Modulo 1 - O Perigo

O objetivo do módulo é explicar por que redes e dados são atacados

- Virtualização - Computadores virtuais podem ser executados dentro de um mesmo computador físico
    - Maquinas virtuais são chamadas de "guests"
    - Computadores físicos são chamados de "hosts"
- OVF - É um padrão aberto para acondicionar e distribuir dispositivos virtuais
    - Um pacote OVF possui vários diretórios. Esse diretório é distribuído para um pacote de OVA.
    - Esse pacote contém todos os arquivos de OVF necessários para implementar a máquina virtual.
- Informações de identificação pessoal (PII) são todas as informações que podem ser usadas para identificar um indivíduo.
    - Nome, número de previdência, número de cartão, etc
- PHI - É um subconjunto do PII, com dados médicos
- PSI - É um tipo de PII, contém informações de indivíduo de acesso à rede.

Módulo 2 - Soldados na guerra contra o crime digital

Objetivo desse módulo é explicar como se preparar para uma carreira em operações de segurança cibernética.

- SOC - Oferece desde monitoramento e gerenciamento até soluções abrangentes de segurança personalizada.
    - Pode ser interno ou contratado por fornecedores de segurança.

Pessoas no SOC

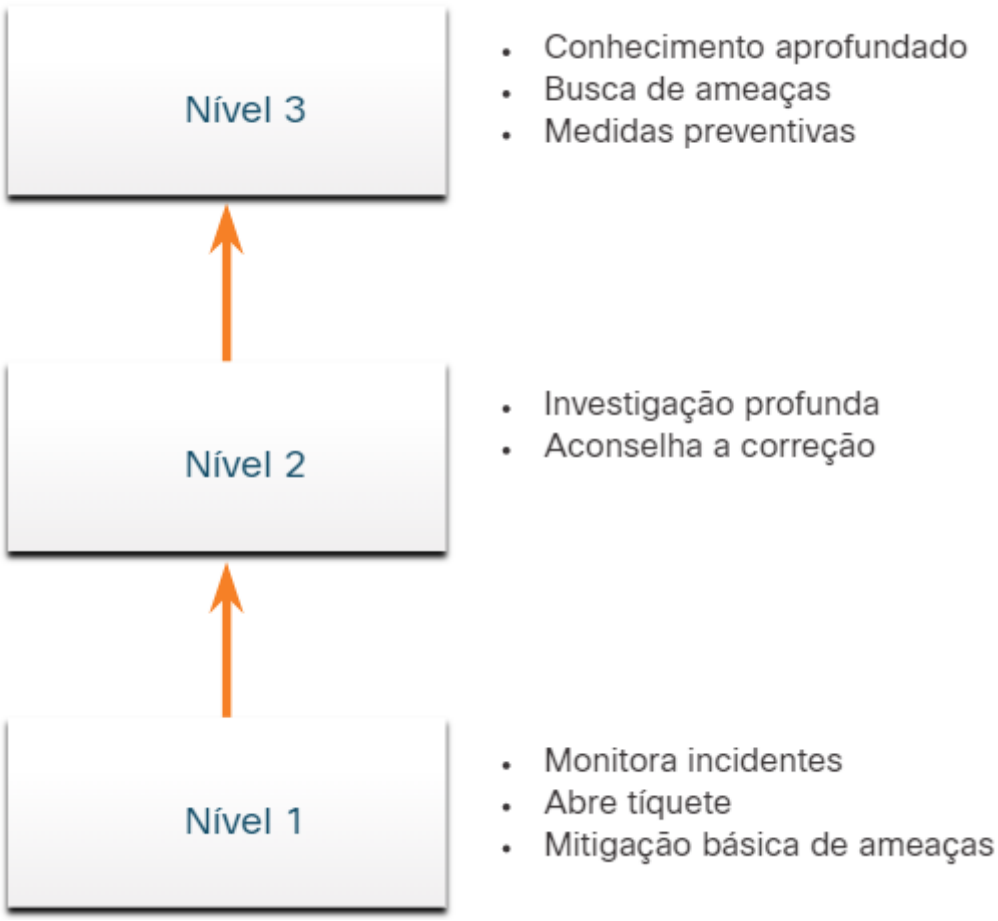
- Analista de alerta 1 - Monitora alerta recebido e envia para o nível 2
- Respondente a incidentes de nível 2 - Investigação aprofundada e aconselha a correção ou ação a ser tomada
- Caçador de ameaças de nível 3 - Habilidades de nível especializado em rede, endpoint, inteligência e engenharia reversa.
    - Busca de ameaças e detecção no sistema.
- Gerente de SOC - Gerencia todos os recursos do SOC.

Processo no SOC

- Um sistema de emissão de tíquetes é frequentemente usado para atribuir alertas a uma fila para que um analista investigue.
- O analista verifica se o alerta é verdadeiro ou falso.

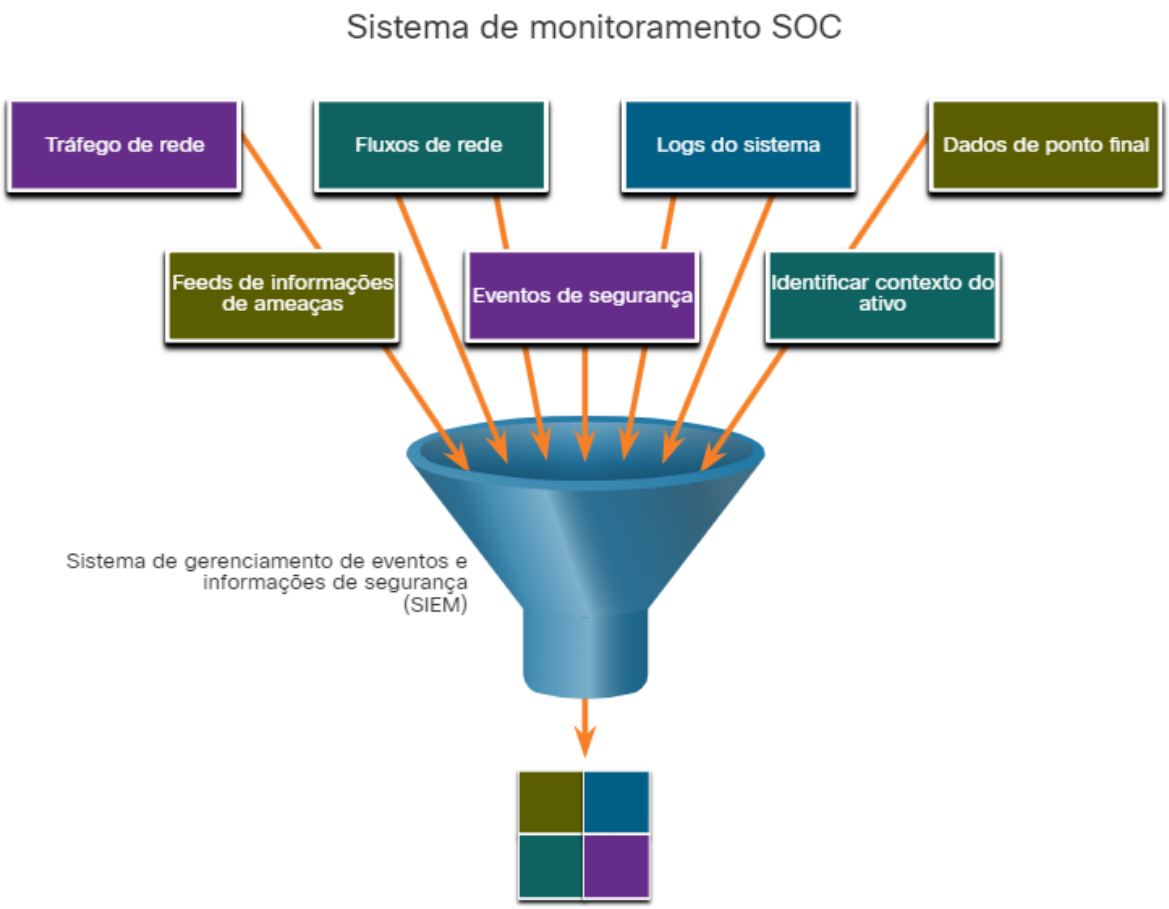
- Quando a verificação for estabelecida, o incidente pode ser encaminhado aos investigadores ou outro pessoal para ser tratado.
    - Caso não, será descartado como um alarme falso.

Se o ticket não puder ser resolvido, será encaminhado para um analista de incidente nivel 2, se este também não puder resolver, será encaminhado para o pessoal do nível 3



Tecnologias no SOC: SIEM

- **SIEM** - Security Information and Event Management System (sistema de gerenciamento de eventos e informações de segurança)
    - O SIEM recebe dados gerados por firewalls, dispositivos de rede, sistemas de detecção de intrusões e outros dispositivos
    - Os sistemas de SIEM são usados para coletar e filtrar dados, detectar e classificar ameaças e analisar e investigar ameaças.
        - Coleta, correção e análise de eventos
        - Monitoramento de segurança
        - Controle de Segurança
        - Gerenciamento de logs
        - Avaliação de vulnerabilidade
        - Controle de vulnerabilidades
        - Inteligência de ameaças

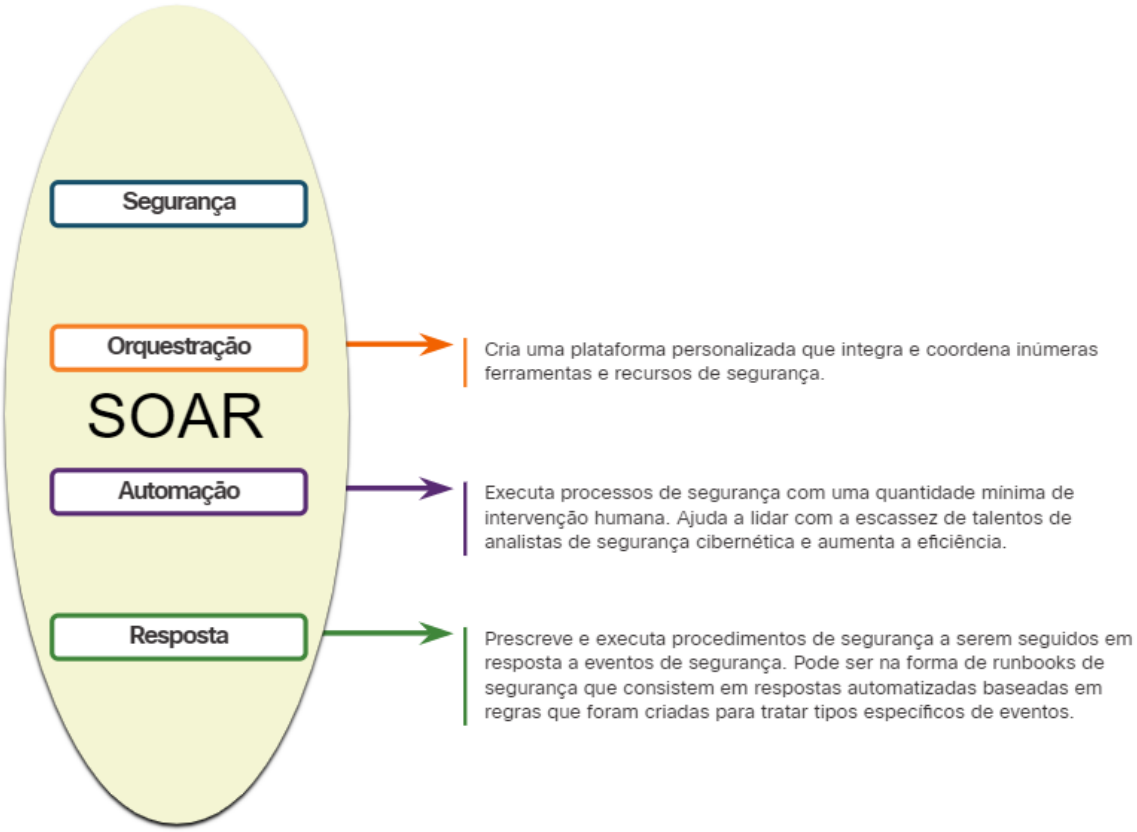


Tecnologias no SOC: SOAR

SIEM e orquestração de segurança, automação e resposta (SOAR) normalmente são colocados juntos pois possuem ferramentas que se complementam.

- SecOps utilizam ambas ferramentas para otimizar o SOC.

SOAR é integrado com sistema de inteligência contra ameaças e automatiza os fluxos de trabalho e investigação e resposta de incidentes, com base em manuais desenvolvidos pela equipe de segurança.



Plataformas de segurança SOAR:

- Reunir dados de alarme de cada componente do sistema
- Ferramentas para pesquisar os dados
- Integrar e automatizar fluxos para respostas mais rápidas
- Incluir playbooks predefinidos que permitem a resposta automática a ameaças específicas.

Devido a automação, o SOAR libera a equipe para cuidar de assuntos mais urgentes.

Métricas SOC

Muitas métricas ou indicadores chave de desempenho (KPI) podem ser projetadas para medir diferentes aspectos específicos do desempenho do SOC.

- Tempo de permanência -
- Tempo médio para detectar (MTTD) -
- Tempo médio para responder (MTTR) -
- Tempo médio para conter (MTTC) -
- Tempo de controle -

Segurança corporativa e gerenciada

A Cisco oferece serviços como:

- Serviço Cisco Smart Net Total Care para Resolução Rápida de Problemas;
- Equipe de resposta a incidentes de segurança do produto (PSIRT) da Cisco;

- Equipe de resposta a incidentes de segurança de computadores da Cisco (CSIRT);
- Serviços Gerenciados Cisco;
- Operações Táticas Cisco (TacOps);
- Programa de Segurança Física e Segurança da Cisco.

Segurança versus disponibilidade

Cada empresa ou setor tem uma tolerância limitada para o tempo de inatividade da rede.

O tempo de atividade preferencial geralmente é medido no número de minutos de inatividade em um ano

Disponibilidade %	Tempo de inatividade
99.8%	17,52 horas
99,9% (“três noves”)	8,76 horas
99,99% (“quatro noves”)	52,56 minutos
99,999% (“cinco noves”)	5.256 minutos
99,9999% (“seis noves “)	31,56 segundos
99,99999% (“sete noves “)	3,16 segundos

Deve existir um equilíbrio entre a segurança e a possibilidade dos funcionários trabalharem.

Módulo 3 - O Sistema Operacional Windows

O Objetivo do módulo é explicar os recursos de segurança do sistema operacional Windows.

- Laboratório para identificar processos em execução utilizando o Windows Sysinternals Suite

Sistema Operacional de Disco

O sistema operacional de disco (DOS) é um sistema operacional que o computador usa para habilitar esses dispositivos de armazenamento de dados para ler e gravar arquivos.

- DOS fornece um sistema de arquivos que organiza os arquivos de uma forma específica no disco.
    - A microsoft comprou o DOS e criou o MS-DOS

Um sistema operacional moderno como o Windows 10 não é considerado um sistema operacional de disco. Ele é construído no Windows NT, que significa “Novas Tecnologias”. O próprio sistema operacional está no controle direto do computador e seu hardware.

- NT é um sistema operacional com suporte para vários processos de usuário.
    - Isso é muito diferente do MS-DOS de um único processo e de usuário único.

Comando MS-DOS	Descrição
dir	Mostra uma lista de todos os arquivos no diretório atual (pasta)
cd *diretório*	Altera o diretório para o diretório indicado
cd ..	Muda o diretório para o diretório acima do diretório atual
cd \	Muda o diretório para o diretório raiz (geralmente C:)
copy *fonte de destino*	Copia arquivos para outro local
del *nome do arquivo*	Exclui um ou mais arquivos.
find	Procura texto em arquivos
mkdir *diretório*	Cria um novo diretório.
ren *nome_antigo nome_novo*	Renomeia um arquivo
help	Exibe todos os comandos que podem ser usados, com uma breve descrição
help *comando*	Exibe a ajuda extensa para o comando indicado

Versões do Windows

A maioria das versões do Windows desde 1993 utilizadas pelo público utiliza o Sistema Operacional NT, devido à segurança de arquivos oferecida pelo sistema.

- A partir do Windows XP, uma edição de 64 bits estava disponível.
- Quando o sistema operacional e o hardware suportam a operação de 64 bits, conjuntos de dados extremamente grandes podem ser usados.
    - Esses grandes conjuntos de dados incluem bancos de dados muito grandes, computação científica e manipulação de vídeo digital de alta definição com efeitos especiais.
- Computadores e sistemas operacionais de 64 bits são compatíveis com programas mais antigos de 32 bits, mas programas de 64 bits não podem ser executados em hardware mais antigo de 32 bits.

Versões do Windows:

SO	Versões
Windows 7	Starter, Home Basic, Home Premium, Professional, Enterprise, Ultimate
Windows Server 2008 R2	Foundation, Standard, Enterprise, Datacenter, Web Server, HPC Server, Itanium-Based Systems
Windows Home Server 2011	Nenhum
Windows 8	Windows 8, Windows 8 Pro, Windows 8 Enterprise, Windows RT
Windows Server 2012	Foundation, Essentials, Standard, Datacenter
Windows 8.1	Windows 8.1, Windows 8.1 Pro, Windows 8.1 Enterprise, Windows RT 8.1
Windows Server 2012 R2	Foundation, Essentials, Standard, Datacenter
Windows 10	Home, Pro, Pro Education, Enterprise, Education, loT Core, Mobile, Mobile Enterprise
Windows Server 2016	Essentials, Standard, Datacenter, Multipoint Premium Server, Storage Server, Hyper-V Server

Vulnerabilidades do Sistema Operacional

Uma **vulnerabilidade** é alguma falha ou fraqueza que pode ser explorada por um invasor para reduzir a viabilidade das informações de um computador.

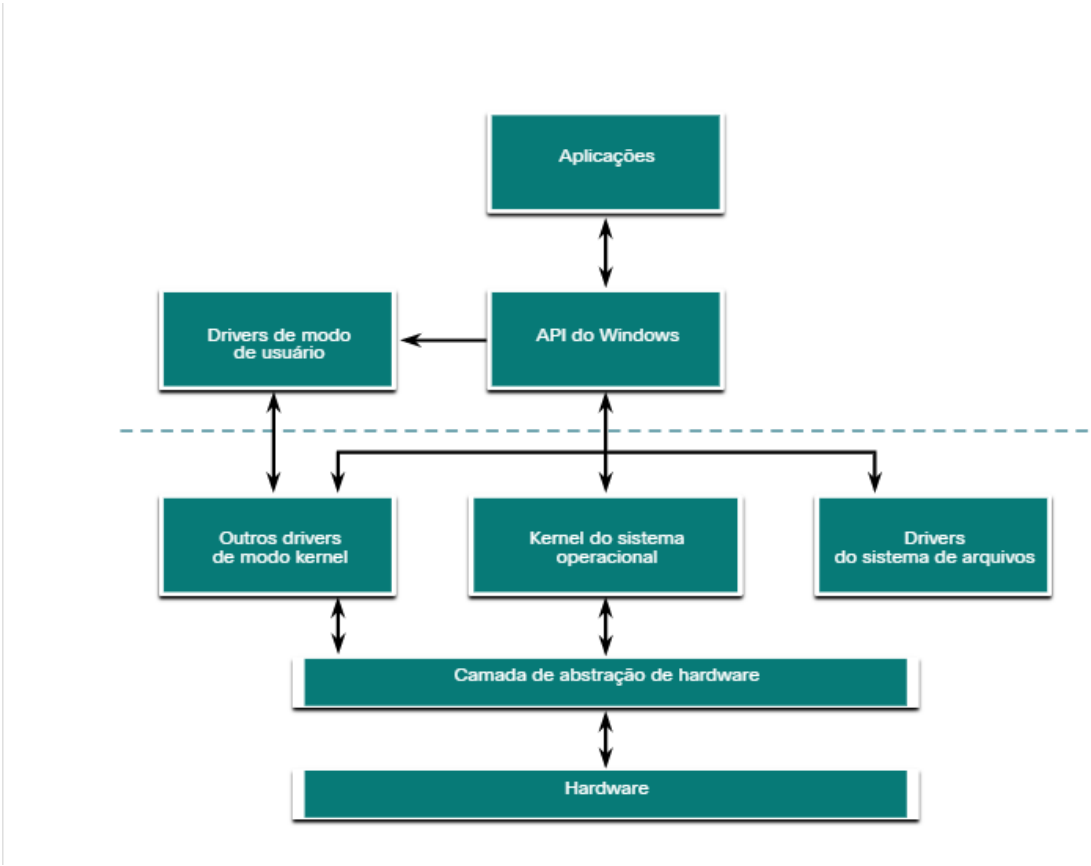
- Para tirar proveito de uma vulnerabilidade do sistema operacional, o invasor deve usar uma técnica ou uma ferramenta para explorar a vulnerabilidade.

Algumas recomendações comuns de Segurança do Windows:

Recomendação	Descrição
Proteção contra vírus ou malware	Por padrão, o Windows usa o Windows Defender para proteção contra malware.O Windows Defender fornece um conjunto de ferramentas de proteção incorporadas ao sistema.Se o Windows Defender estiver desativado, o sistema ficará mais vulnerável a ataques e malware.
Serviços desconhecidos ou não gerenciados	Há muitos serviços que funcionam nos bastidores.É importante certificar-se de que cada serviço é identificável e seguro.Com um serviço desconhecido em execução em segundo plano, o computador pode ficar vulnerável a ataques.
Criptografia	Quando os dados não são criptografados, eles podem ser facilmente coletados e explorados.Isso não é importante apenas para computadores desktop, mas especialmente dispositivos móveis.
Política de segurança	Uma boa política de segurança deve ser configurada e seguida.Muitas configurações no controle de Diretiva de Segurança do Windows podem impedir ataques.
Firewall	Por padrão, o Windows usa o Firewall do Windows para limitar a comunicação com dispositivos na rede.Com o tempo, as regras podem não se aplicar mais.Por exemplo, uma porta pode ser deixada aberta que não deve mais estar prontamente disponível.É importante revisar periodicamente as configurações do firewall para garantir que as regras ainda são aplicáveis e remover as que não se aplicam mais
Permissões de arquivo e compartilhamento	Essas permissões devem ser definidas corretamente. É fácil dar ao grupo “Todos” Controle Total, mas isso permite que todas as pessoas façam o que quiserem a todos os arquivos. É melhor fornecer a cada usuário ou grupo as permissões mínimas necessárias para todos os arquivos e pastas.
Senha fraca ou sem senha	Muitas pessoas escolhem senhas fracas ou não usam nenhuma senha.É especialmente importante certificar-se de que todas as contas, especialmente a conta de Administrador, têm uma senha muito forte.
Login como Administrador	Quando um usuário faz logon como administrador, qualquer programa executado terá os privilégios dessa conta.É melhor fazer login como um Usuário Padrão e usar apenas a senha de administrador para realizar determinadas tarefas.

Arquitetura e operações do Windows

Camada de Abstração de Hardware



Uma **camada de abstração de hardware (HAL)** é um software que lida com toda a comunicação entre o hardware e o kernel.

O **kernel** é o núcleo do sistema operacional e tem controle sobre todo o computador.

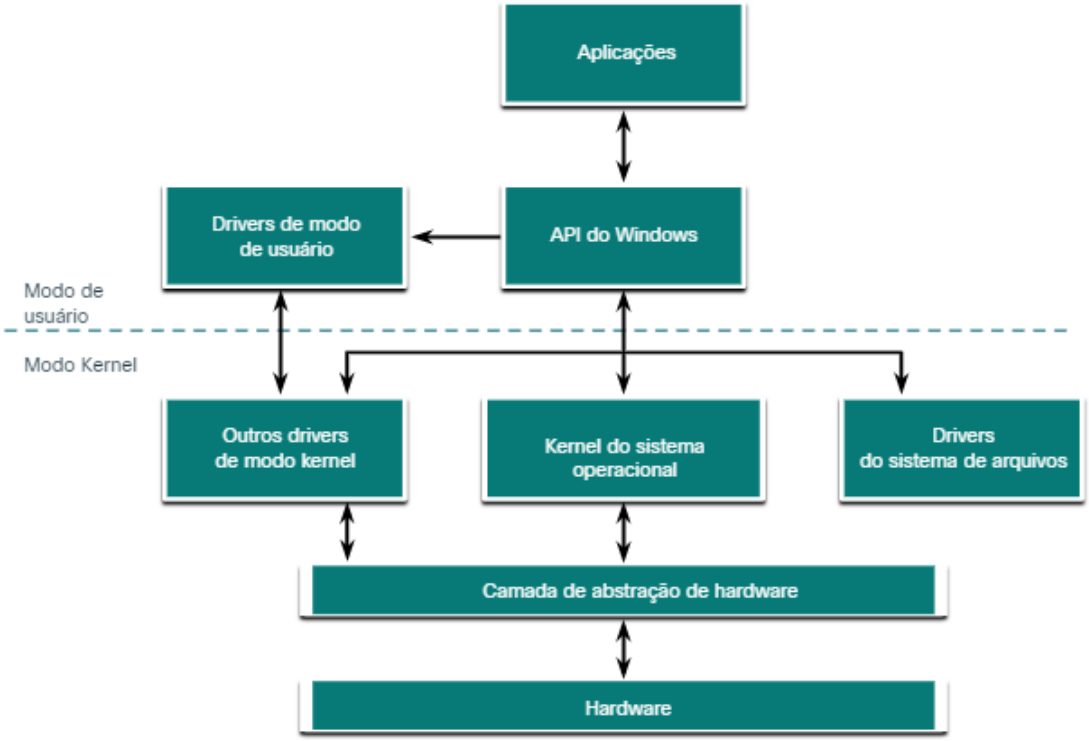
- Ele lida com todas as solicitações de entrada e saída, memória e todos os periféricos conectados ao computador.

Em alguns casos, o kernel ainda se comunica diretamente com o hardware, portanto não é completamente independente do HAL.

- O HAL também precisa do kernel para executar algumas funções.

Modo de usuário e modo kernel

Existem dois modos diferentes em que uma CPU opera quando o computador tem o Windows instalado: **o modo de usuário** e o **modo kernel**.



Os aplicativos instalados são executados no modo de usuário e o código do sistema operacional é executado no modo kernel.

- O código que está sendo executado no modo kernel tem acesso irrestrito ao hardware subjacente e é capaz de executar qualquer instrução de CPU.
- O código do modo kernel também pode referenciar qualquer endereço de memória diretamente.
    - **Falhas no código em execução no modo kernel param a operação de todo o computador**.

Por outro lado, aplicativos de usuário são executados em modo usuário e não tem contato direto com o hardware ou memória.

- O código do modo usuário passa pelo Sistema Operacional para acessara memória.
- Devido a esse isolamento, falhas no modo usuário são restritas apenas ao aplicativo e são recuperáveis.
    - A maioria dos programas do windows são executados em modo usuário.
        - Drivers são executados em modo kernel ou usuário, dependendo do driver.

Todo o código que é executado no modo kernel usa o mesmo espaço de endereço.

- Os drivers de modo kernel não têm isolamento do sistema operacional.
    - Se ocorrer um erro em um driver em execução no modo kernel e ele gravar no local errado, o sistema operacional ou outro driver pode ser afetado negativamente.
    - O driver pode falhar, fazendo com que todo o sistema operacional falhe.

Quando o código de modo de usuário é executado, ele é concedido seu próprio espaço de endereço restrito pelo kernel, juntamente com um processo criado especificamente para o aplicativo.

- O objetivo é justamente impedir que aplicativos alterem o código do sistema operacional.
- Ao ter seu próprio processo, esse aplicativo tem seu próprio espaço de endereço privado, tornando outros aplicativos incapazes de modificar os dados nele.
    - Isso ajuda evitar que o sistema operacional ou outros aplicativos falhem se o aplicativo falhar.

Sistema de arquivos do Windows

Sistema de arquivos é como a informação é organizada dentro da mídia de armazenamento.

Sistema de arquivos do Windows:

Sistema de Arquivos Windows	Descrição
exFAT	Este é um sistema de arquivos simples suportado por muitos sistemas operacionais diferentes.O FAT tem limitações para o número de partições, tamanhos de partições e tamanhos de arquivo que pode resolver, portanto, não é mais usado para discos rígidos (HDs) ou unidades de estado sólido (SSDs).Tanto o FAT16 quanto o FAT32 estão disponíveis para uso, sendo o FAT32 o mais comum porque tem muito menos restrições do que o FAT16.
Sistema de Arquivos Hierárquico Plus (HFS+)	Este sistema de arquivos é usado em computadores MAC OS X e permite nomes de arquivos, tamanhos de arquivo e tamanhos de partição muito mais longos do que os sistemas de arquivos anteriores.Embora não seja suportado pelo Windows sem software especial, o Windows é capaz de ler dados de partições HFS+.
Sistema de arquivos estendido (EXT)	Este sistema de arquivos é usado com computadores baseados em Linux.Embora não seja suportado pelo Windows, o Windows é capaz de ler dados de partições EXT com software especial.
New Technology File System (NTFS)	Este é o sistema de arquivos mais comumente usado ao instalar o Windows. Todas as versões do Windows e Linux suportam NTFS.Computadores Mac-OS X só podem ler uma partição NTFS. Eles são capazes de gravar em uma partição NTFS depois de instalar drivers especiais.

O NTFS é o sistema de arquivos mais utilizado para windows

- Suporta arquivos e partições grandes
- Compatível com outros sistemas operacionais

- Confiável e tem suporte a recursos de recuperação
- Suporta muitos recursos de segurança
- O acesso aos dados é obtido através de **descritores de segurança**
    - Esse descritor contém permissões e propriedades do arquivo
- Também controla carimbos de data/hora para controle do arquivo, também chamado de MACE
    - **MACE** > Access, Create e Entry Modified
- Também suporta criptografia.

Antes que um dispositivo de armazenamento possa ser usado, ele deve ser formatado com um sistema de arquivos.

- Antes de ser formatado, precisa ser particionado
    - O disco rígido é dividido em partições.
        - Cada partição é uma unidade lógica de armazenamento
- Normalmente o próprio Sistema operacional já formada com o sistema de arquivos NTFS.

A formatação em NTFS cria estruturas importantes:

- **Setor de inicialização de partição** - Primeiro 16 setores de unidade. Contém o local da tabela de arquivos mestre (MFT). Os últimos 16 setores contêm uma cópia do setor de inicialização.
- **Tabela de arquivos mestre (MFT)** - Contêm os locais de todos os arquivos e diretórios na partição (carimbo, atributos e informações de segurança)
- **Arquivos de sistema** - Arquivos ocultos com informações sobre valores e atributos
- **Área de arquivo** - Área principal onde os arquivos e diretórios são armazenados.

OBS: Ao formatar uma partição, os dados podem ser recuperados, por que nem todos os dados são completamente removidos.

- É importante realizar um apagamento seguro em uma unidade que está sendo reutilizada
    - O **apagamento seguro** grava dados várias vezes em toda unidade para garantir que não há dados restantes.

Fluxos de dados alternativos

NTFS armazena arquivos como uma série de atributos.

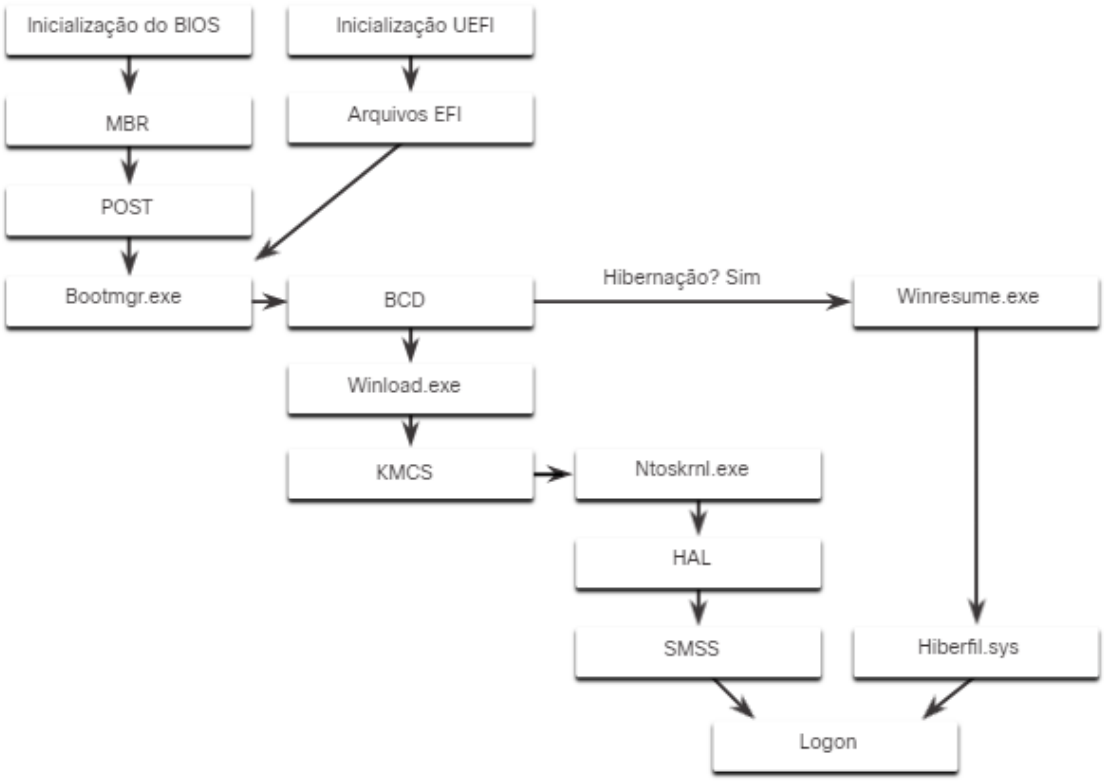
- Os dados que o arquivo possui são armazenados no atributo **$DATA**, conhecido como **fluxo de dados**
- Utilizando NTFS é possível conectar fluxo de dados alternativos (ADSs) ao arquivo.
    - As vezes é utilizado por aplicativos que estão armazenando informações adicionais sobre o arquivo.

    - ADS é um fator importante quando se trata de malwares.
        - Ocorre por ser fácil ocultar dados em um ADS
        - Um invasor pode armazenar dados dentro de um ADS que pode ser chamado por um arquivo diferente.

- Em um NFTS, um arquivo ADS é identificado por ADS após dois pontos: Testfile.txt:ADS

Processo de Inicialização do Windows

Processo de inicialização do windows:



Existem dois tipos de firmware de computador:

- **Sistema básico de entrada-saída (BIOS)** - Criado no início da década de 1980, já nao suporta todos os novos recursos solicitados pelos usuários.
- **UEFI (Unified Extensible Firmware Interface)** - Projetado para substituir a BIOS e suportar novos recursos

Na BIOS, o processo começa com a fase de inicialização da BIOS

- Ocorre quando os dispositivos são inicializados e um POST (Power On Self-Test) é executado para garantir que todos os dispositivos estejam se comunicando.
    - Quando o disco do sistema é descoberto, o POST termina.
    - A última instrução do POST é procurar o registro mestre de inicialização (MBR)

- A MBR possui um programa responsável por localizar e carregar o Sistema Operacional

O firmware UEFI tem mais visibilidade sobre o processo de inicialização.

- Começa carregando arquivos de programa EFI, armazenados como arquivos.efi em uma partição de disco especial, conhecida como EFI System Partition (ESP).

Nota: Um computador que usa UEFI armazena o código de inicialização no firmware.

- Ajuda a aumentar a segurança do computador pois o computador entra em modo protegido

Depois que uma instalação válida do Windows é detectada o arquivo **Bootmgr.exe** é executado.

- **Bootmgr.exe** alterna o sistema do modo real para o modo protegido para que toda a memória do sistema possa ser usada.
- **Bootmgr.exe** lê o Banco de Dados de Configuração de Inicialização (BCD).
    - O BCD contém qualquer código adicional necessário para iniciar o computador, bem como informa se o computador está saindo de hibernação ou arranque frio.
    - Se o computador estiver saindo da hibernação, o processo de inicialização continuará com **Winresume.exe**.
        - Isso permite que o computador leia o arquivo **Hiberfil.sys** que contém o estado em que o computador parou.
    - Se for início frio, o arquivo **Winload.exe** será carregado.
        - O arquivo **Winload.exe** cria um registro da configuração de hardware no registro.
            - O registro é um registro de todas as configurações, opções, hardware e software do computador.
        - **Winload.exe** também usa o Kernel Mode Code Signing (KMCS) para garantir que todos os drivers sejam assinados digitalmente.
            - Isso garante que os drivers sejam seguros para iniciar.

Depois que os drivers forem examinados, o winload.exe executado, Ntoskrnl.exe iniciado o kernel, o subsistema do Gestor de Sessões (SMSS) lê o registo para criar o ambiente do utilizador, iniciar o serviço Winlogon e preparar a área de trabalho.

Inicialização do Windows

Há dois itens importantes em registro utilizados para iniciar automaticamente aplicativos e serviços:

- **HKEY\ _LOCAL\ _MACHINE** - configurações do Windows, incluindo informações sobre serviços que começar na inicialização.
- **HKEY\ _CURRENT\ _USER** - Aspectos do usuário conectado, incluindo serviços que só iniciar com o logon.

Entradas diferentes informam como os serviços e aplicativos serão iniciados.

- Esses tipos incluem Run, RunOnce, RunServices, RunServicesOnce e Userinit.
    - Essas entradas podem ser inseridas manualmente mas é melhor utilizar o **msconfig.exe**
        - Essa ferramenta é usada para alterar as opções de inicialização do PC.
            - Existem 5 guias:
                - Geral
                - Inicialização do Sistema
                - Serviços
                - Startup

Desligamento do Windows

O computador precisa de tempo para fechar cada aplicativo, desligar cada serviço e registrar quaisquer alterações de configuração antes de qualquer desligamento, para não perder as configuraçções de serviços e aplicativos.

No desligamento, primeiro são fechados os programas do usuário, seguido pelo kernel.

- Se as aplicações do modo usuário demorarem, aparecerá uma janela para aguardar ou forçar encerramento.
- Se as aplicações do kernel não responderem, o desligamento irá travar e talvez será necessário desligar o computador no botão.

O Windows pode ser desligado com o comando **shutdown** ou pelo **Ctrl+Alt+Delete**

Processos, Threads e Serviços