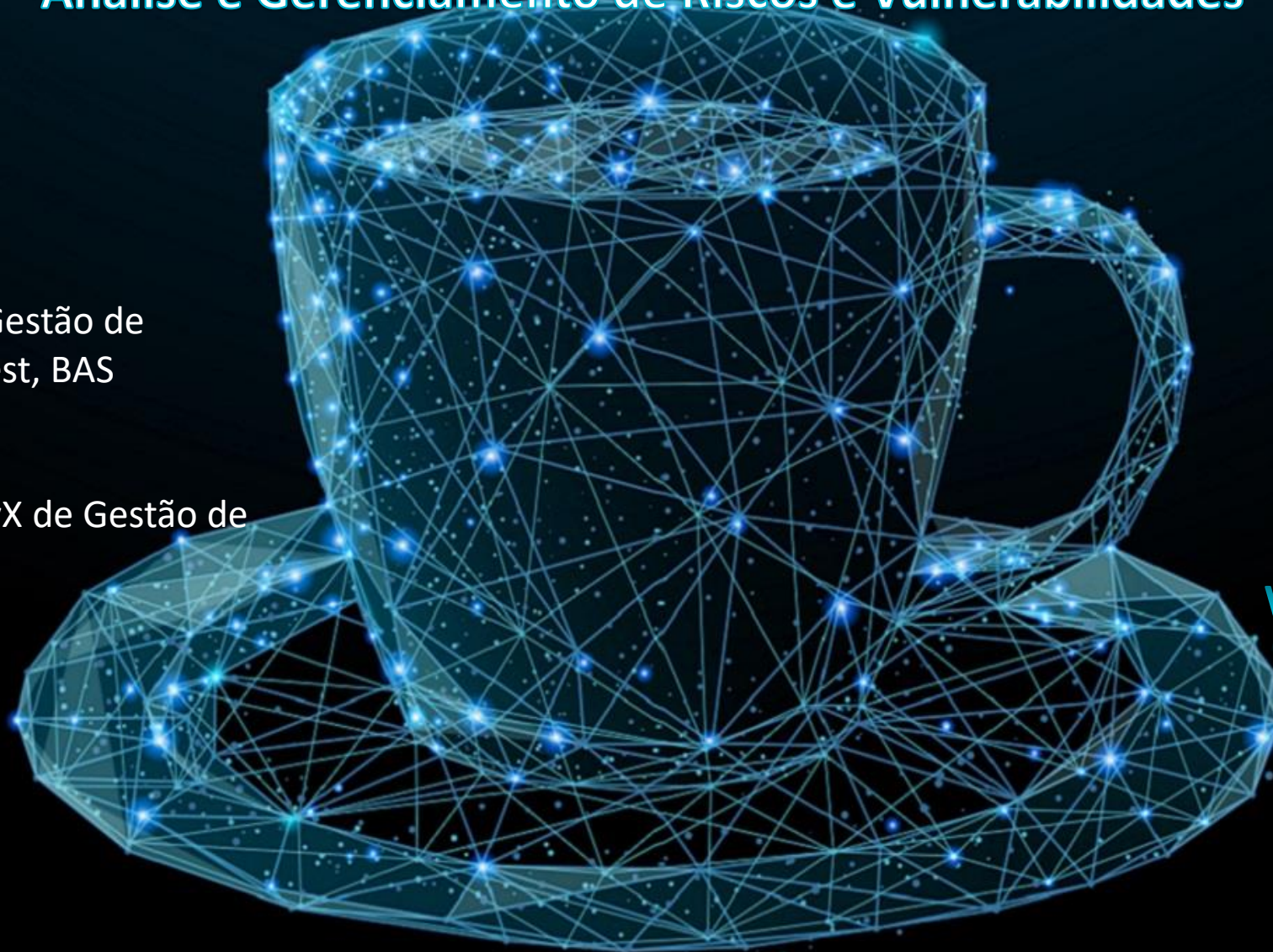
Análise e Gerenciamento de Riscos e Vulnerabilidades

1 – Boas Vindas  
(Alex De Boni)

2 - Desmistificar Scan/Gestão de  
Vulnerabilidades, Pentest, BAS  
(Andrey Souza)

3 – Apresentação SupryX de Gestão de  
vulnerabilidades  
(Alex De Boni)

4 - ReiteLog - Case  
(Angelo Sironi)



BEM VINDOS  
WELCOME  
BIENVENIDOS  
BENVENUTI  
WILLKOMMEN

Data: 15/03/20/2023



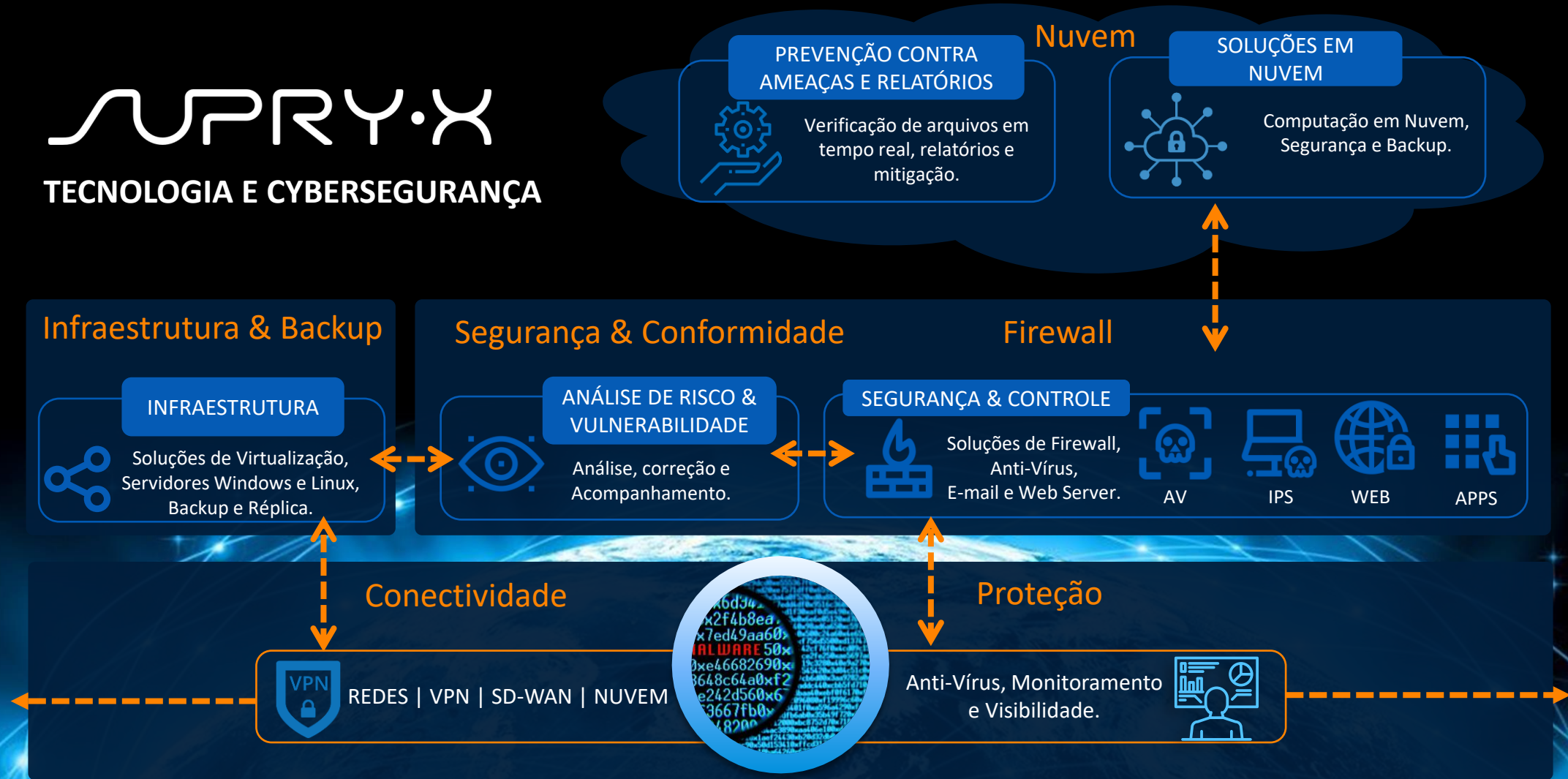
# Análise e Gerenciamento de Riscos e Vulnerabilidades

Cybersegurança não é um problema a ser solucionado, mas sim uma condição a ser gerenciada!

Hacker in a box

# UPRY·X

## TECNOLOGIA E CYBERSEGURANÇA





## Contexto Atual – Incidentes de segurança com repercussão na mídia\*







# **5 passos para evitar vazamento de dados**

**1. CONSCIENTIZAÇÃO E CULTURA**

**2. IDENTIFIQUE AS AMEAÇAS E CONHEÇA SEUS DADOS**

**3. PROTEJA SEUS APPS E SUAS APIS**

**4. REALIZE TESTES DE INVASÃO**

**5. MANTENHA SEU PARQUE TECNOLÓGICO ATUALIZADO**



# Em qual geração de proteção a sua empresa está?

1983 a 2003 entre 40 a 20 anos atrás...	2004 a 2009 Entre 18 a 13 anos atrás...	2010 a 2015 Entre 12 a 7 anos atrás....	2016 a 2023 entre 6 anos atrás e atualidade
<ul style="list-style-type: none"><li>• Anti-Malware por assinatura</li><li>• Anti-Malware em tempo real</li><li>• Firewall UTM</li><li>• Anti-Phishing</li></ul>	<ul style="list-style-type: none"><li>• Anti-Malware realtime com base em reputação</li><li>• Anti-Rootkit</li><li>• Firewall no End-point com HIPS (Prevenção de Intrusão no Endpoint).</li><li>• Gestão inteligente de Firewall</li><li>• Gestão de Vulnerabilidade</li><li>• Atualização de Software</li></ul>	<ul style="list-style-type: none"><li>• Mecanismos de proteção de conexão</li><li>• Prevenção automática de Exploits</li><li>• Controle de Dispositivos</li><li>• Detecção e Reposta (EDR)</li></ul>	<ul style="list-style-type: none"><li>• Proteção de Dados Pessoais: LGPD</li><li>• Identificação, Proteção, Detecção, Resposta e Restauração. (NIST)</li><li>• CIS Controls</li></ul>





# CIS CONTROLS v8 e NIST

<b>CONTROL 01</b> Inventory and Control of Enterprise Assets 5 Safeguards 161 2/5 162 4/5 163 5/5	<b>CONTROL 02</b> Inventory and Control of Software Assets 7 Safeguards 161 3/7 162 6/7 163 7/7	<b>CONTROL 03</b> Data Protection 14 Safeguards 161 6/14 162 12/14 163 14/14
<b>CONTROL 04</b> Secure Configuration of Enterprise Assets and Software 12 Safeguards 161 7/12 162 11/12 163 12/12	<b>CONTROL 05</b> Account Management 6 Safeguards 161 4/6 162 6/6 163 6/6	<b>CONTROL 06</b> Access Control Management 8 Safeguards 161 5/8 162 7/8 163 8/8
<b>CONTROL 07</b> Continuous Vulnerability Management 7 Safeguards 161 4/7 162 7/7 163 7/7	<b>CONTROL 08</b> Audit Log Management 12 Safeguards 161 3/12 162 11/12 163 12/12	<b>CONTROL 09</b> Email and Web Browser Protections 7 Safeguards 161 2/7 162 6/7 163 7/7
<b>CONTROL 10</b> Malware Defenses 7 Safeguards 161 3/7 162 7/7 163 7/7	<b>CONTROL 11</b> Data Recovery 5 Safeguards 161 4/5 162 5/5 163 5/5	<b>CONTROL 12</b> Network Infrastructure Management 8 Safeguards 161 1/8 162 7/8 163 8/8
<b>CONTROL 13</b> Network Monitoring and Defense 11 Safeguards 161 0/11 162 6/11 163 11/11	<b>CONTROL 14</b> Security Awareness and Skills Training 9 Safeguards 161 8/9 162 9/9 163 9/9	<b>CONTROL 15</b> Service Provider Management 7 Safeguards 161 1/7 162 4/7 163 7/7
<b>CONTROL 16</b> Applications Software Security 14 Safeguards 161 0/14 162 11/14 163 14/14	<b>CONTROL 17</b> Incident Response Management 9 Safeguards 161 3/9 162 8/9 163 9/9	<b>CONTROL 18</b> Penetration Testing 5 Safeguards 161 0/5 162 3/5 163 5/5

## NIST Cybersecurity Framework 1.1

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management Business Environment Governance Risk Assessment Risk Management Strategy Supply Chain Risk Management	Identity Management and Access Control Awareness and Training Data Security Information Protection Processes Maintenance Protective Technology	Anomalies and Events Security Continuous Monitoring Detection Processes	Response Planning Communications Analysis Mitigation Improvements	Recovery Planning Improvements Communications

<https://www.cisecurity.org/partner/outpost-24>

Outpost24



# Relatórios de resultados detalhados

GERENCIAMENTO CONTÍNUO DE CYBERSEGURANÇA

# CYBER SECURITY TECHNOLOGY

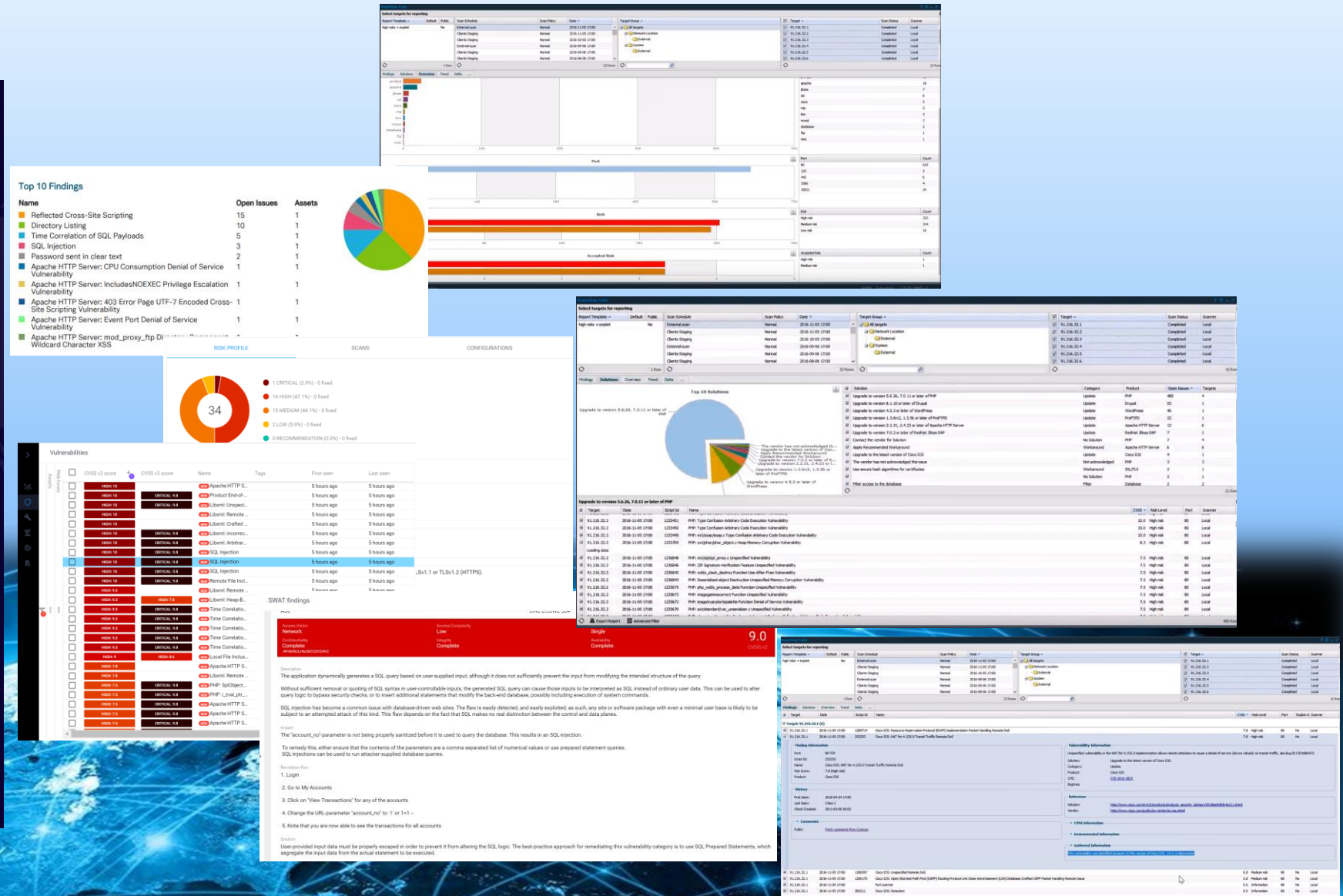
## SUPRYX



**CLIENTE**

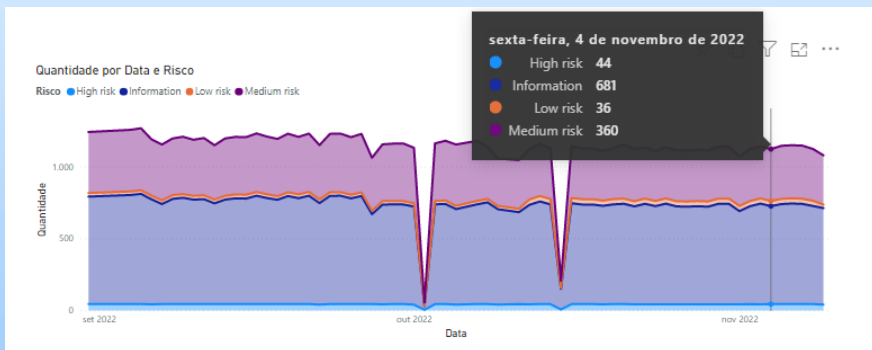
Cybersegurança não é um problema a ser solucionado, mas sim uma condição a ser gerenciada!

supryx.com.br

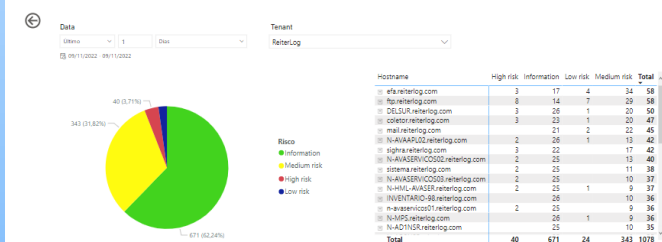




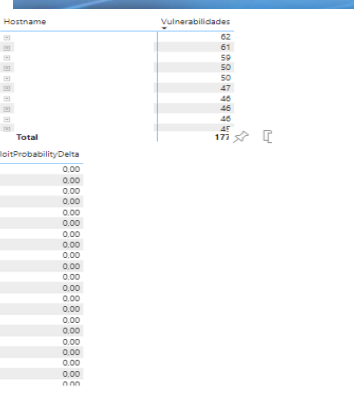
## Analise em PowerBI – Maior Visibilidade



HOST	VUL	AÇÃO
Servidor J	38	Remover autenticação tls 1.0 e 1.1 no servidor de emails



HOST	VUL.	AÇÃO
Servidor A	8	Isolamento do Serviço para IPS de Origem
Servidor B	3	Acesso somente de alguns IP's – Verificar para trocar esta plataforma
Servidor C	4	Migrado para Windows Server2019.
Servidor D	3	Atualizado Windows
Servidor E	3	Migrado para outro produto com suporte
Servidor F	5	Corrigidos os graves – Trabalhando no SSL





# Obrigado !



Contato: Alex De Boni  
Email: [alex@supryx.com.br](mailto:alex@supryx.com.br)  
Site: [supryx.com.br](http://supryx.com.br)