Projeto: Construção de um Laboratório de Análise de Malware

SERPRO

Líder em soluções de TI para governo

AGENDA

- Sobre o Palestrante
- Sobre o SERPRO
- CSIRT SERPRO – Serviços do GRA
- Introdução
- Objetivos do Projeto
- Arquitetura do Projeto do Laboratório Análise de Malware
- Metodologia de Análise de Malware
- Processo do Laboratório de Análise de Malware
- Portal LAM
- Cuckoo
- RemNUX

AGENDA

- Ferramentas de Análise Estática
- Ferramentas de Análise Dinâmica
- Ferramentas de Análise de Memória
- Arquitetura do Laboratório de Análise de Malware
- Integração, Colaboração entre empresas Anti Malware
- Cartilha “ Construindo um laboratório de análise de Malware”
- Roadmap

Sobre o Palestrante

José Olympio R. R. De Castro
Gerente de Segurança da Informação
Bacharel em Ciência da Computação – IMB
MBA – Gestão de Segurança da Informação – NCE/UFRJ
Lato-sensu em Forense Computacional e Digital -IPOG

Projetos
Governança e Gestão de Segurança da Informação
Segurança em Infraestrutura e Conectividade.

Certificações
DRI - CBCP
ISACA – CISM / COBIT 5
BSI - Auditor Líder ISO 27001
Microsoft – MCSE+Security
Red Hat – RHCSA
LPI - LPIC 1

Sobre o SERPRO

- Líder no mercado de TI para o setor público, o nosso compromisso é com a segurança, qualidade e confiabilidade.
- Presença nacional, robusta infraestrutura tecnológica e ampla experiência com os grandes sistemas da Administração Pública Federal.
- Ampliando nossa atuação no mercado, oferecemos serviços especializados para os setores privado e público, baseados em informações de governo com oferta de produtos diversificados.

Sobre o SERPRO

MISSÃO:

- Conectar governo e sociedade com soluções digitais.

VISÃO:

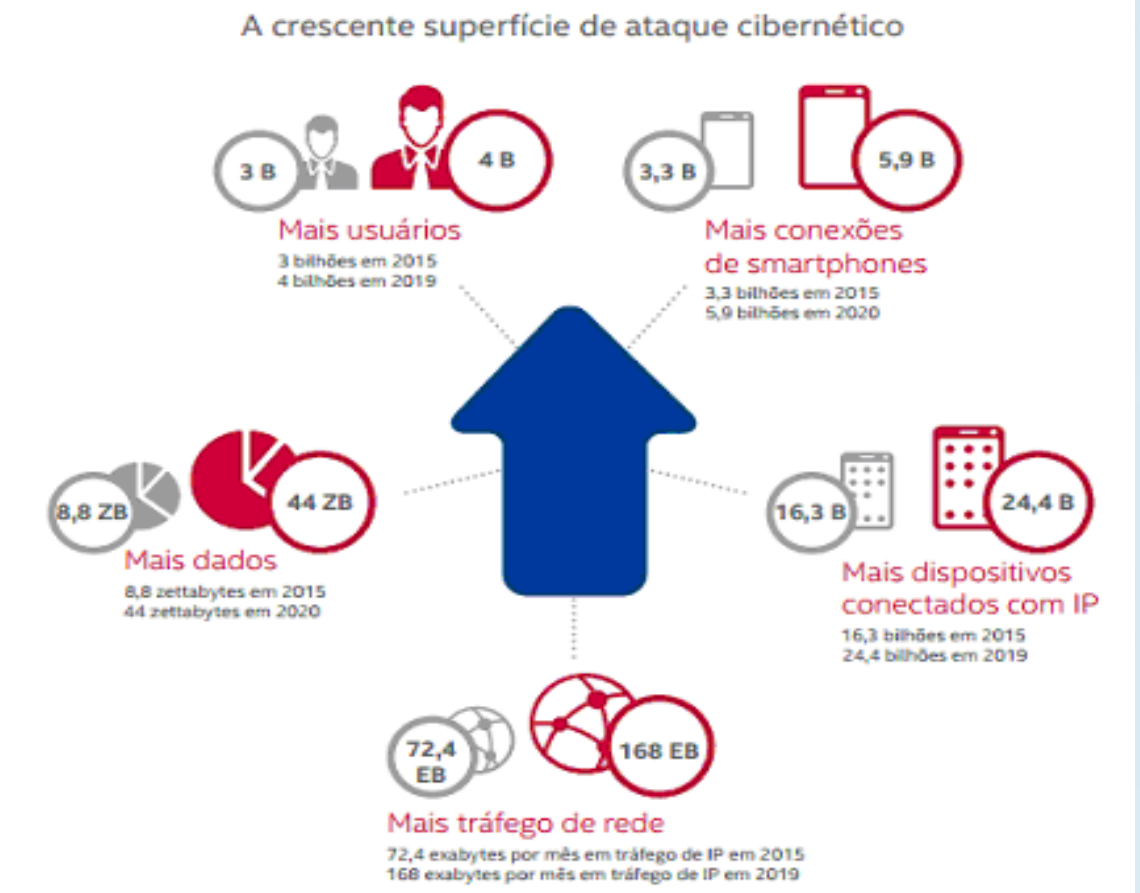
- Ser líder em soluções digitais para governo e sociedade.

VALORES:

- **Segurança:** soluções íntegras e confiáveis
- **Excelência:** conhecimento do negócio para entrega de soluções integradas de qualidade
- **Responsividade:** entregas com agilidade
- **Proatividade**: antecipação de soluções
- **Responsabilidade:** com as informações e soluções estratégicas para o Brasil
- **Orgulho:** uma empresa onde as pessoas praticam os princípios da ética e da integridade

INTRODUÇÃO

- Crescimento exponencial de dispositivos inteligentes e conectados com a Internet;
- Previsão de 200 bilhões até o ano 2020;
- Maior superfície de ataque implica em um aumento de cybercrimes;
- A Symantec, em seu relatório *Internet Security Threat Report – ISTR,* de 2016, registrou uma estimativa de 1,79 milhão de Malwares adicionados por dia em 2015, um aumento de 36% em relação a 2014.

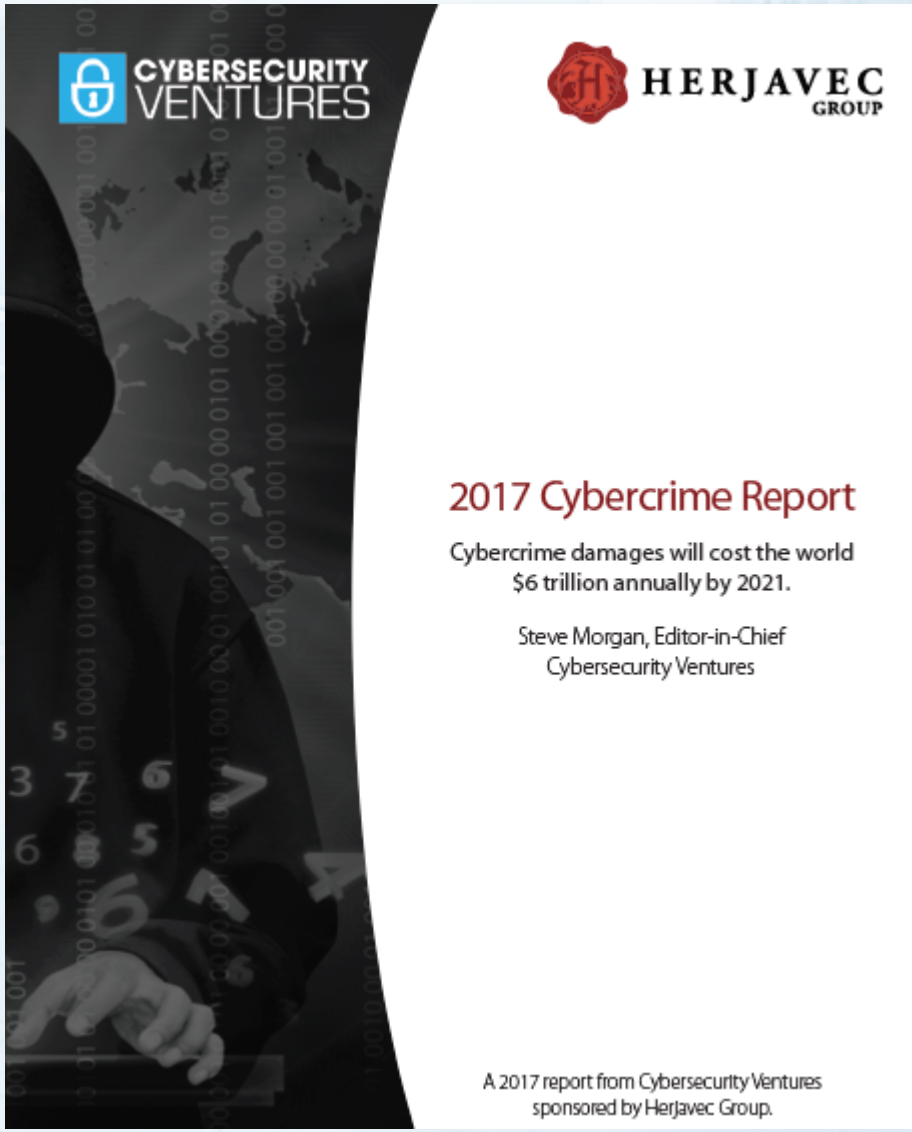


INTRODUÇÃO

Cibercrime vai custar US$ 6 trilhões em prejuízos anuais até 2021. **Hackerpocalypse: "A Cybercrime Revelation".**

- As perdas para o cibercrime não incluem apenas recursos financeiros roubados e informações, mas também destruição de sistemas e dados, bem como perda de produtividade, danos à reputação, entre outros. Uma das principais razões do cibercrime estar aumentando rapidamente tem a ver com o número crescente de empresas informatizadas e "coisas" ligadas à internet.

  Aumento exponencial de pessoas e dispositivos conectados à internet, a humanidade terá de proteger 50 vezes mais dados em 2020 do que hoje. O número de pontos que um hacker poderá atacar e penetrar deve crescer dez vezes ao longo dos próximos cinco anos.



INTRODUÇÃO

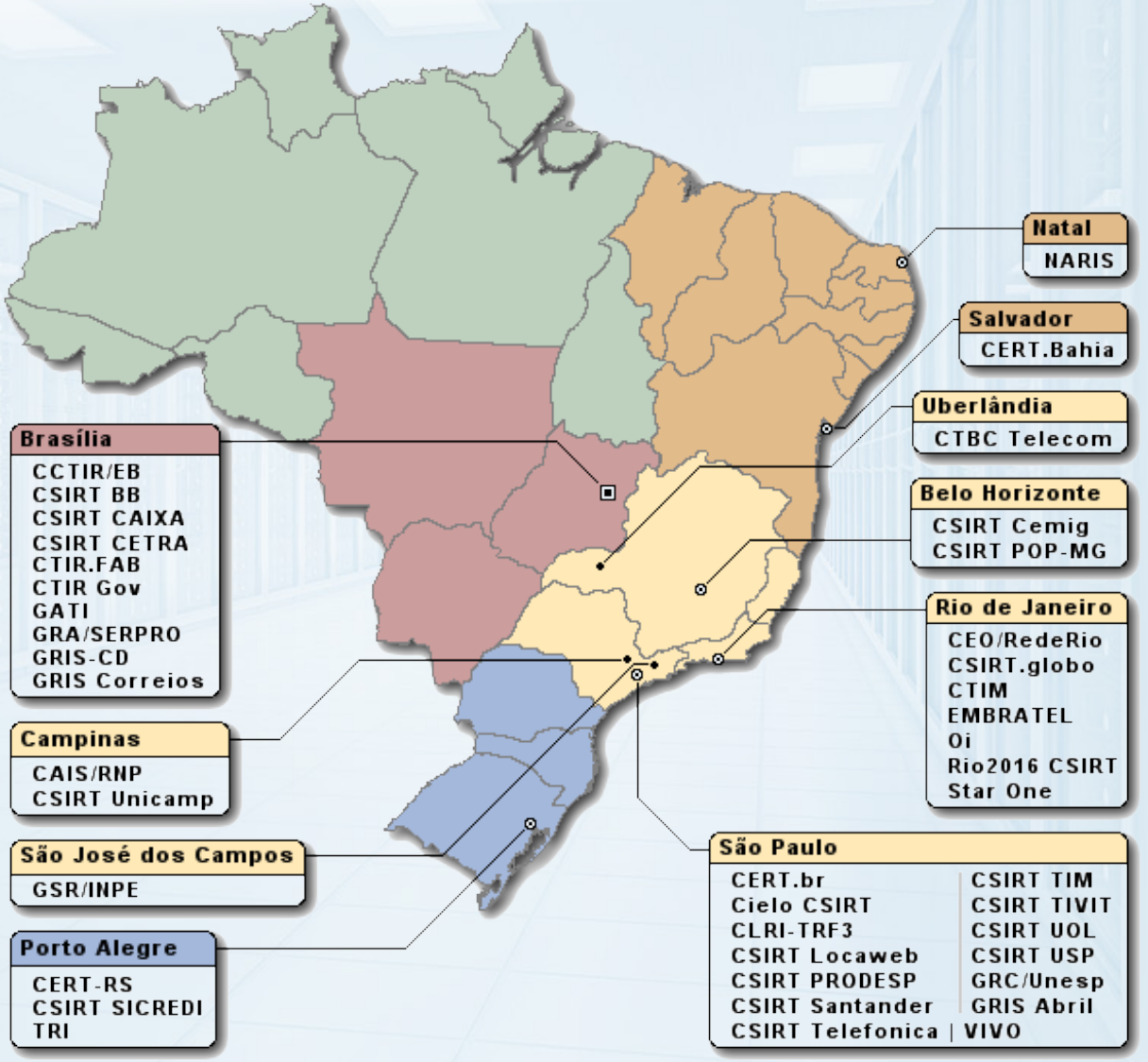
A McAfee foi adquirida em 2010 pela Intel. Desde então, os mecanismos de segurança desenvolvidos pela empresa passaram a fazer parte do sistema “Intel Security”.

“Eu não uso antivírus”, comentou o programador, sem papas nos dedos. “Acho que eles estão mortos e que são baseados em uma tecnologia velha, que não é mais relevante. Kits de hackers são lançados 10 vezes mais rápido [que atualizações para os antivírus]. Os antivírus não têm sentido”, admitiu.

Presença Nacional CSIRTS

- Nosso CSIRT está dividido em BSA, RJ, SP e RE. Chama-se Grupo de resposta a ataques -**GRA**.

- **Serviços**: **Blue Team** equipe defensiva, **Red Team** equipe análise de vulnerabilidade e testes de invasão, equipe de Forense computacional e análise de Malware.

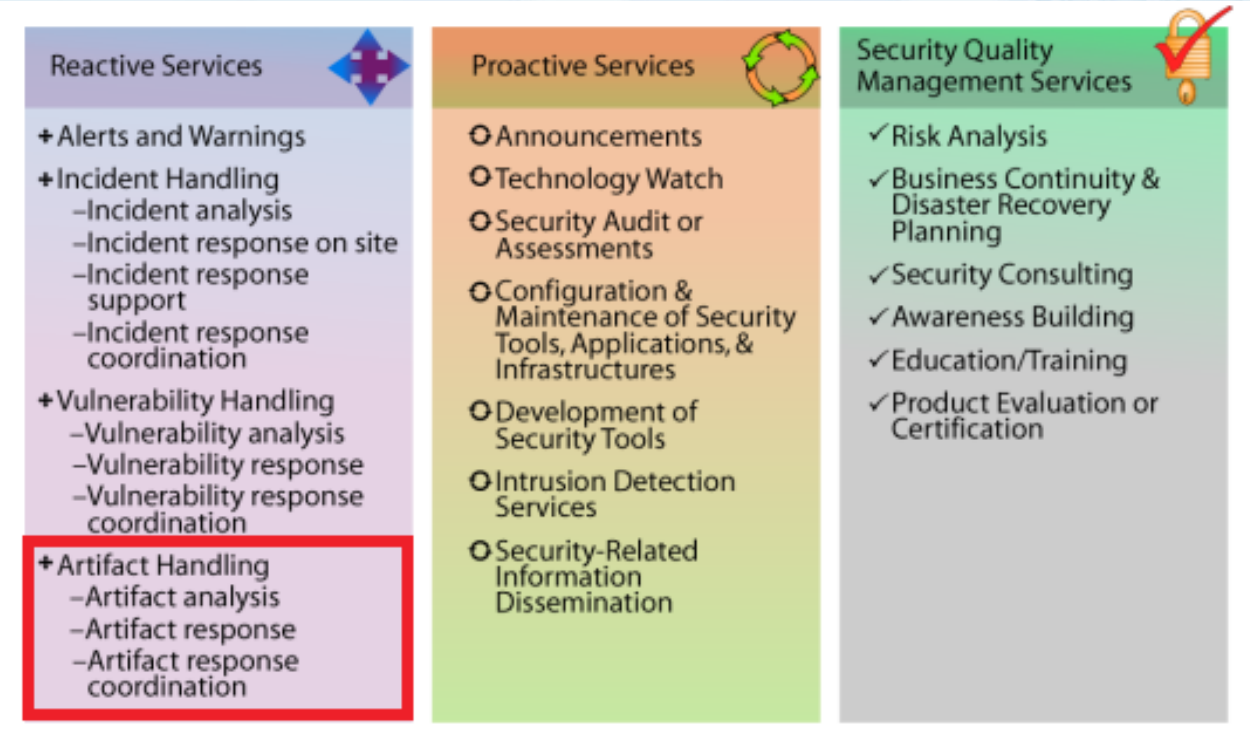


Como surgiu a ideia da construção LAM

HANDBOOK CSIRT

- Curso Oficial do CERT® Division:
  Fundamentals of Incident Handling.

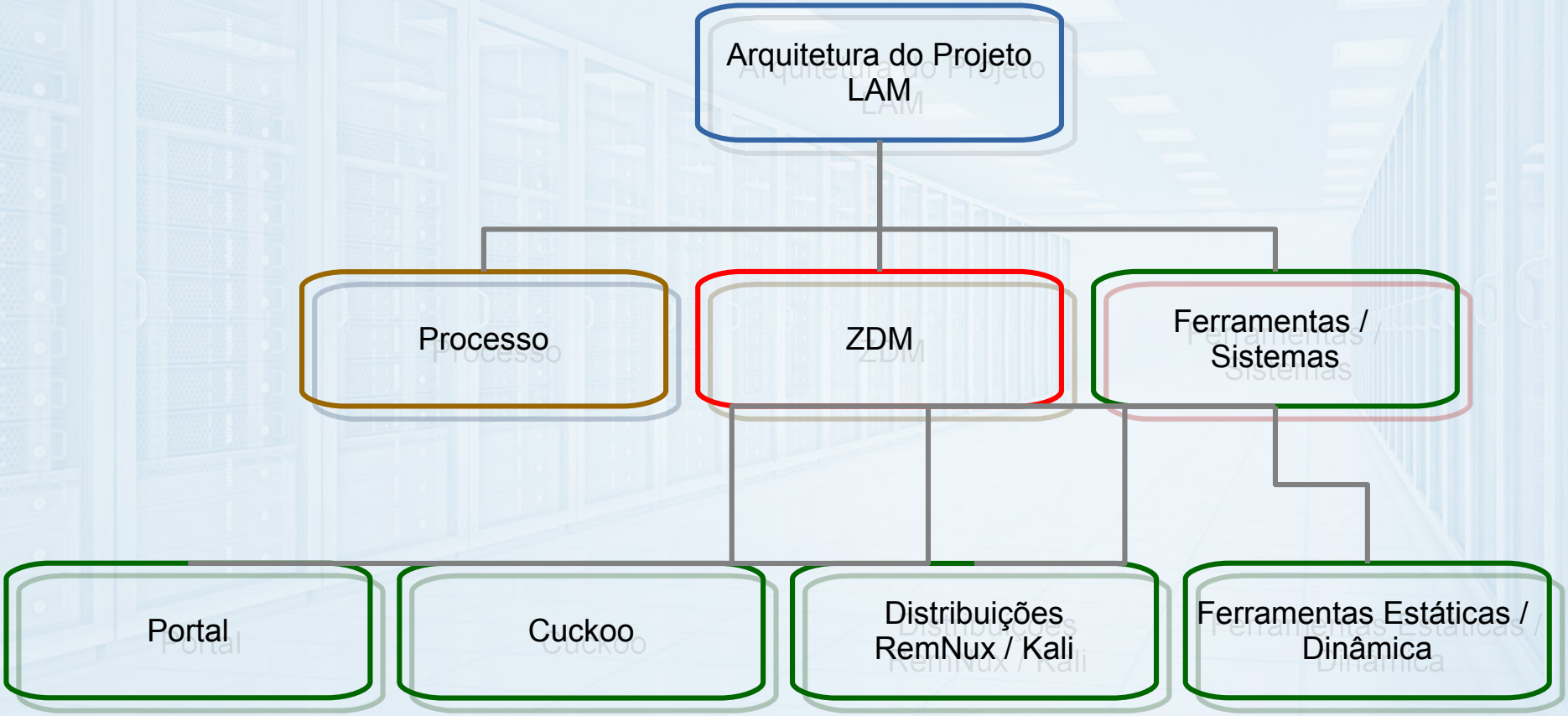
- Curso Oficial do CERT® Division:
  Advanced Incident Handling for Technical Staff



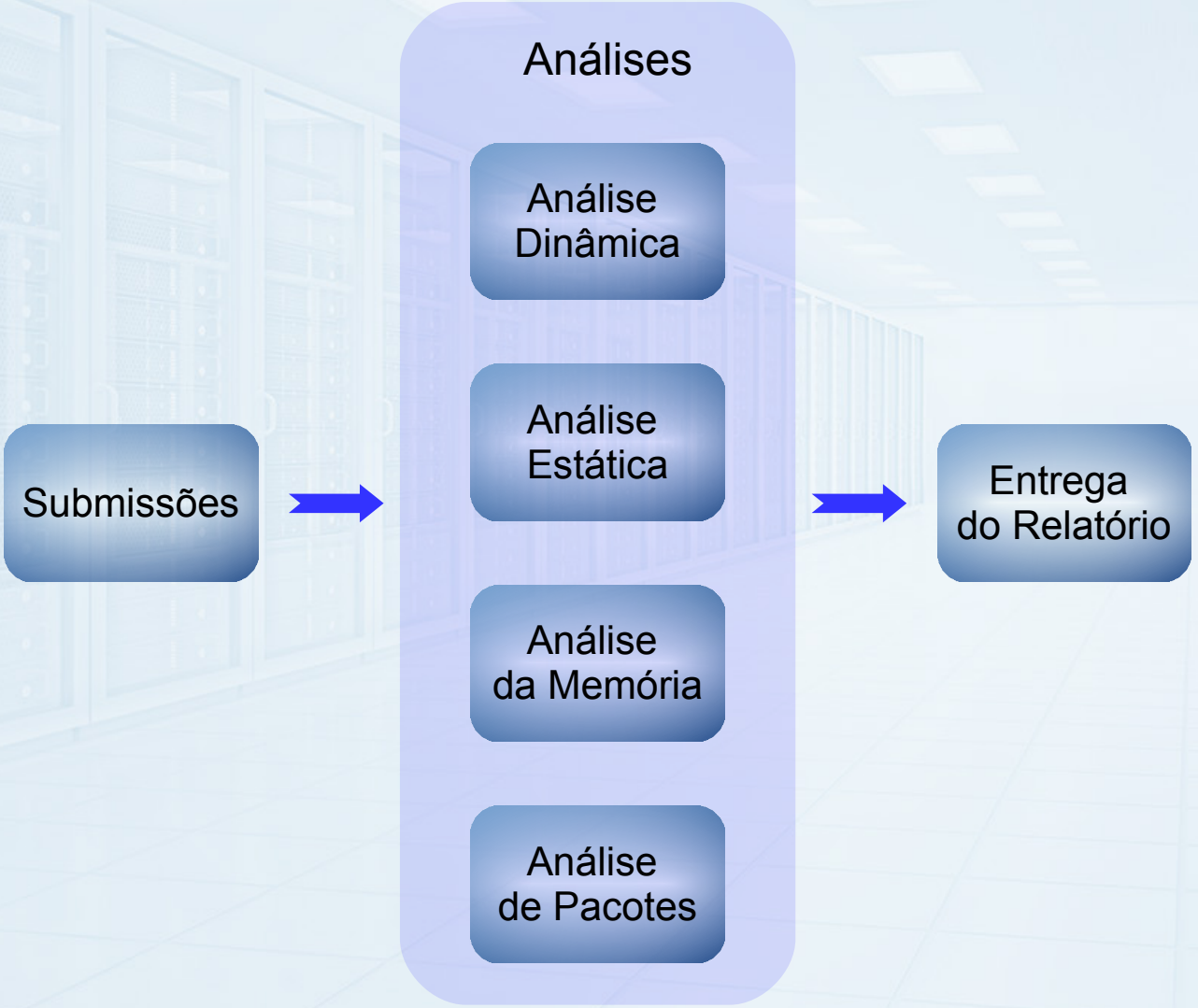
Objetivos do Projeto

- Construir um Laboratório de Análise de Malware (LAM) para o SERPRO;
- Previnir a contaminação em larga escala de códigos maliciosos;
- Fornecer um serviço colaborativo, integrado e de inteligência de Segurança da Informação para o Governo Federal, por meio dos CSIRTS da Adminstração Pública Federal;
- Integrar os principais laboratórios de antivírus, tais como Symantec, Mcafee, Kaspersky.

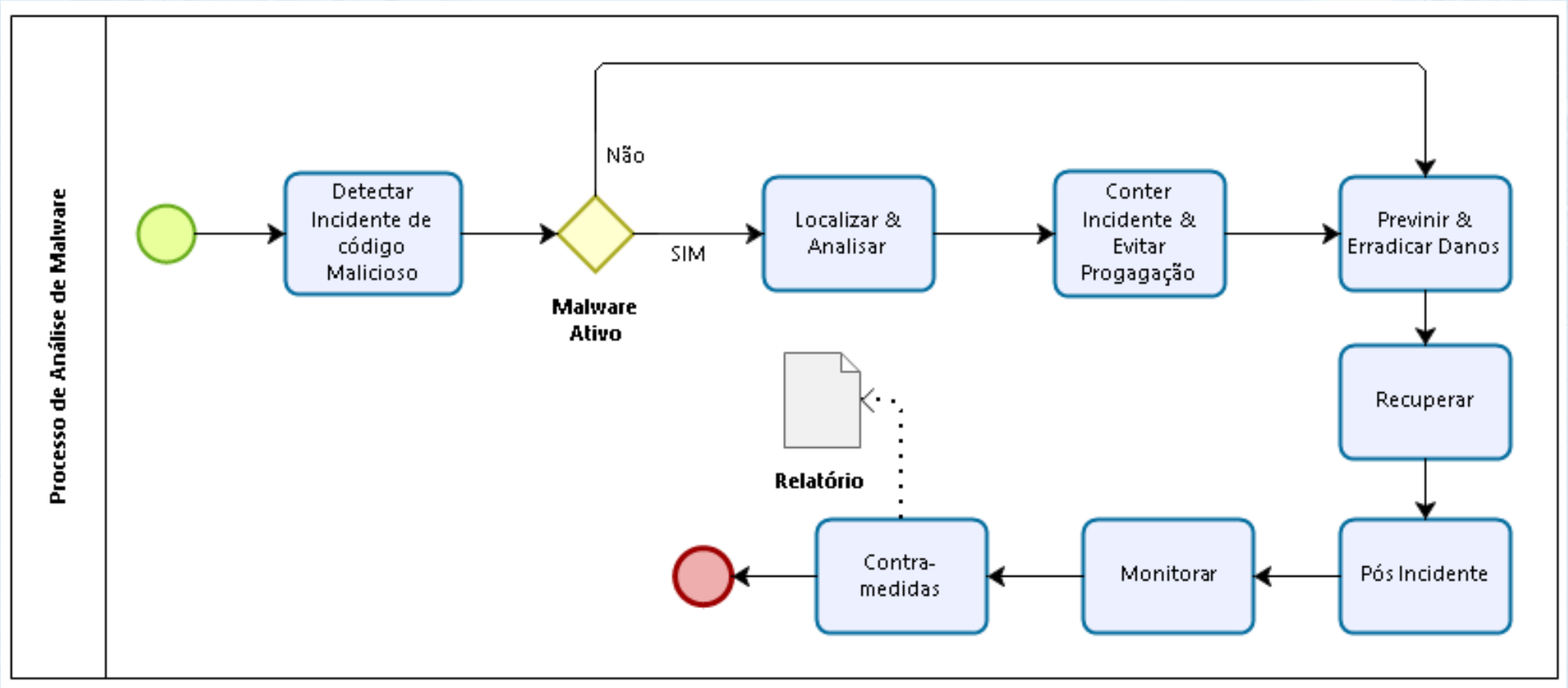
Arquitetura do Projeto LAM



Metodologia de Análise de Malware



Processos do LAM



1ª versão do Processo de Análise de Malware, baseado nos processos Handbook Csirt Carnegie Mellon e NIST 800-83 Guide to Malware Incident Prevention and Handling

Portal LAM

Portal WEB baseado no Demoiselle Framework v. 2.5

Justificativa:

- Ponto único de recebimento dos malwares e resposta/feedback dos relatórios de análise.

Pré-requisitos:

- Cadastro prévio dos representantes dos órgãos e entidades que enviarão amostras de malware para análise;
- Confirmação da identidade dos usuários cadastrados junto aos órgãos ou entidades referenciadas.

Principais Funcionalidades:

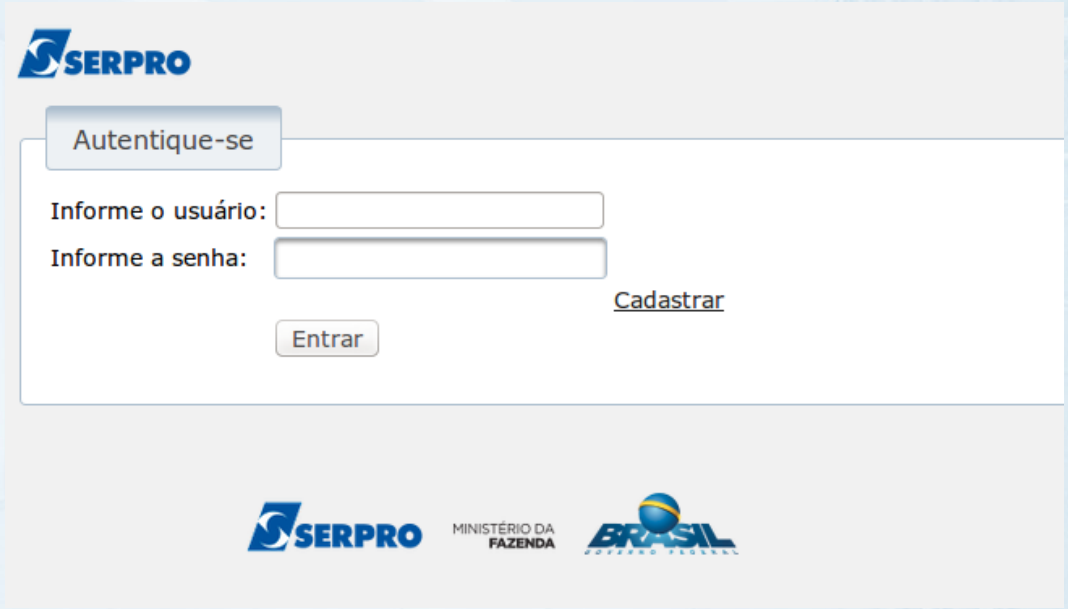
- Detalhamentos da fonte e formato do arquivo e descrição do contexto do malware;
- Feedback através da lista dos arquivos submetidos para análise e acesso aos relatórios das análises submetidas pelo usuário;
- Organização do *pipeline* de **Entrada** (arquivos recebidos), **Processamento** (arquivos em análise) e **Saída / Resultados** (arquivos com análise concluída) do Processo de Análise de Malware.

Portal LAM

Tela Inicial

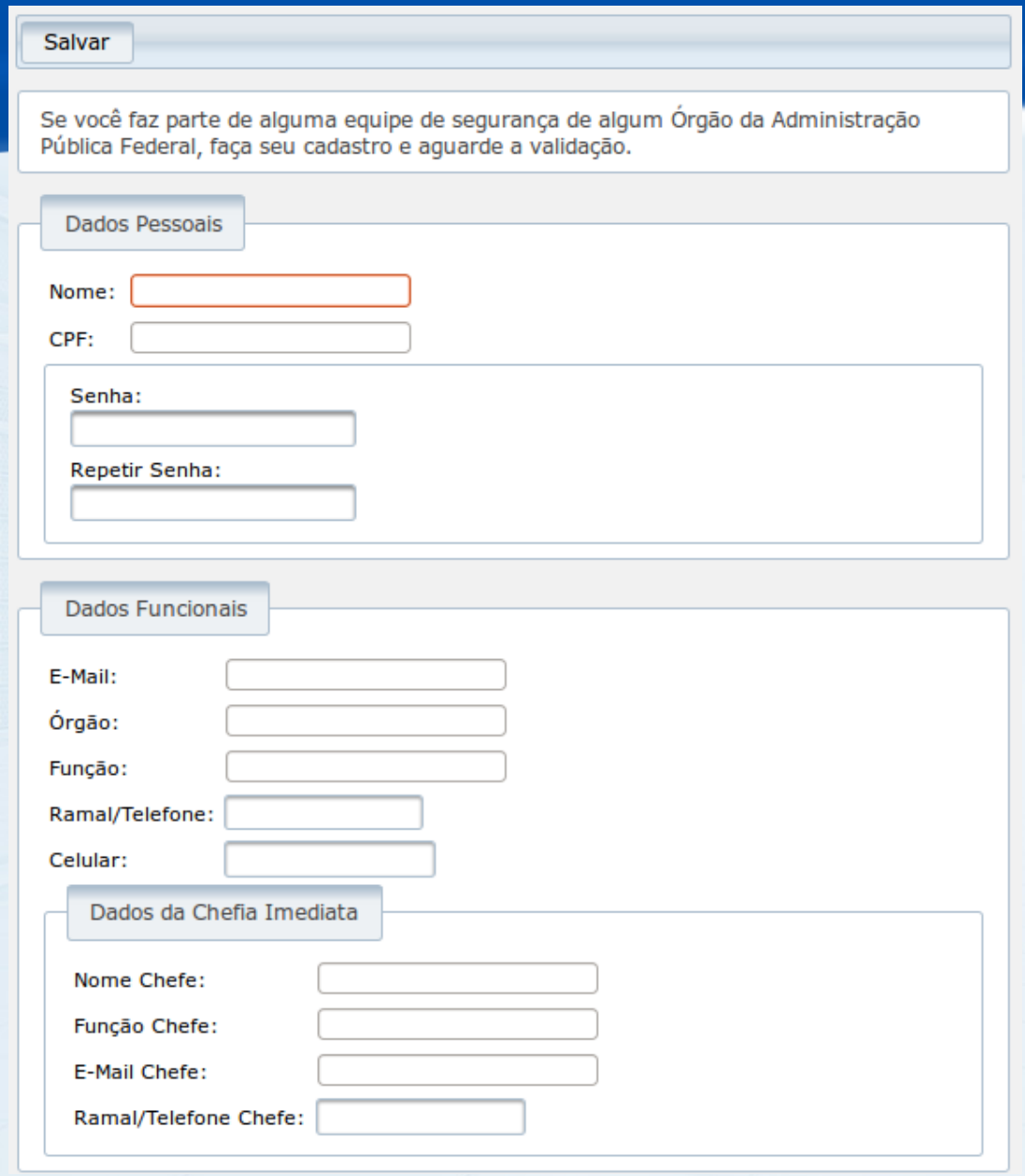
Portal LAM

Tela de Login



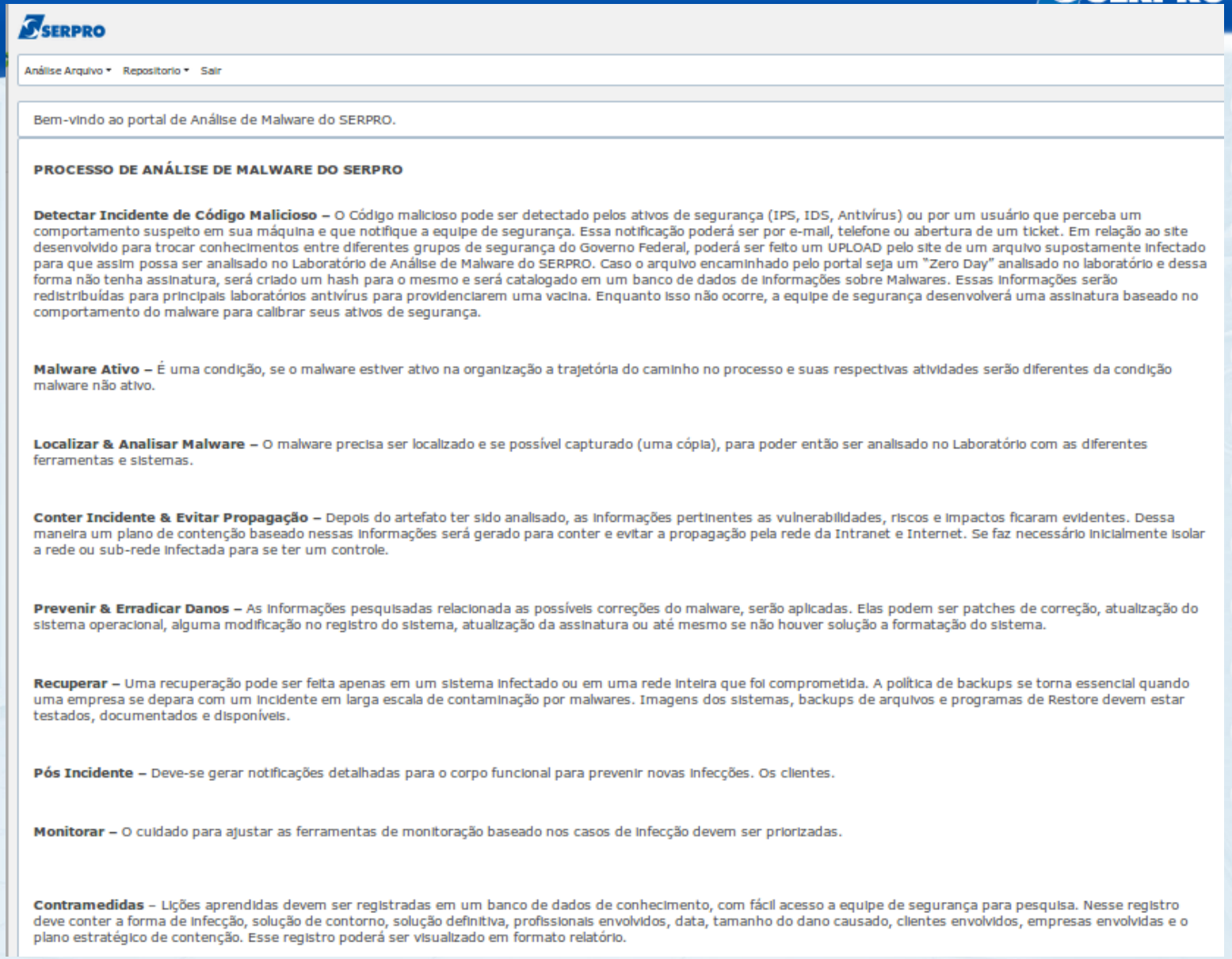
Portal LAM

Tela de Cadastro



Portal LAM

Tela Inicial Após o Login



SERPRO

Análise Arquivo ▾ Repositorio ▾ Sair

Bem-vindo ao portal de Análise de Malware do SERPRO.

PROCESSO DE ANÁLISE DE MALWARE DO SERPRO

Detectar Incidente de Código Malicioso – O Código malicioso pode ser detectado pelos ativos de segurança (IPS, IDS, Antivírus) ou por um usuário que perceba um comportamento suspeito em sua máquina e que notifique a equipe de segurança. Essa notificação poderá ser por e-mail, telefone ou abertura de um ticket. Em relação ao site desenvolvido para trocar conhecimentos entre diferentes grupos de segurança do Governo Federal, poderá ser feito um UPLOAD pelo site de um arquivo supostamente infectado para que assim possa ser analisado no Laboratório de Análise de Malware do SERPRO. Caso o arquivo encaminhado pelo portal seja um "Zero Day" analisado no laboratório e dessa forma não tenha assinatura, será criado um hash para o mesmo e será catalogado em um banco de dados de informações sobre Malwares. Essas informações serão redistribuídas para principais laboratórios antivírus para providenciarem uma vacina. Enquanto isso não ocorre, a equipe de segurança desenvolverá uma assinatura baseado no comportamento do malware para calibrar seus ativos de segurança.

Malware Ativo – É uma condição, se o malware estiver ativo na organização a trajetória do caminho no processo e suas respectivas atividades serão diferentes da condição malware não ativo.

Localizar & Analisar Malware – O malware precisa ser localizado e se possível capturado (uma cópia), para poder então ser analisado no Laboratório com as diferentes ferramentas e sistemas.

Conter Incidente & Evitar Propagação – Depois do artefato ter sido analisado, as informações pertinentes as vulnerabilidades, riscos e impactos ficaram evidentes. Dessa maneira um plano de contenção baseado nessas informações será gerado para conter e evitar a propagação pela rede da Intranet e Internet. Se faz necessário inicialmente isolar a rede ou sub-rede infectada para se ter um controle.

Prevenir & Erradicar Danos – As informações pesquisadas relacionada as possíveis correções do malware, serão aplicadas. Elas podem ser patches de correção, atualização do sistema operacional, alguma modificação no registro do sistema, atualização da assinatura ou até mesmo se não houver solução a formatação do sistema.

Recuperar – Uma recuperação pode ser feita apenas em um sistema infectado ou em uma rede inteira que foi comprometida. A política de backups se torna essencial quando uma empresa se depara com um incidente em larga escala de contaminação por malwares. Imagens dos sistemas, backups de arquivos e programas de Restore devem estar testados, documentados e disponíveis.

Pós Incidente – Deve-se gerar notificações detalhadas para o corpo funcional para prevenir novas infecções. Os clientes.

Monitorar – O cuidado para ajustar as ferramentas de monitoração baseado nos casos de infecção devem ser priorizadas.

Contramedidas – Lições aprendidas devem ser registradas em um banco de dados de conhecimento, com fácil acesso a equipe de segurança para pesquisa. Nesse registro deve conter a forma de infecção, solução de contorno, solução definitiva, profissionais envolvidos, data, tamanho do dano causado, clientes envolvidos, empresas envolvidas e o plano estratégico de contenção. Esse registro poderá ser visualizado em formato relatório.

Portal LAM

Tela Inicial Após o Login

redistribuídas para principais laboratórios antivírus para providenciarem uma vacina. Enquanto isso não ocorre, a equipe de segurança desenvolverá uma assinatura baseado no comportamento do malware para calibrar seus ativos de segurança.

Malware Ativo – É uma condição, se o malware estiver ativo na organização a trajetória do caminho no processo e suas respectivas atividades serão diferentes da condição malware não ativo.

Localizar & Analisar Malware – O malware precisa ser localizado e se possível capturado (uma cópia), para poder então ser analisado no Laboratório com as diferentes ferramentas e sistemas.

Conter Incidente & Evitar Propagação – Depois do artefato ter sido analisado, as informações pertinentes as vulnerabilidades, riscos e impactos ficaram evidentes. Dessa maneira um plano de contenção baseado nessas informações será gerado para conter e evitar a propagação pela rede da Intranet e Internet. Se faz necessário inicialmente isolar a rede ou sub-rede infectada para se ter um controle.

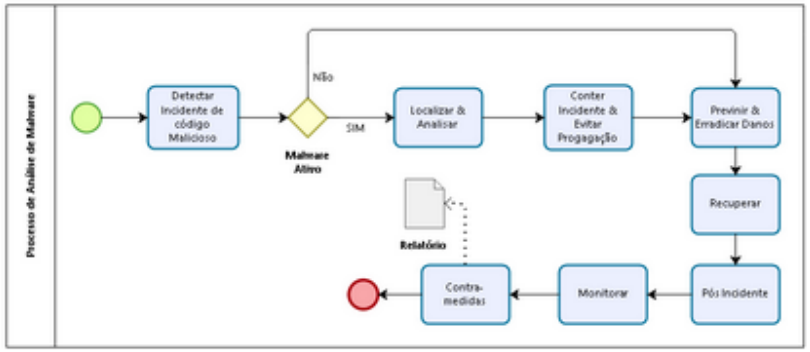
Prevenir & Erradicar Danos – As informações pesquisadas relacionada as possíveis correções do malware, serão aplicadas. Elas podem ser patches de correção, atualização do sistema operacional, alguma modificação no registro do sistema, atualização da assinatura ou até mesmo se não houver solução a formatação do sistema.

Recuperar – Uma recuperação pode ser feita apenas em um sistema infectado ou em uma rede inteira que foi comprometida. A política de backups se torna essencial quando uma empresa se depara com um incidente em larga escala de contaminação por malwares. Imagens dos sistemas, backups de arquivos e programas de Restore devem estar testados, documentados e disponíveis.

Pós Incidente – Deve-se gerar notificações detalhadas para o corpo funcional para prevenir novas infecções. Os clientes.

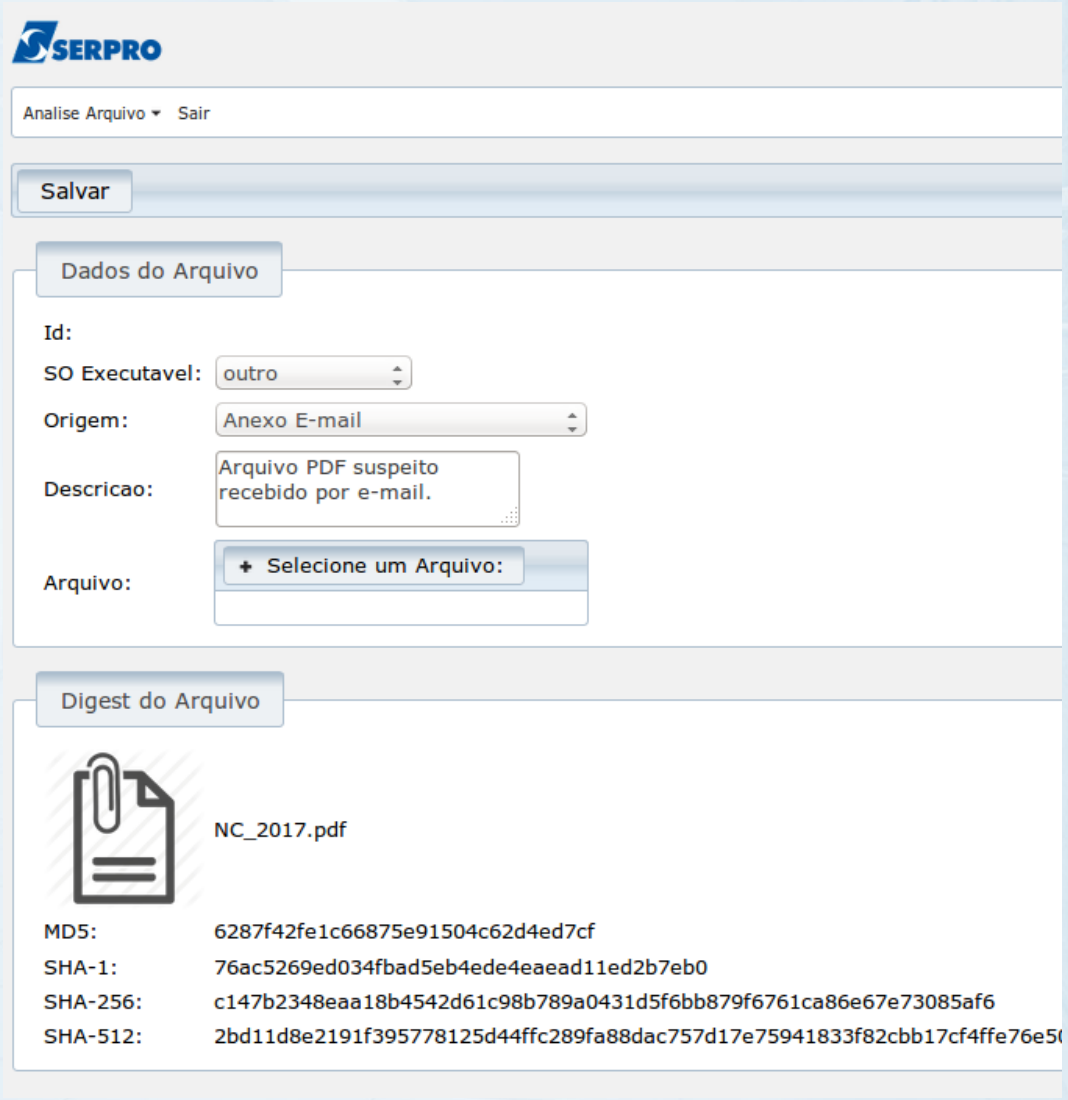
Monitorar – O cuidado para ajustar as ferramentas de monitoração baseado nos casos de infecção devem ser priorizadas.

Contramedidas – Lições aprendidas devem ser registradas em um banco de dados de conhecimento, com fácil acesso a equipe de segurança para pesquisa. Nesse registro deve conter a forma de infecção, solução de contorno, solução definitiva, profissionais envolvidos, data, tamanho do dano causado, clientes envolvidos, empresas envolvidas e o plano estratégico de contenção. Esse registro poderá ser visualizado em formato relatório.

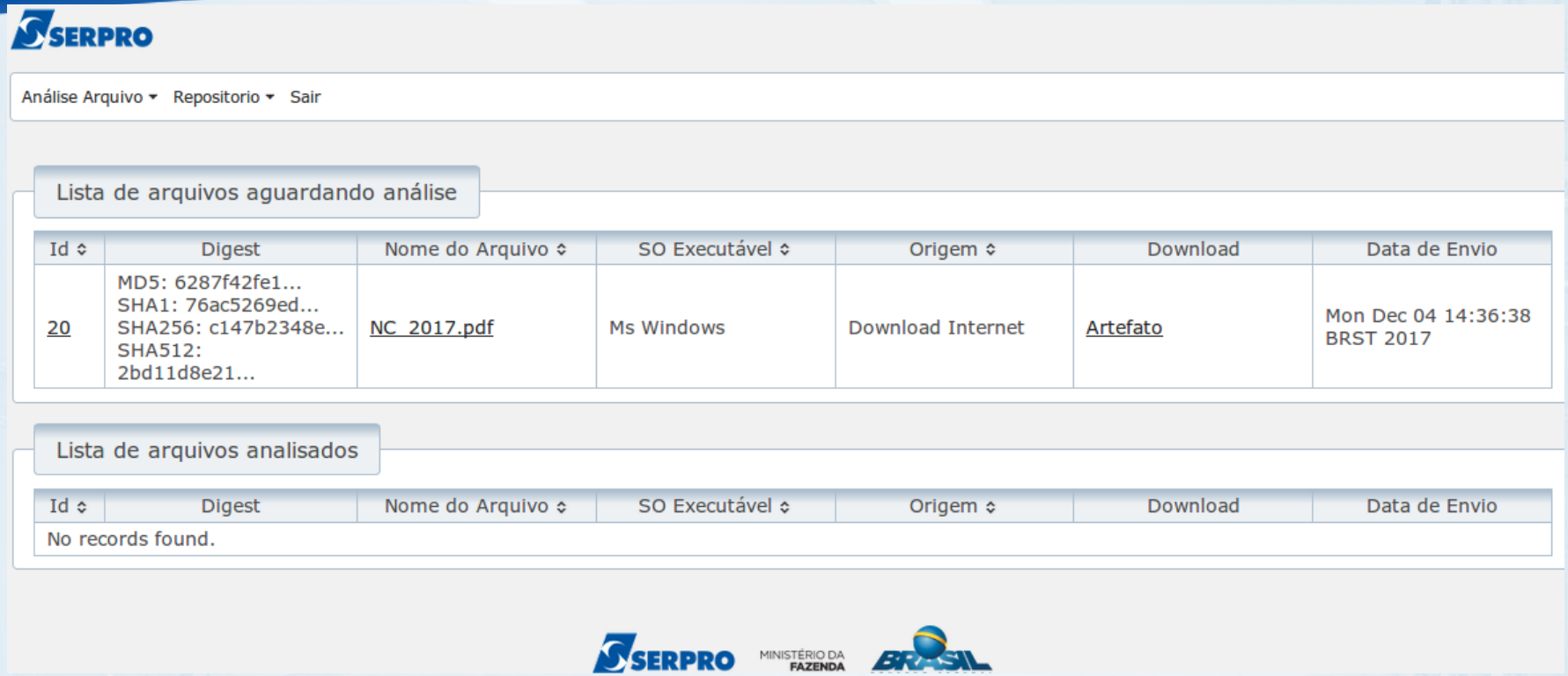


Portal LAM

Formulário de envio de arquivo



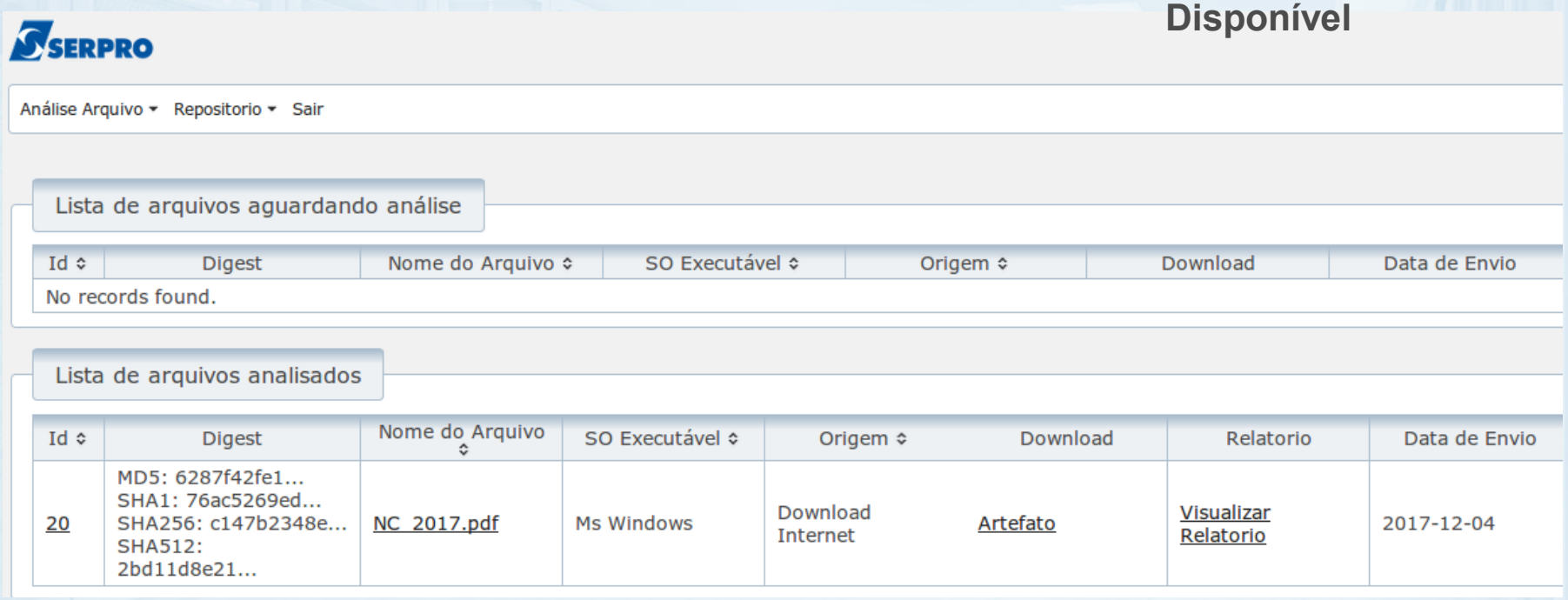
Portal LAM



Após o envio do artefato pelo usuário o arquivo vai para a lista de arquivos aguardando análise

Portal LAM

Relatório de Análise Disponível



Após a conclusão da análise, o arquivo vai para a lista de arquivos analisados

Portal LAM

SERPRO

Link de Download do Artefato

Lista de Arquivos Aguardando Analise

	Id	Digest	Organização de Origem	Usuario	Nome do Arquivo	SO Executável	Origem	Download	Data de Envio
☑	20	MD5: 6287f42fe1... SHA1: 76ac5269ed... SHA256: c147b2348e... SHA512: 2bd11d8e21...	CERT.br	user1@mail.con	NC_2017.pdf	Ms Windows	Download Internet	Artefato	2017-12-04

Analisar

Lista de Arquivos em Analise

	Id	Digest	Organização de Origem	Usuario	Nome do Arquivo	SO Executável	Origem	Download	Relatório	Data de Envio
No records found.										

Concluir

Lista de Arquivos Analisados

Id	Digest	Organização de Origem	Usuario	Nome do Arquivo	SO Executável	Origem	Download	Relatório	Data de Envio
No records found.									

Após o envio do artefato por parte dos usuários, na tela dos Administradores aparece uma lista contendo os novos artefatos que estão aguardando análise

Portal LAM

SERPRO

Lista de Arquivos Aguardando Analise

	Id	Digest	Organização de Origem	Usuario	Nome do Arquivo	SO Executável	Origem	Download	Data de Envio
No records found.									

Analisar

Link de Edição do Relatório

Lista de Arquivos em Analise

	Id	Digest	Organização de Origem	Usuario	Nome do Arquivo	SO Executável	Origem	Download	Relatório	Data de Envio
☐	20	MD5: 6287f42fe1... SHA1: 76ac5269ed... SHA256: c147b2348e... SHA512: 2bd11d8e21...	CERT.br	user1@mail.c	NC_2017.pdf	Ms Windows	Download Internet	Artefato	Editar Relatório	2017-12-04

Concluir

Lista de Arquivos Analisados

Id	Digest	Organização de Origem	Usuario	Nome do Arquivo	SO Executável	Origem	Download	Relatório	Data de Envio
No records found.									

Após baixar os artefatos, o arquivo passa para o estado de “em ananlise”, onde vai permanecer até que seja submetido o relatório da análise

Portal LAM

SERPRO

Lista de Arquivos Aguardando Analise

	Id	Digest	Organização de Origem	Usuario	Nome do Arquivo	SO Executável	Origem	Download	Data de Envio
No records found.									

Analisar

Link de Acesso do Relatório

Lista de Arquivos em Analise

	Id	Digest	Organização de Origem	Usuario	Nome do Arquivo	SO Executável	Origem	Download	Relatório	Data de Envio
No records found.										

Concluir

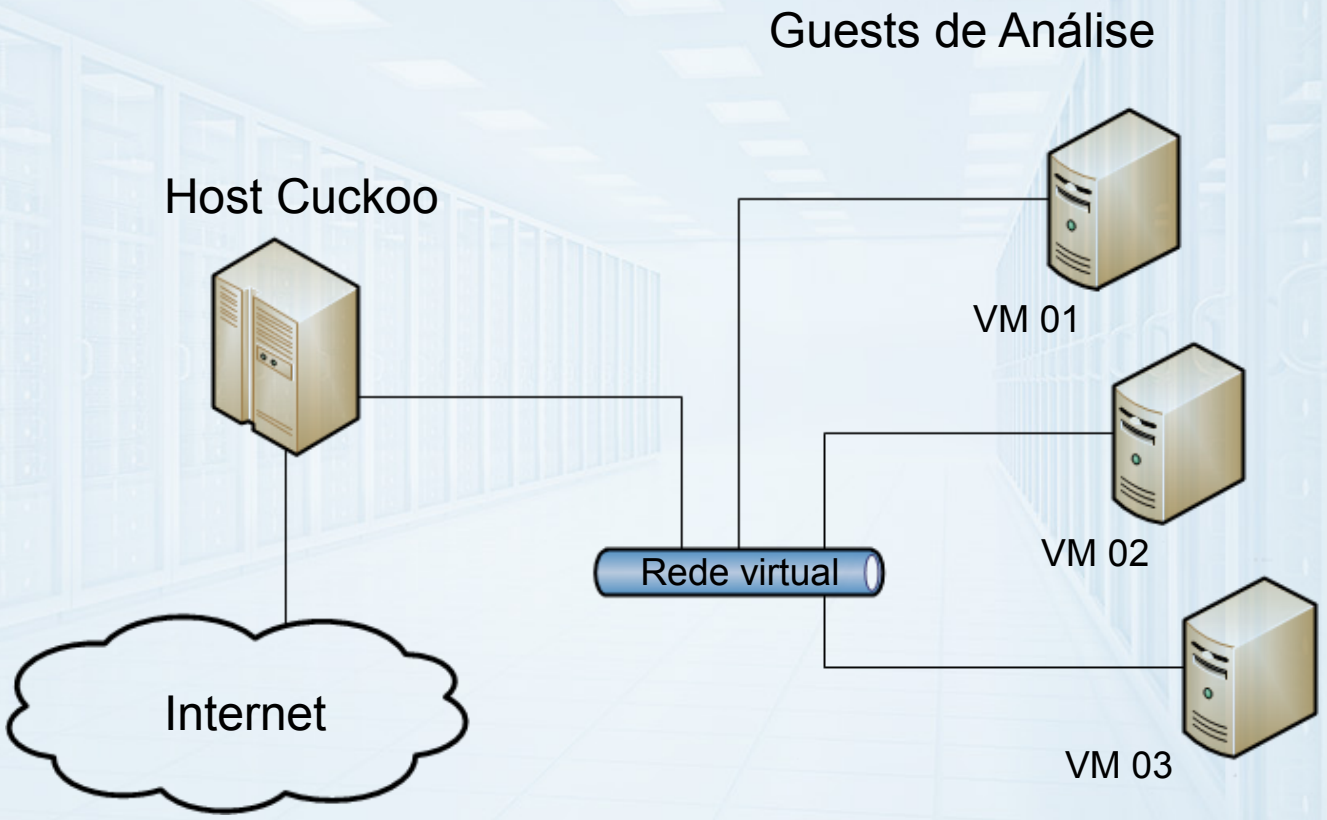
Lista de Arquivos Analisados

Id	Digest	Organização de Origem	Usuario	Nome do Arquivo	SO Executável	Origem	Download	Relatório	Data de Envio
20	MD5: 6287f42fe1... SHA1: 76ac5269ed... SHA256: c147b2348e... SHA512: 2bd11d8e21...	CERT.br	user1@mail.cc	NC_2017.pdf	Ms Windows	Download Internet	Artefato	Visualizar Relatorio	2017-12-04

Após submissão do relatório da análise, o arquivo vai para a lista de arquivos analisados, servindo de histórico para o administrador

Cuckoo

- Arquitetura Automatizada de Análise de Malware;
- Conceito de *sandbox (*mecanismo de segurança para separar programas em execução, de modo a permitir uma análise dinâmica do comportamento de um *malware);*
- Consiste em uma central de gerenciamento que coleta e analisa amostras de execução de arquivos suspeitos.



Arquitetura original do Cuckoo

RemNUX

REMnux: A Linux Toolkit for Reverse-Engineering and Analyzing Malware

Uma distribuição FREE, criada pelo Lenny Zeltser, baseada no UBUNTU. Existe a versão para máquina virtual e docker.

1. **Examine Browser Malware** – Thug, Wget, Network Miner.
2. **Examine Document Files** – AnalizePDF, qpdf, shellcode2exe.
3. **Extract and Decode Artifacts** – FLOSS, strings, foremost.
4. **Handle Network Interactions** – Wireshark, TCPdump, tcpik.
5. **Process Multiple Samples** – Viper, Maltrieve, MASTIFF.
6. **Examine File Properties and Contents** – YARA, totalhash.
7. **Investigate Linux Malware** – strace, BokKen, Pyew.
8. **Edit and View Files** – Xpdf, feh, Vim.
9. **Examine Memory Snapshots** – Volatility, Rekall, findaes.
10. **Statically Examine PE Files** – UPX, Peframe, Vivisect.
11. **Investigate Mobile Malware** – Androwarn, AndroGuard.
12. **Perform Other Tasks** – Docker, Procdot, vtTOOL

KALI

A empresa *Offensive Security* é mundialmente conhecida pelo seguimento de testes de vulnerabilidades de segurança, análise de malware e diferentes ferramentas para segurança da informação.

1. **Information Gathering** – Dnsmap, arp-scan, casefile.
2. **Vulnerability Analysis** – Cisco-auditing-tool, nmap.
3. **Wireless Attacks** – Aircrack-ng, mdk3, asleep.
4. **Web Applications** – Apache-users, fimap, maltego teeth.
5. **Exploitation Tools** – Armitage, backdoor factory, BeEF.
6. **Forensics Tools** – Volatility, p0f, capstone.
7. **Stress Testing** – T50, inundator, ipv6-toolkit.
8. **Sniffing & Spoofing** – Wireshark, tcpdump, DNSchef.
9. **Password Attacks** – Brutespray, hashcat, truecrack.
10. **Maintaining Access** – Cryptcat, pwnat, webshells.
11. **Reverse Engineering** – OlyDBG, apktool, jad.
12. **Hardware Hacking** – Arduino, smali, dex2jar.
13. **Reporting Tools** – Dradis, cherrytree, pipal.

Ferramentas de Análise Estática

Análise Estática

- Método de examinar um programa/código de computador **SEM** executar o programa.

Disassemblers
· IDA Pro Free

Debuggers
· OllyDbg · Immunity Debugger · WinDbg

Decompiladores
· DeDe · VB Decompiler Pro · Hex-Rays Decompiler

Identificadores de Arquivos
· PeiD · Exeinfo · RDG Packer Detector · File

Ferramentas de Análise Dinâmica

Análise Dinâmica

- Método de examinar um programa /código de computador **ENQUANTO** o programa estiver em execução.

Monitoramento do Sistema
· Autoruns
· Process Explorer
· Process Hacker
· Process Monitor
· Regshot
· TCPView
· Wireshark

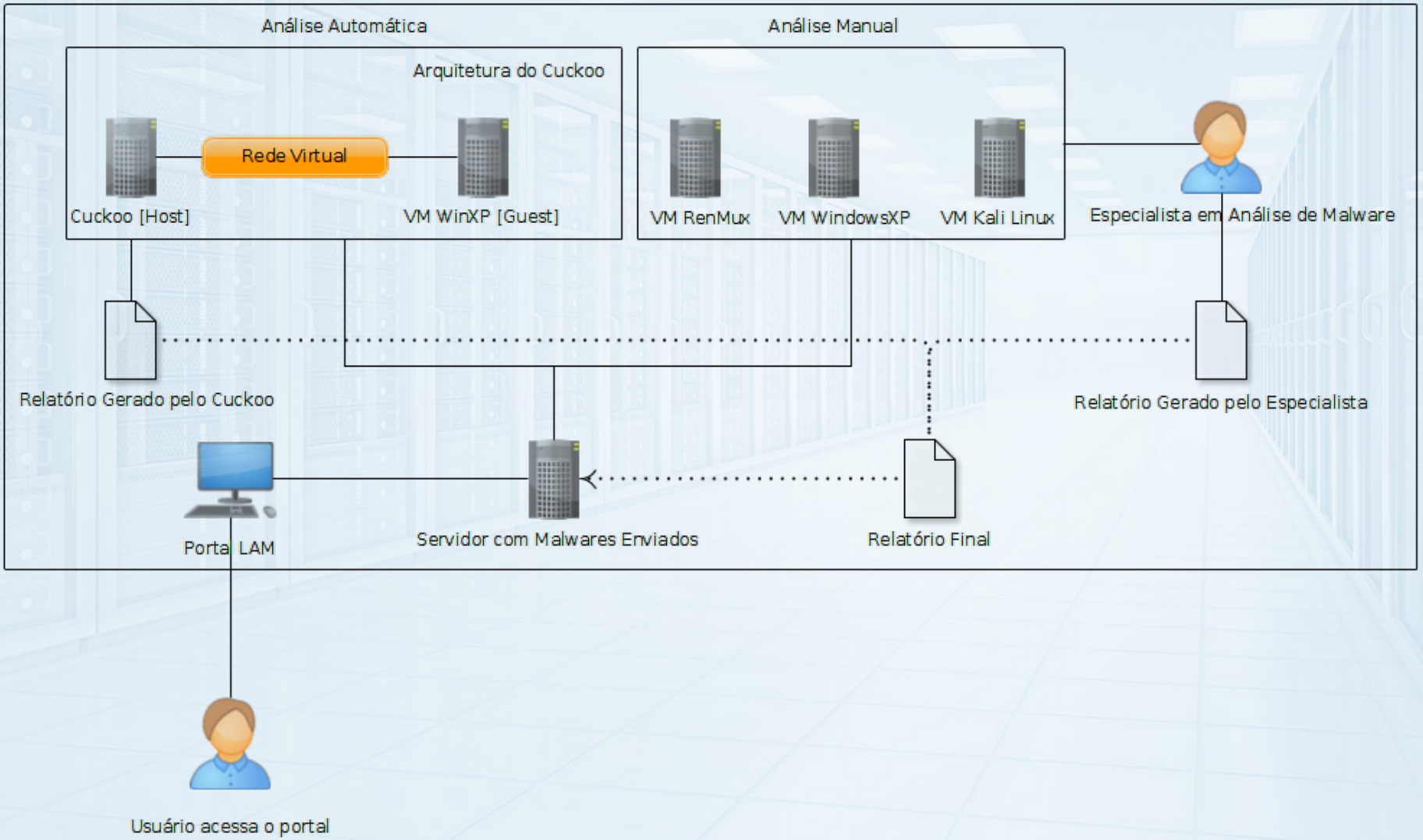
Ferramentas de Análise de Memória

Análise de Memória

- Método de examinar a memória de um computador **APÓS** a execução do programa suspeito.

Forense de Memória
· LordPE · MoonSols · Windows Memory Toolkit · Memoryze · Volatility Framework

Visão Geral da Integração da Arquitetura do LAM



Integração, Colaboração entre empresas Anti-Malware

- Realizado contato com representantes de outros laboratórios.
- Interessados em participar do projeto e compartilhar informações e conhecimento:
  - Kaspersky
  - McAfee
  - Symantec

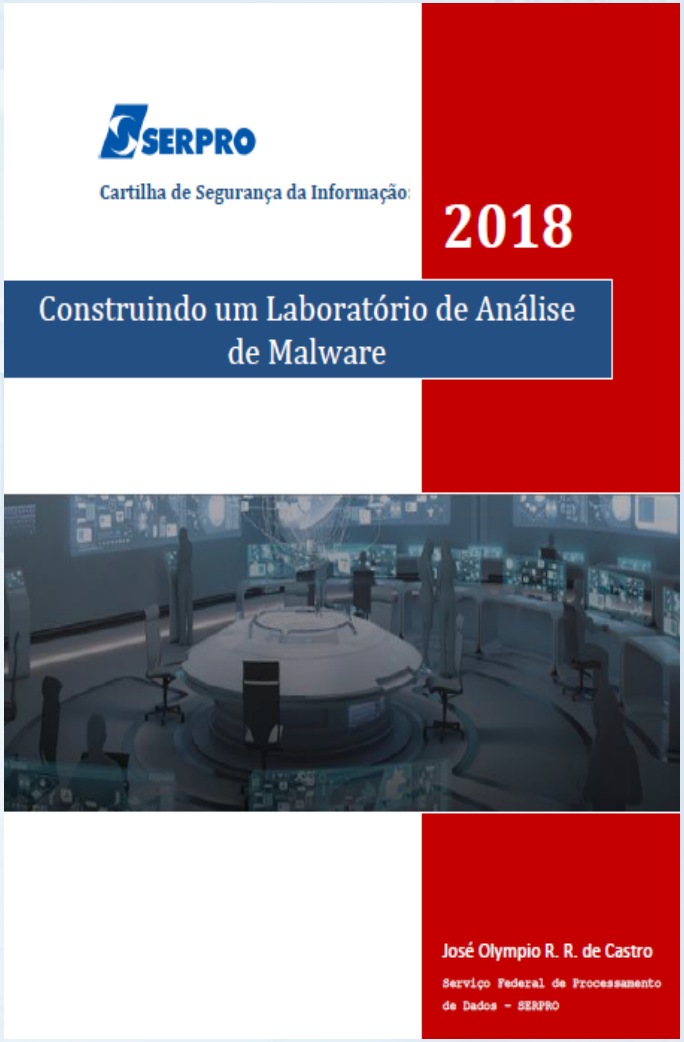
KASPERSKY lab

McAfee®
Proven Security™

Symantec™

Cartilha “Construindo um laboratório de análise de Malware”

A cartilha de segurança da informação do SERPRO será gratuita e seu foco será na construção de um laboratório de análise de malware. Poderá ser personalizado para o tamanho da organização e o tipo de negócio que ela exerce.



ROADMAP - Novos componentes para LAM

MISP
Threat Sharing

MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing

Uma plataforma de inteligência contra ameaças para compartilhar, armazenar e correlacionar indicadores de comprometimento de ataques direcionados, informações sobre ameaças, informações sobre fraudes financeiras, informações sobre vulnerabilidades ou até mesmo informações sobre antiterrorismo. Descubra como o **MISP** é usado hoje em várias organizações. Não apenas para armazenar, compartilhar, colaborar em indicadores de segurança cibernética, análise de malware, mas também para usar os IoCs e informações para detectar e prevenir ataques ou ameaças contra infraestruturas de TIC, orga

Co-financed by the European Union
Connecting Europe Facility

http://www.misp-project.org/features.html

ROADMAP - Novos componentes para LAM

Home › Virus & Threats

Canada's CSE Spy Agency Releases Malware Analysis Tool

By Eduard Kovacs on October 20, 2017

Share G+ Tweet Recomendar 13 RSS

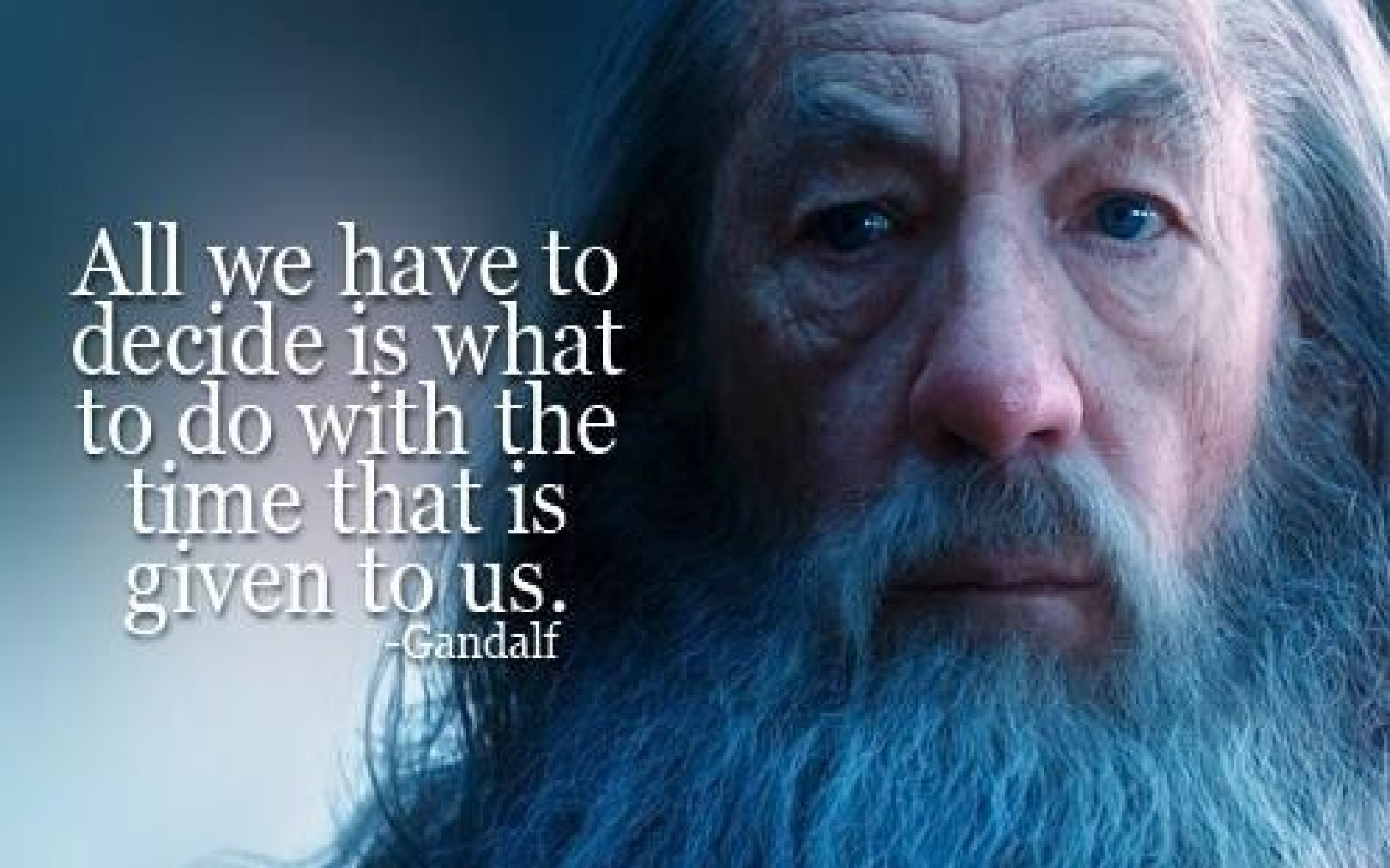
Canada's Communications Security Establishment (CSE) agency announced this week that the source code for one of its malware detection and analysis tools has been made public.

The Python-based tool released as open source by the spy agency is named **Assemblyline** and it was created within the CSE's Cyber Defence program. The organization says this is one of the tools it uses to protect the country's computer systems against advanced cyber threats.

Assemblyline allows defenders to automate the analysis of malicious files. The analysis process, which has been compared to a conveyor belt, involves assigning a unique identifier to files as they travel through the system, looking for signs of malicious functionality and extracting features for further analysis, generating alerts for malicious files and assigning them a score, and sending data to other protection systems so that identified threats can be neutralized.

Users can also add their own analytics, including custom-built software and antiviruses, to enhance Assemblyline's capabilities.

ASSEMBLYLINE


All we have to decide is what to do with the time that is given to us.
-Gandalf

Ficha Técnica

Maria da Gloria Guimarães dos Santos
Diretor Presidente

Ulysses Alves Machado
Coordenador da Coordenação Estratégica de Gestão da Segurança da Informação – CEGSI

Gerente do Projeto
José Olympio Rezende Ribeiro de Castro
Gerente Departamento de Segurança da Informação – DP/CEGSI/SISEI

Izabella Matos – DP/CEGSI/SISEI/SIDES
Tarcisio Viera – DP/CEGSI/SISEI/SIDES
Equipe

José Roberto Cabral - DP/CEGSI/SISEI/SIDES
Gestor de Qualidade do Projeto

Leandro Gomes **- Gerente de Segurança de Desenvolvimento Seguro**
Ismael Tedesco **- Gerente de Serviço de Segurança e Monitoração**
Gustavo Alencar **- Chefe do GRA Recife**
Equipe GRA Recife
Colaboradores