Frameworks de Resposta a Incidentes
• ABNT ISO/IEC 27035:2023 - Gestão de incidentes de segurança da informação
ü ABNT ISO/IEC 27001 e 27002 - Estabelecer, implementar, manter e melhorar um sistema de gestão de segurança da informação
• SANS Incident Handler's Handbook
• NIST Cybersecurity Framework (versão 2)
• NIST Special Publication 800-61 (rev. 2) – Computer Security Incident Handling
• NIST Special Publication 800-61 (rev.
Recommendations and Considerations
Management
3) – Incident Response
for Cybersecurity Risk
ü NIST Special Publication 800-86 - Guide to Integrating Forensic Techniques into Incident Response

Frameworks de Resposta a Incidentes
ABNT ISO/IEC 27035 – Gestão de Incidentes de Segurança da Informação
1) Planejar e Preparar (Plan & Prepare)
2) Identificar, Detectar e Comunicar
(Identify, Detect & Report)
3) Avaliar e Decidir (Assessment &
Detection)
4) Responder (Reponse)
5) Lições Aprendidas (Lessons Learnt)

Frameworks de Resposta a Incidentes
SANS Incident Handler's Handbook
1) Preparação (Preparation)
2) Identificação (Identification)
3) Contenção (Containment)
4) Erradicação (Eradication)
5) Recuperação (Recovery)
6) Lições Aprendidas (Lessons Learned)

Frameworks de Resposta a Incidentes
NIST Cyber Security Framework versão 2.0
1) Governança (Govern)
2) Identificar (Identify)
3) Proteger (Protect)

4) Detectar (Detect)
5) Responder (Respond)
6) Recuperar (Recover)

Frameworks de Resposta a Incidentes
NIST SP 800-61r2 – Computer Security Incident Handling
1) Preparação (Preparation)
2) Detecção e Análise
(Detection & Analysis)
3) Contenção, Erradicação e
Recuperação (Containment,
Eradication & Recovery)
4) Atividades Pós-Incidentes
(Post-Incident Activity)

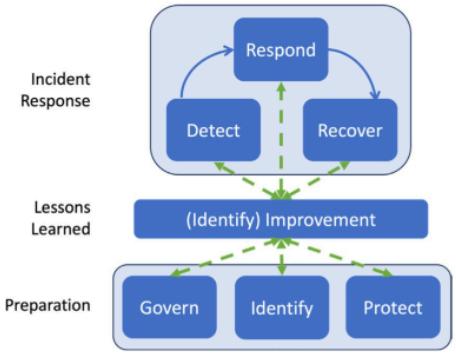
Frameworks de Resposta a Incidentes
• Comparativo dos frameworks de Resposta a Incidentes

<table>
<tr><th>ABNT ISO 27035</th><th>SANS</th><th>NIST CSF 2</th><th>NIST SP 800-61r2</th></tr>
<tr><td rowspan="2">Planejar e Preparar</td><td rowspan="2">Preparation</td><td>Identify</td><td rowspan="2">Preparation</td></tr>
<tr><td>Protect</td></tr>
<tr><td>Detectar e Comunicar</td><td rowspan="2">Identification</td><td rowspan="2">Detect</td><td rowspan="2">Detect and Analysis</td></tr>
<tr><td>Avaliar e Decidir</td></tr>
<tr><td rowspan="3">Responder</td><td>Containment</td><td rowspan="2">Respond</td><td rowspan="3">Containment, Eradication & Recovery</td></tr>
<tr><td>Eradication</td></tr>
<tr><td>Recovery</td><td rowspan="2">Recover</td></tr>
<tr><td>Lições aprendidas</td><td>Lessons Learned</td><td>Post-Incident Activity</td></tr>
</table>

Fases de Resposta a Incidentes
NIST SP 800-61 rev.3
• Baseado no CSF 2.0

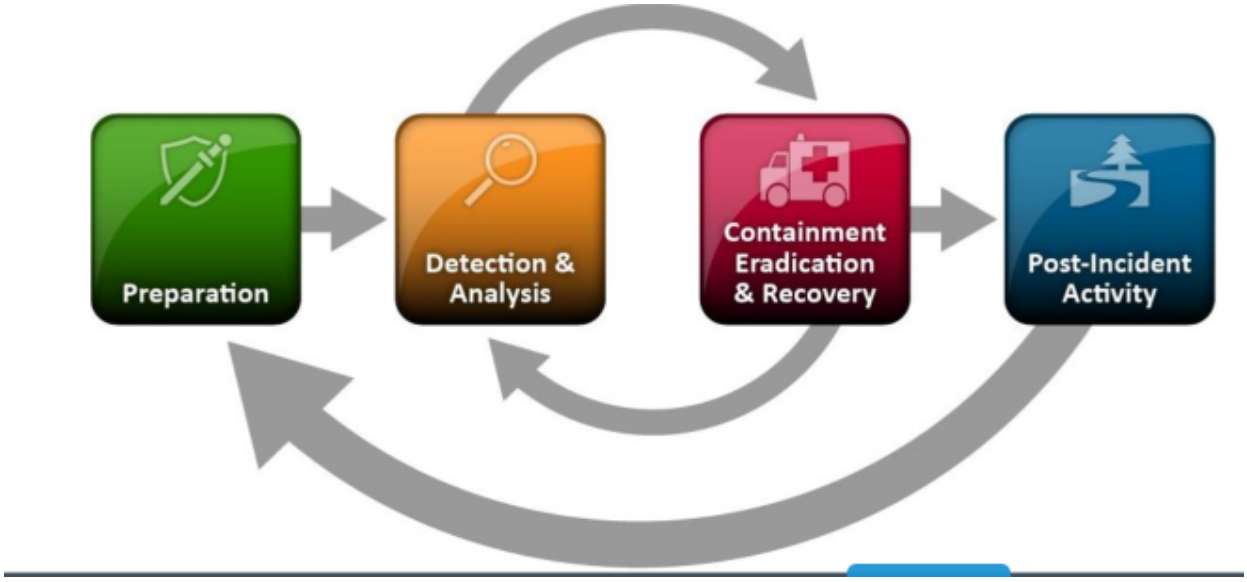
NIST SP 800-61 rev.3

- **Baseado no CSF 2.0**



Previous Incident Response Life Cycle Phase	CSF 2.0 Functions
Preparation	Govern Identify (all Categories) Protect
Detection & Analysis	Detect Identify (Improvement Category)
Containment, Eradication & Recovery	Respond Recover Identify (Improvement Category)
Post-Incident Activity	Identify (Improvement Category)

Fases de Resposta a Incidentes
1 – Preparação
2 – Detecção e Análise
3 – Contenção, Erradicação e Recuperação
4 – Atividades Pós-incidente



Fases de Resposta a Incidentes
1 – Preparação
1.Selecionar Frameworks de Respostas a Incidentes (NIST SP 800-61r2, ABNT ISO/IEC 27035:2023, SANS
Incident Handler's Handbook, NIST CSF v2)
2.Selecionar Frameworks de Perícia Digital (NIST SP 800-86)
3.Criar e aprovar a Política de Resposta a Incidentes e o respectivo plano (RFC 2350)
4.Mapear ativos e efetuar uma Análise de Riscos (NIST SP 800-30r1)

5.Criar o Plano de Continuidade de Negócios e de Recuperação de Desastres (NIST SP 800-34r1)
6.Estabelecer critérios de priorização de incidentes
7.Estabelecer linhas de comunicação e protocolos de notificação
8.Designar e capacitar as equipes de resposta a incidentes
9.Alocar recursos (pessoal, treinamento, equipamentos, aplicativos, ...)
10. Realizar campanhas de conscientização dos membros da organização sobre segurança cibernética e
privacidade (NIST SP 800-50r1)
11. Realizar testes, treinamentos e exercícios (NIST 800-84)
12. Aplicar Frameworks de Controles Preventivos (CIS, ISO 27001, NIST SP 800-53r5) e melhores práticas

Fases de Resposta a Incidentes
2 – Detecção e Análise
• Coletar e centralizar logs (SIEM)
• Criar baselines e identificar anomalias (sinais precursores ou indicadores)
• Implementar sistemas de monitoramento de rede e detecção/prevenção de intrusão(IDS/IPS)
• Analisar registros de segurança, logs de eventos e outras fontes de dados
• Identificar indicadores de comprometimento (IoCs) e indicadores de comportamento (IoBs)
• Avaliar do impacto do incidente na organização e categorizar/priorizar o incidente
• Declarar quando um incidente ocorrer e notificar as pessoas/áreas responsáveis

Fases de Resposta a Incidentes
2 – Detecção e Análise
• Recomendações para identificar incidentes (devem ser implementados na fase de Preparação):
ü Criar perfis de rede e de sistemas
ü Entender comportamentos normais
ü Criar uma política de retenção de logs
ü Executar correlações de eventos
ü Sincronizar horários entre equipamentos (inclusive fusos horários)
ü Coletar pacotes de rede para obter dados adicionais
ü Filtrar os dados
ü Procurar ajuda de outras ETIRs da organização (se existentes) ou fora dela (https://www.cert.br/csirts/brasil/)

Fases de Resposta a Incidentes

3 – Contenção, Erradicação e Recuperação
• Iniciar a investigação preliminar do incidente
• Determinar a natureza e o escopo do incidente
• Segmentar redes ou desativar sistemas comprometidos para conter a propagação
• Implementar medidas de controle de acesso para limitar a atividade maliciosa
• Ativar firewalls adicionais ou filtros de rede para bloquear tráfego suspeito
• Suspender serviços não críticos para reduzir a superfície de ataque
• Iniciar comunicação com equipes de resposta a incidentes para coordenar esforços de contenção
• Coletar e preservar evidências digitais para análise forense

Fases de Resposta a Incidentes
3 – Contenção, Erradicação e Recuperação
• Identificar as vulnerabilidades exploradas
• Monitorar as TTPs utilizadas pelos atacantes
• Aplicar patches de segurança e atualizações para corrigir as vulnerabilidades identificadas
• Utilizar ferramentas de remoção de malware para limpar sistemas comprometidos
• Eliminar arquivos e processos maliciosos identificados durante a análise forense
• Reinicializar e restaurar serviços essenciais afetados pelo incidente
• Verificar a integridade e a funcionalidade dos sistemas restaurados antes de retorná-los ao ambiente de produção

Fases de Resposta a Incidentes
3 – Contenção, Erradicação e Recuperação
• Identificar backups limpos e confiáveis
• Avaliar a atualização das Gold Images
• Reforçar políticas de segurança, configurações de firewall e controles de acesso
• Revisar e atualizar processos de backup e recuperação para evitar futuros incidentes
• Realizar testes de penetração e avaliações de vulnerabilidade para verificar a eficácia das medidas de recuperação
• Monitorar continuamente os sistemas restaurados para detectar e responder rapidamente a quaisquer anomalias ou atividades suspeitas

Fases de Resposta a Incidentes
4 – Atividades Pós-incidente
• Documentar e revisar o incidente
• Determinar suas causas raiz e impacto
• Identificar falhas nos processos, tecnologias ou práticas de segurança
• Documentar as lições aprendidas e recomendações para melhorias
• Atualização de políticas, procedimentos e controles de segurança com base nas lições aprendidas

• Compartilhamento de informações sobre o incidente e as medidas corretivas tomadas com partes interessadas relevantes
• Posteriormente, revisar se as recomendações foram implementadas (principalmente para incidentes graves)
• Se ocorrerem mudanças significativas na organização ou no cenário de ameaças, refazer a análise de risco

Estrutura de Resposta a Incidentes
• Nomenclaturas das equipes de Resposta a Incidentes:
ü ETIR – Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais
ü IRT – Incident Response Team
ü CSIRT – Computer Security Incident Response Team
ü CERT – Computer Emergency Response Team
ü CTIR – Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos
ü CLRI – Comissão Local de Resposta a Incidentes de Segurança da Informação
ü GRA – Grupo de Resposta a Ataques
• Nenhuma equipe de resposta a incidentes é idêntica a outra

Estrutura de Resposta a Incidentes
• Modelos das equipes:
ü Centralizada – uma única ETIR gerencia os incidentes de segurança da informação em toda organização.
ü Distribuída – existem várias ETIRs, cada uma responsável por um segmento lógico ou físico da organização. Deve haver coordenação entre as equipes. Ex: ETIR da região sul; ETIR do financeiro.
ü Coordenada – uma ETIR assessora outros times sem ter autoridade sobre eles (uma ETIR para ETIRs). Normalmente composto por membros com mais experiência.

Estrutura de Resposta a Incidentes
• Modelos de formação dos times:
ü Funcionários próprios – funcionários da organização fazem toda resposta a incidentes.
ü Parcialmente terceirizado – parte da resposta a incidentes é terceirizado. Geralmente se terceiriza o monitoramento 24/7 para um Managed Security Services Provider (MSSP), que reporta para a ETIR da organização.
ü Totalmente terceirizado – toda resposta a incidentes é terceirizada, sendo supervisionado por pelo menos um funcionário da organização.

Estrutura de Resposta a Incidentes
EQUIPES
• Uma pessoa responsável pela gestão, com um ou mais substitutos:
ü Interface com a alta administração, outros times e outras organizações

ü Desarmar incidentes
ü Garantir que cada time tenha pessoal, recursos e capacitação necessários
• Uma pessoa responsável pela área técnica (opcional):
ü Deve ter muita experiência e conhecimentos técnicos
ü Pode atuar em mais de uma equipe
ü Não é necessariamente o responsável pela resposta ao incidente

Estrutura de Resposta a Incidentes
EQUIPES
• Membros da ETIR:
ü Conhecimentos técnicos (administração de redes e sistemas, programação, perícia, análise de malware, segurança, ...)
ü Resolução de problemas e pensar fora da caixa
ü Deve haver preocupação com burnout (possibilitar outras atividades, crescimento de carreira, mentoria, ...)
ü Capacitação constante e testes periódicos

Estrutura de Resposta a Incidentes
• Pontos a se levar em conta para estruturação da ETIR e seleção dos seus integrantes:
ü Necessidade de atuação 24/7
ü Dedicação exclusiva X Dedicação parcial
ü Moral dos funcionários
ü Custos
ü Experiência da equipe
ü Divulgação de informações sensíveis para terceiros

Estrutura de Resposta a Incidentes
• Pontos a se levar em conta para terceirização da ETIR :
ü Qualidade à Avaliar o esforço da Contratada em manter a qualidade dos trabalhos atuais e melhoria para ações futuras
ü Divisão de responsabilidades à avaliar se será delegada à Contratada a tomada de decisões sobre o ambiente (desligar servidores, interromper rede, ...) e documentar quais são os limites
ü Acesso a informações sensíveis à dividir responsabilidades, restringindo acesso a informações pela Contratada: por exemplo, a Contratada identifica que a Matrícula X causou o incidente, mas não sabe quem é o funcionário, e a Contratante continua com a investigação
ü Falta de informações sobre a contratante à a análise e priorização de incidentes exigem conhecimento profundo sobre o ambiente tecnológico da Contratante, que deve fornecer documentação correta e atualizada constantemente
Estrutura de Resposta a Incidentes

ü Falta de correlação à a correlação entre múltiplas fontes de dados é muito importante: por exemplo, se o atacante tenta acessar o servidor web, mas a Contratada não tem acesso a esses logs, não pode saber o resultado do ataque – uma solução seria ter acessos administrativos sob demanda, mas haverá aumento de custos para gerenciamento
ü Gerenciando incidentes em várias localizações à muitos casos de resposta a incidentes demandam a presença física na Contratante, com isso deve-se avaliar o tempo e o custo de deslocamento até suas dependências
ü Mantendo conhecimentos de resposta a incidentes dentro da Contratante à empresas que terceirizam totalmente a resposta a incidentes devem manter conhecimento básico na Contratante, pois é possível que o ataque interrompa o acesso da Contratante à Contratada, então a Contratante deve estar preparada para um processo de resposta básica de incidentes

Categorias de Incidentes
• Existem vários critérios que podem ser utilizados para categorização de incidentes, tais como:
ü Impacto
ü Severidade
ü Complexidade do incidente
ü Ameaça
ü Vetores de Ataque
• A European Union Agency For Cybersecurity – ENISA, criou uma taxonomia de Classificação de Incidentes e está disponível em:
ü https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

Categorias de Incidentes

INCIDENT CLASSIFICATION	INCIDENT EXAMPLES	DESCRIPTION
Abusive Content	Spam	or "Unsolicited Bulk Email", this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content
	Harmful Speech	Discreditation or discrimination of somebody (e.g. cyber stalking, racism and threats against one or more individuals)
	Child/Sexual/Violence/ ...	Child pornography, glorification of violence, ...
Malicious Code	Virus	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
	Worm	
	Trojan	
	Spyware	
	Dialler	
	Rootkit	
Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This includes also some kind of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...), port scanning.
	Sniffing	Observing and recording of network traffic (wiretapping).
	Social engineering	Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).

Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This includes also some kind of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...), port scanning.
	Sniffing	Observing and recording of network traffic (wiretapping).
	Social engineering	Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).
Intrusion Attempts	Exploiting known vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (e.g. buffer overflow, backdoor, cross site scripting, etc.).
	Login attempts	Multiple login attempts (Guessing / cracking of passwords, brute force).
	New attack signature	An attempt using an unknown exploit.
Intrusions	Privileged account compromise	A successful compromise of a system or application (service). This can have been caused remotely by a known or new vulnerability, but also by an unauthorized local access. Also includes being part of a botnet.
	Unprivileged account compromise	

Availability	DoS	By this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. DoS examples are ICMP and SYN floods, Teardrop attacks and mail-bombing. DDoS often is based on DoS attacks originating from botnets, but also other scenarios exist like DNS Amplification attacks. However, the availability also can be affected by local actions (destruction, disruption of power supply, etc.) – or by Act of God, spontaneous failures or human error, without malice or gross neglect being involved.
	DDoS	
	Sabotage	
	Outage (no malice)	
Information Content Security	Unauthorised access to information	Besides a local abuse of data and systems the information security can be endangered by a successful account or application compromise. Furthermore, attacks are possible that intercept and access information during transmission (wiretapping, spoofing or hijacking). Human/configuration/software error can also be the cause.
	Unauthorised modification of information	
Fraud	Unauthorized use of resources	Using resources for unauthorized purposes including profit-making ventures (E.g. the use of e-mail to participate in illegal profit chain letters or pyramid schemes).
	Copyright	Offering or Installing copies of unlicensed commercial software or other copyright protected materials (Warez).
	Masquerade	Type of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it.
	Phishing	Masquerading as another entity in order to persuade the user to reveal a private credential.
Vulnerable	Open for abuse	Open resolvers, world readable printers, vulnerability apparent from Nessus etc scans, virus signatures not up-to-date, etc

Categorias de Incidentes

• Uma categorização de incidentes (não só de segurança da informação) muito utilizada usa como parâmetro a ameaça. Exemplos:

ü Incidente de Desastre Natural
ü Incidente de Tumulto Social
ü Incidente de Dano Físico
ü Incidente de Falha de Infraestrutura
ü Incidente de Falha Técnica
ü Incidente de Malware
ü Incidente de Ataque Técnico
ü Incidente de Violação de Regra
ü Incidente de Conteúdo Nocivo
ü Outros Incidentes

Categorias de Incidentes

• Outra categorização de incidentes utiliza o Vetor de Ataques.

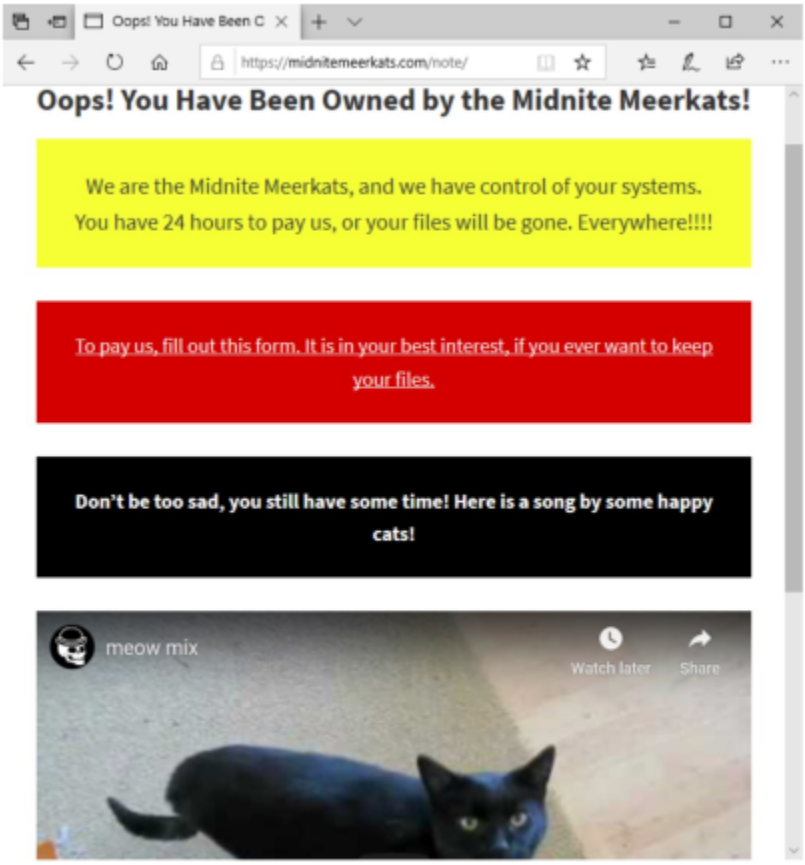
• A utilização de uma nomenclatura padrão para os vetores de ataque é fundamental para que as equipes de Resposta a Incidentes e as várias áreas envolvidas da organização possam se comunicar adequadamente

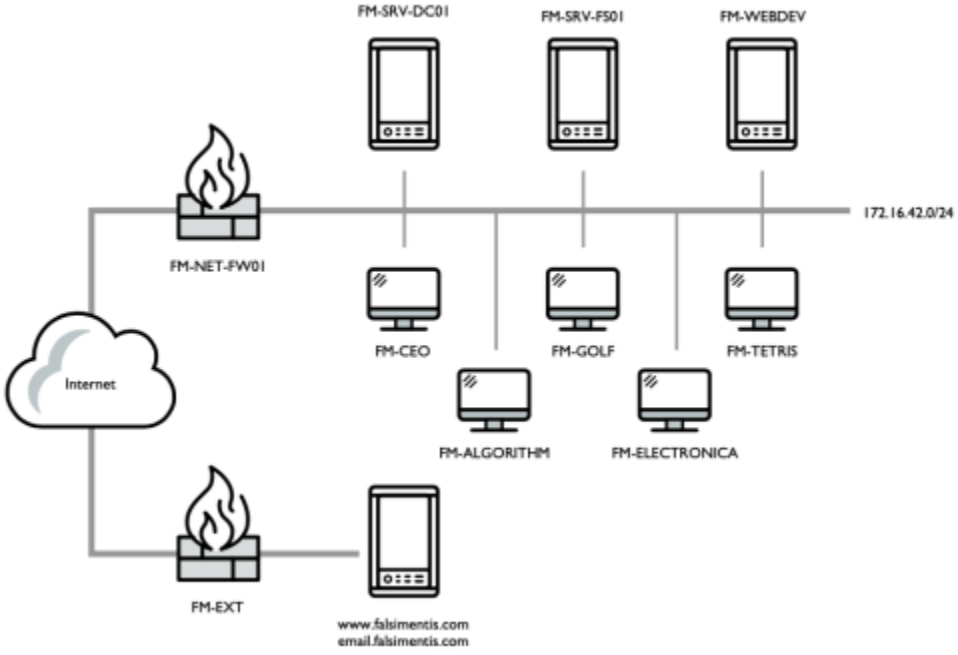
Vetor de Ataque	Descrição	Exemplo
E-mail	Ataque executado através de uma mensagem de e-mail	Malware disfarçado de documento anexo ou link para um site malicioso
Periférico ou mídia removível	Ataque executado de uma mídia removível ou periférico	Código malicioso que se espalha através de um pendrive infectado
Personificação ou Spoofing	Um ataque envolvendo substituição de conteúdo ou serviço legítimos por um substituto malicioso	Spoofing, man in the Middle, roque wireless access point e SQL Injection são ataques que envolvem personificação
Uso impróprio	Um incidente resultante de violação da política de uso aceitável da organização por um usuário autorizado, desde que não esteja em uma das categorias acima	O usuário instala um aplicativo de compartilhamento de arquivos, levando ao vazamento de dados sensíveis, ou o usuário executa atividades ilegais em um sistema
Perda ou roubo de equipamento	A perda ou roubo de dispositivos computacionais ou mídias utilizadas pela organização	Um laptop ou celular perdidos
Outros	Um método de ataque que não se enquadra em nenhuma das categorias acima	

Incidente Cibernético

Incidente
• Empresa Falsimentis, localizada em Los Angeles, Califórnia, nos Estados Unidos
• Fábrica de Software para aplicações do setor hospitalar.
• O CEO saiu para o almoço, por volta das 11:50 AM, horário local de Los Angeles, travando o computador do trabalho antes de sair.
• Ao retornar, por volta das 01:05 PM, o CEO percebeu que seu computador foi reiniciado.
• Ao se autenticar, tinha uma mensagem exibida pelo navegador.
• A mensagem era uma notificação de um grupo de ransomware que se auto intitulava de Midnite Meerkats.
•
A mensagem informava que a máquina e outras da rede foram cifradas e, para recuperar, tinha que ser feito um pagamento em até 24hrs.

Incidente
https://midnitemeerkats.com/note/


Oops! You Have Been C
https://midnitemeerkats.com/note/
Oops! You Have Been Owned by the Midnite Meerkats!
We are the Midnite Meerkats, and we have control of your systems.
You have 24 hours to pay us, or your files will be gone. Everywhere!!!!
To pay us, fill out this form. It is in your best interest, if you ever want to keep your files.
Don't be too sad, you still have some time! Here is a song by some happy cats!
meow mix
Watch later
Share


FM-SRV-DC01
FM-SRV-FS01
FM-WEBDEV
172.16.42.0/24
FM-NET-FW01
FM-CEO
FM-GOLF
FM-TETRIS
Internet
FM-ALGORITHM
FM-ELECTRONICA
FM-EXT
www.falsimentis.com
email.falsimentis.com

IP	Hostname	Description
172.16.42.2	FM-SRV-DC01.falsimentis.com	Domain controller
172.16.42.3	FM-SRV-FS01.falsimentis.com	Corporate file server
172.16.42.10	FM-NET-FW01.falsimentis.com	Network firewall and Squid server
172.16.42.20	FM-WEBDEV.falsimentis.com	Internal web development server
172.16.42.103	FM-TETRIS.falsimentis.com	System administrator's workstation
172.16.42.105	FM-ELECTRONICA.falsimentis.com	Web developer's workstation
172.16.42.107	FM-CEO.falsimentis.com	CEO's workstation
172.16.42.108	FM-ALGORITHM.falsimentis.com	V.P. of Operations' workstation
172.16.42.109	FM-GOLF.falsimentis.com	An engineer's workstation

The publicly accessible Falsimentis systems are as follows:

IP	Hostname	Description
52.219.120.171	www.falsimentis.com (http://www.falsimentis.com)	Public website

IP	Hostname	Description
52.219.120.171	email.falsimentis.com	Webmail client (on same server as www)
10.5.96.4	n/a	Private IP address of the server hosting the public website
144.202.115.64	fm-ext.falsimentis.com	Firewall and VPN server
10.5.96.3	n/a	The private IP address of the firewall and VPN server

CTF

Incidente

• O CEO travou o computador por volta das 11:05 AM e foi almoçar.
• O CEO retornou do almoço por volta das 01:05 PM.
• Ao se autenticar na máquina, o CEO viu a mensagem de ransomware.
• A mensagem estava hospedada em https://midnitemeerkats.com/note
• A empresa tinha que fazer um pagamento nas próximas 24hrs.
• Sistema inicialmente comprometidos:

ü 172.16.42.107 (FM-CEO)