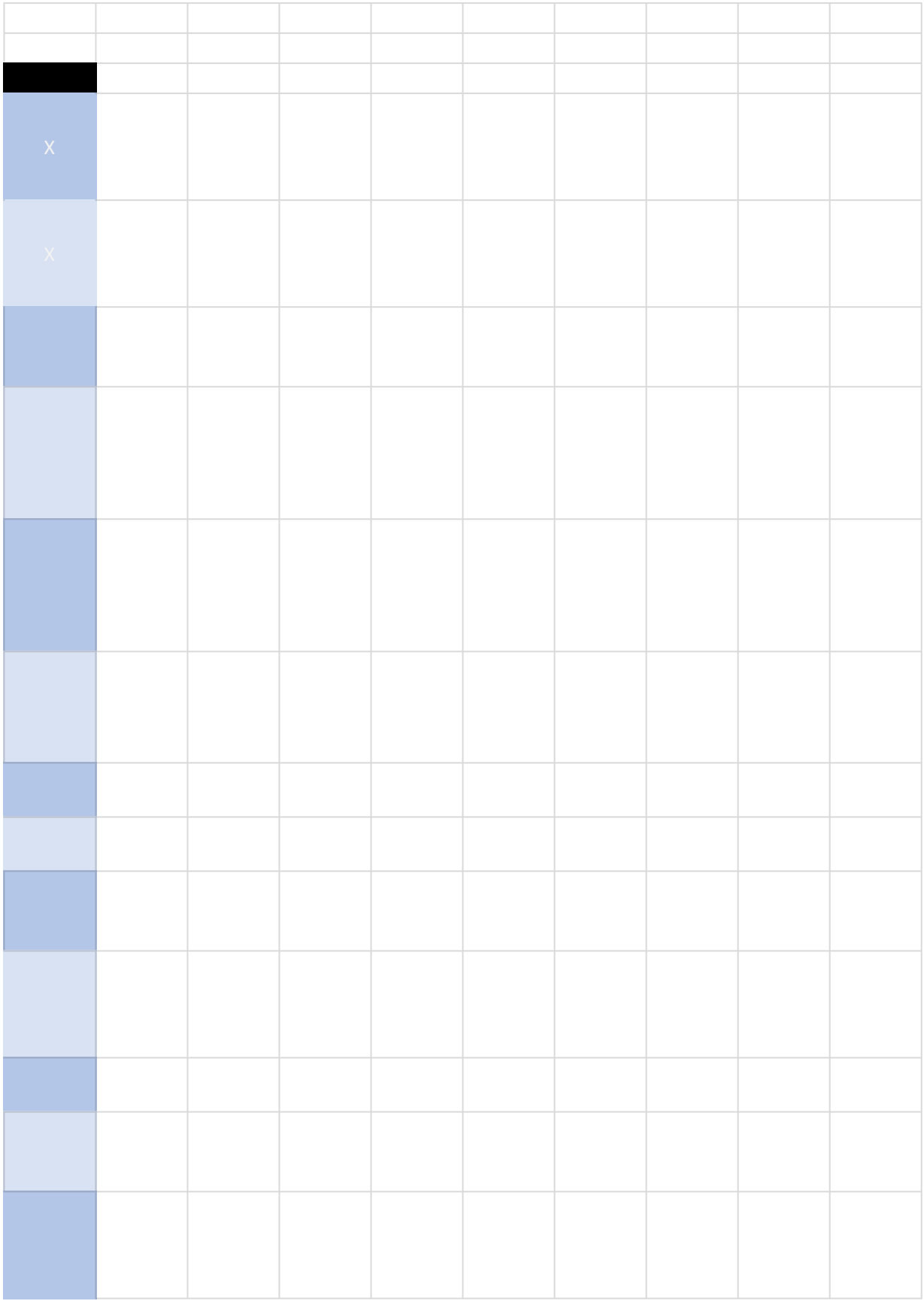
One Digital

Linux/kernel Linux	**CVE-2022-24959**	Problema No Kernel do Linux, com vazamento de memoria em yam_siocdevprivate em drivers/net/hamradio/yam.c.	ON
Nvidia	**CVE-2022-22821**	Vulnerabilidade no ASR WebApp, levando exclusão de qualquer diretorio quando privilegios estiverem disponiveis	ON
Interno		Falta de uma politica de senha	ON
Web Application Firewall (WAF)	CVE-2018-15904	Regras configuradas para bloquear ataques de injeção de SQL mal manipulado	ON
Interno		Inserção de midias com possiveis malweres	ON
Interno		Falta de um servidor de backup fora do parque de servidores	
Interno		Softwares de comuniucação não homologados	ON
Externa		Falta de politica de segurança externa	ON
apache	CVE-2022-23307	Identificou um problema de desserialização que estava presente no Apache Chainsaw	ON
Inscrição	CVE-2019-15898	O Nagios Log Server antes de 2.0.8 permite o Reflected XSS através do nome de usuário na página de login.	ON
Interno		Falta de manutenção dos servidores e computadores	ON
IBM	CVE-2010-3187	Execução de codiggos arbitrarios por meeio de um comando NLST longo	ON
IBM	CVE-2006-1247	usuários locais sobrescrevam arquivos arbitrários por meio de um ataque de link simbólico em arquivos temporários.	ON

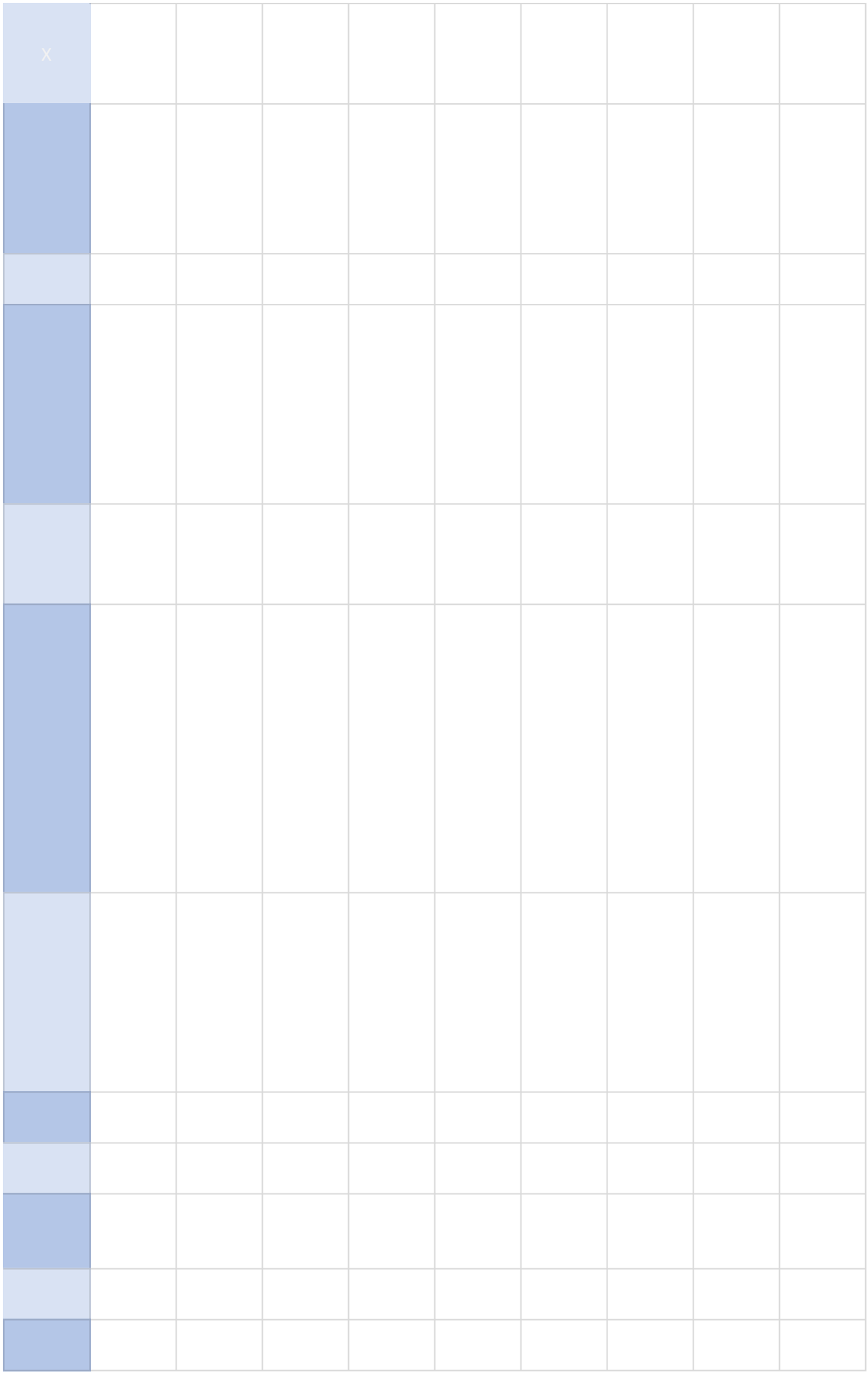
Nome: Leonardo Henrique dos Santos Ferreira da Silva

					CRITICA
Monitoramento de habitos e atualização do kernel	bufer overflow exploit	Hardware/software			
Atualização de versão 1.6.0	e de disponibilidade e integ	software			
conscientização com palestras e adiquirir um gerenciador de senhas	ues de dedução e brute for	Humana		X	
A atualização para a versão 2.7.1, 2.7.2-P12, 4.1.0-P11, 4.1.1-P8 ou 4.1.2-P4 elimina essa vulnerabilidade.	SQL INJECTION	software	X		
Proibição do uso de portas e sistemas que permitem a inserção de midias que podem afetar o CID da empresa.	Malware	Midia Digital		X	
Backup na nuvem	ataques de disponibilidade	Natural	X		
Software de comunicação homologados	Ransomware	software			X
VPN/PROXY	Malware	Humana			X
Atualização de versão corrigida 18/02/2022	DDOS	software	X		
Atualização de versao corrigida	Escala de privileios	Software			X
Manutenção cotidiana		Hardware			X
Atualização de versao corrigida	Buffer overflow	Software	X		
Atualização de versao corrigida	XSS	Software			X


X
X

Firewall	CVE-2016-5410	permite que usuários locais ignorem a autenticação e modifiquem as configurações do firewall	ON
WAF	CVE-2017-14705	permite a execução de comandos remotos não autenticados via porta TCP 3001 porque os metacaracteres do shell podem ser inseridos no parâmetro type para a função tailDateFile	ON
Interna		Falta de controle de acesso no parque de servidores	ON
Linux	**CVE-2021-44965**	Vulnerabilidade de passagem de diretório no diretório /admin/includes/* para PHPGURUKUL Employee Record Management System 1.2 O invasor pode recuperar e baixar informações confidenciais do servidor vulnerável.	ON
Interna		Falta de um plano de contingencia	ON
Interna		ma distribuição dos servidores	ON
Broadcom	CVE-2022-23992	Versões XCOM Data Transport para Windows, Linux e UNIX 11.6 contêm uma vulnerabilidade devido à validação de entrada insuficiente que pode permitir que invasores remotos executem comandos arbitrários com privilégios elevados.	ON
Microsoft	CVE-2022-23273	Vulnerabilidade de elevação de privilégio do Microsoft Dynamics	ON
ZEROF	CVE-2022-25323	ZEROF Web Server 2.0 permite /admin.back XSS.	ON
Windows	CVE-2022-22718	Vulnerabilidade de elevação de privilégio do spooler de impressão do Windows	ON
	CVE-2022-22712	Windows Hyper-V Denial of Service Vulnerability.	ON
Interna		Separação fisica entre redes visitantes corporativas	ON

Atualização de versao corrigida	Escala de privileios	software			
Atualização de versao corrigida	SQL INJECTION / XSS	software	X		
sistema de autenticação de acesso fisicco	Roubo de dados	física	X		
Mudar para CPE 2.2	Roubo de dados	Software			
Criação de uma área de segurança da informação focada em planos de contigencia e pentester	instavel e mais vulneravel	Física	X		
descentralizar a quantidade de servidores, distribuindo em diversas áreas	Desastres naturais	Natural		X	
Atualização de versao corrigida	Elevação de privilegios	Software	X		
Atualização de versao corrigida	Elevação de privilegios	Software	X		
Atualização de versao corrigida	XSS	Software			X
Atualização de versao corrigida	Elevação de privilegios	Software			X
Atualização de versao corrigida	DOS	SOFTWARE			X
Separação fisia entre ambas as redes	Elevação de privilegios	Física		X	


X

Windows	CVE-2022-21992	Vulnerabilidade de execução remota de código do Windows Mobile Device Management.	ON
Linux	CVE-2022-0286	Uma falha foi encontrada no kernel do Linux. Uma desreferência de ponteiro nulo em bond_ipsec_add_sa() pode levar à negação de serviço local.	ON
Linux	CVE-2004-0596	O Equalizer Load-balancer para interfaces de rede serial (eql.c) no kernel Linux 2.6.x até 2.6.7 permite que usuários locais causem uma negação de serviço por meio de um nome de dispositivo inexistente que aciona uma desreferência nula.	ON
Cisco	**CVE-2022-20647**	Várias vulnerabilidades na interface de gerenciamento baseada na Web do Cisco Security Manager podem permitir que um invasor remoto não autenticado conduza ataques de script entre sites contra um usuário da interface.	
Interno		Controle de acesso ao interior da empresa	ON

Atualização de versao corrigida	XSS	Software	X		
Atualização de path	DOS	Software			
Atualização de path	DDOS	Software			
Atualização de path	XSS	Software			X
Sistema de cracha para identificação	Roubo de dados	física	X		

X									
X									