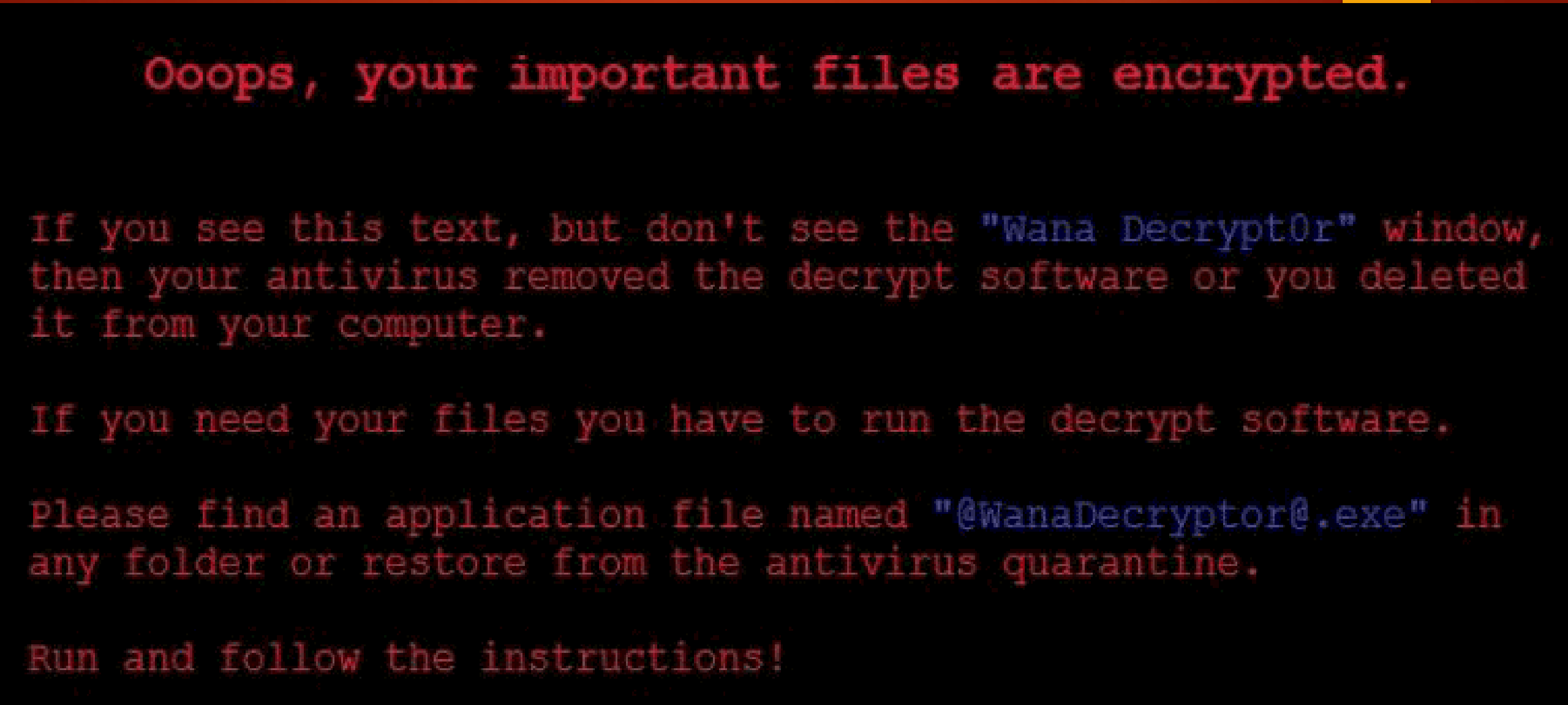
A ERA DOS CRYPTO RANSOMWARES: UM ESTUDO DE CASO SOBRE O WANNACRY



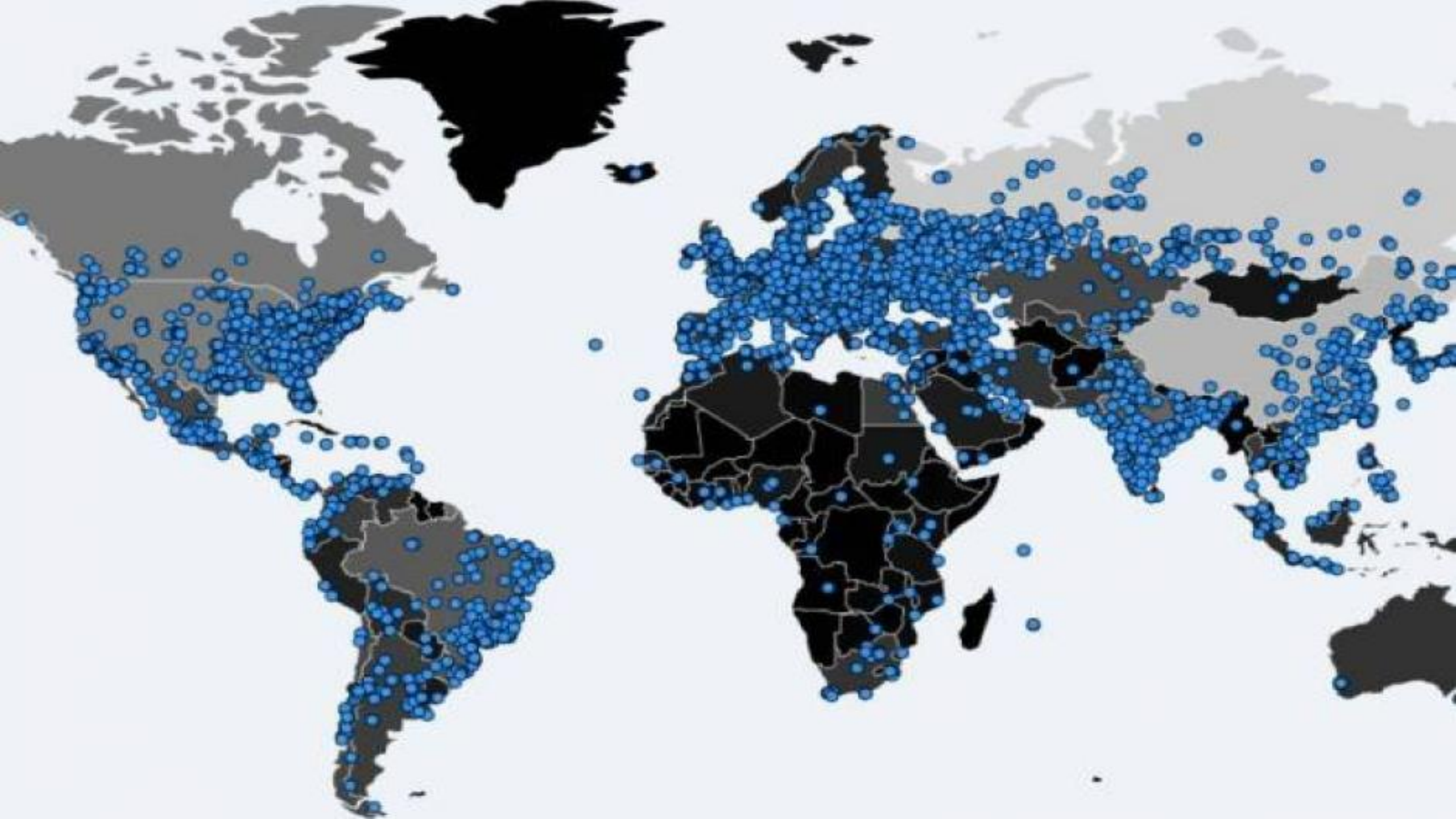
Acadêmicos: Rafael Rosário e Vanessa Lucion

WannaCry

- Gerou grande impacto e pânico internacional;
- *Kill Switch*;
- Utilizou um código roubado da NSA;
- Levou a Microsoft a desenvolver, extraordinariamente, atualizações para o Windows XP;
- Apesar do impacto, o *malware* não possui qualidades inovadoras.

```
qmemcpy(&szUrl, sinkholeddomain, 0x39u);      // previously unregistered domain, now sinkholed
v8 = 0;
v9 = 0;
v10 = 0;
v11 = 0;
v12 = 0;
v13 = 0;
v14 = 0;
v4 = InternetOpenA(0, 1u, 0, 0, 0);
v5 = InternetOpenUrlA(v4, &szUrl, 0, 0, 0x84000000, 0);// do HTTP request to previously unregistered domain
if ( v5 )                                     // if request successful quit
{
  InternetCloseHandle(v4);
  InternetCloseHandle(v5);
  result = 0;
}
else                                          // if request fails, execute payload
{
  InternetCloseHandle(v4);
  InternetCloseHandle(0);
  detonate();
  result = 0;
}
return result;
}
```

iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com



Ciclo de vida de resposta a incidentes de segurança

1º dia 12/05/2017

Identificação

a equipe de monitoração detectou um serviço estranho, o nome era um conjunto aleatório de caracteres, em um servidor virtual

a equipe contatou o responsável pelo servidor

foi detectado que o servidor estava infectado pelo *ransomware* WannaCry e a equipe de resposta a incidentes foi acionada

uma hora depois, foram confirmados 12 servidores virtuais, no mesmo segmento de rede, infectados

o sistema de prevenção de intrusão nos host (HIPS) detectaram tráfego suspeito oriundos de filias

mssecsvc2.0

1º dia 12/05/2017

Contenção

- os primeiros servidores infectados detectados faziam parte de uma mesma subrede, que foi isolada com o objetivo de conter a propagação a partir deles
- foram bloqueadas as portas exploradas pelo ransomware nas conexões com redes de filiais
- segmentos onde a TI não possuía autonomia para atuar, mas que apresentaram tráfego suspeito, foram isolados
- *hosts* não isolados, que não foram contemplados nos casos anteriores foram desligados, quando possível
- foi configurado o bloqueio da execução de binários previamente conhecidos do ransomware
- foi iniciada nova distribuição das atualizações que corrigiam as vulnerabilidades, com reinicialização obrigatória
- a primeira "vacina" foi disponibilizada pelo fornecedor de antivírus;

2º dia

Contenção

foi desconectado da rede 3 mil hosts, como medida para evitar a propagação ransomware.

3º dia

Contenção

instalado um servidor web interno e o DNS da companhia foi configurado para direcionar as chamadas as URLs do “kill switch” para este servidor

4º dia

Erradicação

foram bloqueadas as extensões do WannaCry (.WNCRY) nos servidores de arquivos

foi iniciada rotina para detecção de máquinas suspeitas/vulneráveis e tratamento

equipes de suporte local foram instruídas a aplicar os procedimentos necessários antes de religar as máquinas suspeitas

5º dia

Recuperação

foi estabelecido um fluxo padrão para autorização do desbloqueio de portas

redes de filiais foram ligadas gradativamente, na medida em que seus administradores reportavam status seguro

no processo de avaliação das redes de filiais, foram detectados vários problemas de padronização e arquitetura

Melhorias

- Estabelecer critérios e regras de detecção;
- Modelo de seleção, configuração e operação de ferramentas de monitoração;
- Colaboração e pesquisa externa para acompanhar as novidades sobre o ataque;
- Melhorar a distribuição de atualizações e pacotes de software;
- Identificar os responsáveis pelos servidores;
- Equipe de resposta a incidentes possuir mais privilégios de acesso aos hosts;
- Pessoa dedicada a documentação de todo o processo e registro.