SOC176 - RDP Brute Force Detected

Caso conduzido individualmente no simulador SOC da plataforma LetsDefend. Atuei como analista SOC N1, realizando todas as etapas de triagem, investigação, contenção e relatório.

Descrição:

Recebido alerta SOC176 referente a uma tentativa de brute-force via RDP no host "Matthew" (IP 172.16.17.148), detectado pelo SIEM.

Análise:

Em 7 de março de 2024, às 11h44, nosso SIEM gerou o alerta SOC176, sinalizando diversas tentativas de login RDP no host “Matthew”. O IP de origem 218.92.0.56 tentou autenticação utilizando diversas contas genéricas e inexistentes.

Análise de reputação do IP:
- O IP 218.92.0[.]56 apresentou reputação maliciosa pelo VirusTotal e AbuseIPDB.
- Geolocalização indica origem na China.

Foram identificados:
- 29 falhas de autenticação (Event ID 4625)
- 1 sucesso de login (Event ID 4624), às 11h45:18

Após o login bem-sucedido, o invasor executou os seguintes comandos no host:
- cmd.exe
- whoami
- net user letsdefend
- net localgroup administrators
- netstat -ano

Esses comandos indicam a tentativa do invasor de obter informações sobre o sistema, usuários e conexões de rede.

Ação tomada:

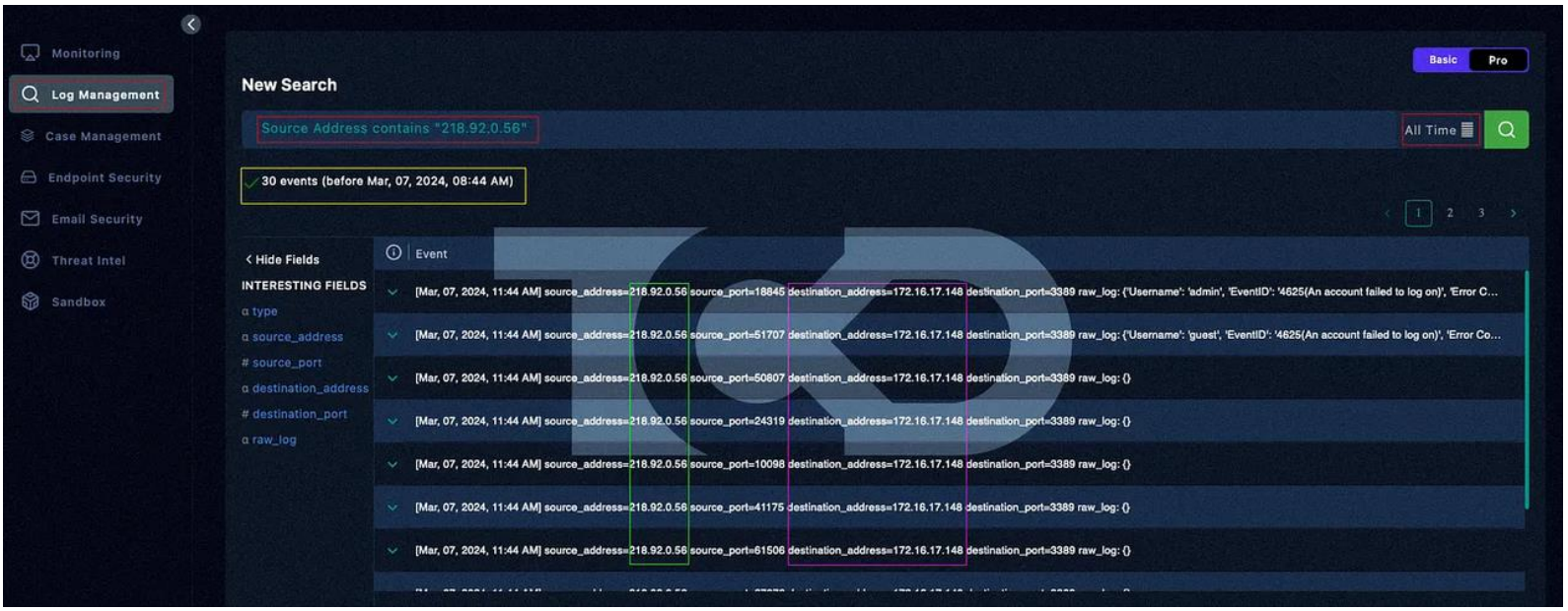
- Alerta classificado como **True Positive** após análise completa dos logs e reputação.
- Host “Matthew” foi isolado via EDR conforme playbook da LetsDefend.

Escalonamento:

Evidências foram coletadas e o incidente foi escalado para o time N2.

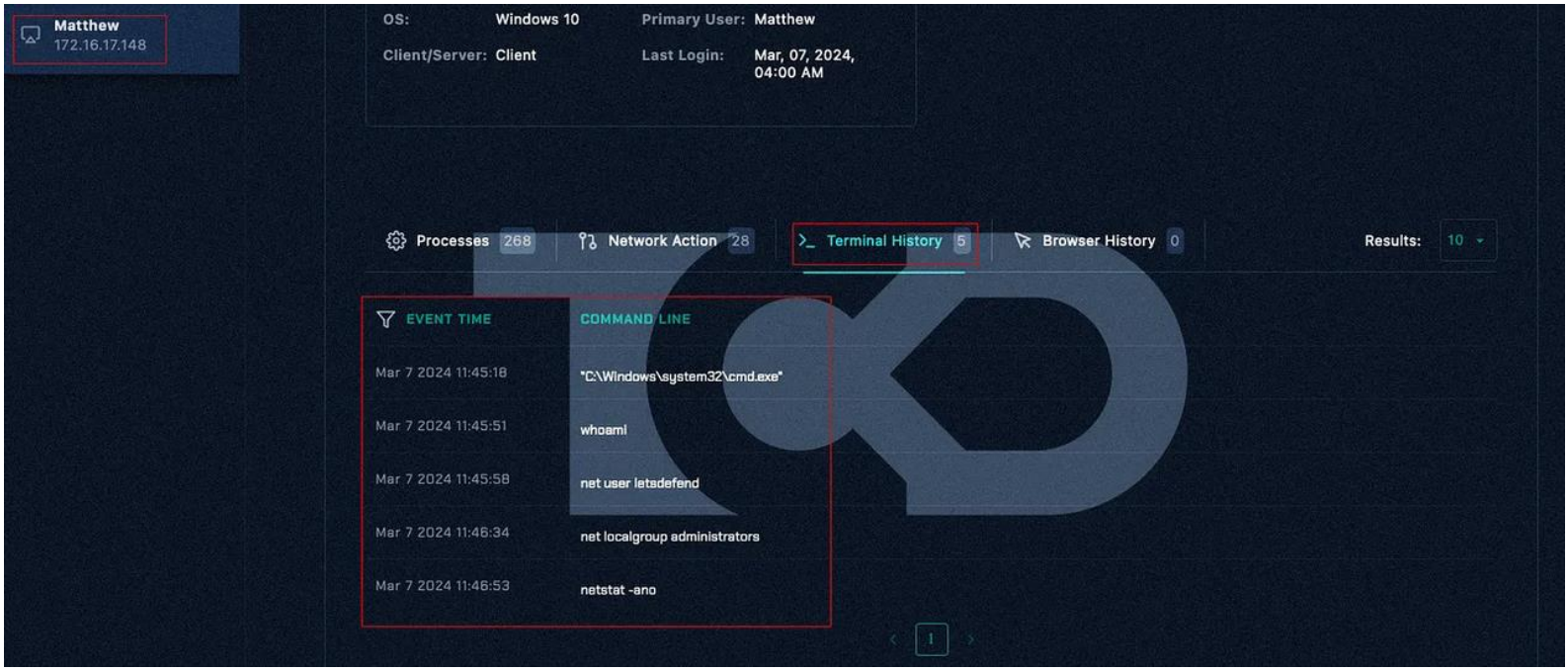
Evidências/IOC:

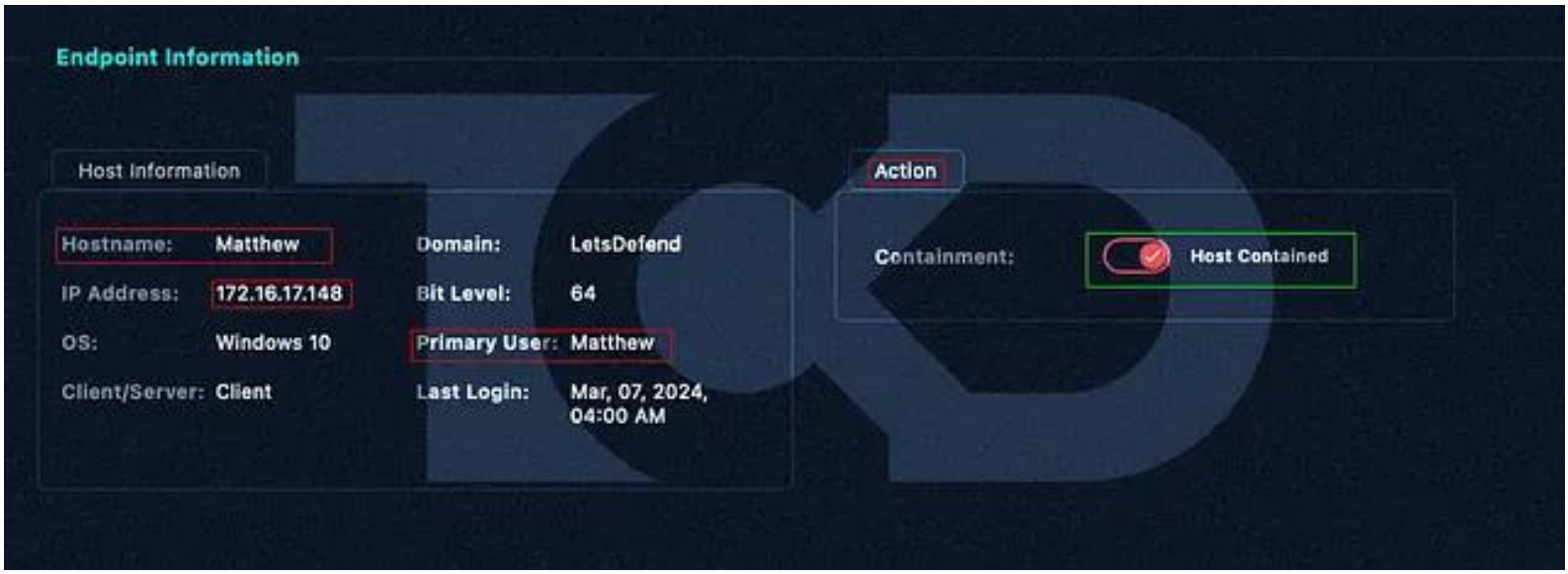
Type	Value	Description
Source IP	218.92.0.56	Source IP from China
Destination Host	172.16.17.148	Targeted host


Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
New Search
Basic
Pro
Source Address contains "218.92.0.56"
All Time
30 events (before Mar, 07, 2024, 08:44 AM)
1
2
3
Hide Fields
INTERESTING FIELDS
a type
a source_address
source_port
a destination_address
destination_port
a raw_log
Event
[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=18845 destination_address=172.16.17.148 destination_port=3389 raw_log: {'Username': 'admin', 'EventID': '4625(An account failed to log on)', 'Error C...
[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=51707 destination_address=172.16.17.148 destination_port=3389 raw_log: {'Username': 'guest', 'EventID': '4625(An account failed to log on)', 'Error Co...
[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=50807 destination_address=172.16.17.148 destination_port=3389 raw_log: {}
[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=24319 destination_address=172.16.17.148 destination_port=3389 raw_log: {}
[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=10098 destination_address=172.16.17.148 destination_port=3389 raw_log: {}
[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=41175 destination_address=172.16.17.148 destination_port=3389 raw_log: {}
[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=61506 destination_address=172.16.17.148 destination_port=3389 raw_log: {}


Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
New Search
Basic
Pro
Type contains "OS" and Source Address contains "218.92.0.56" and Raw Log contains "4624"
All Time
1 events (before Mar, 07, 2024, 08:44 AM)
1
Hide Fields
INTERESTING FIELDS
a type
a source_address
source_port
a destination_address
destination_port
a raw_log
Event
[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=31245 destination_address=172.16.17.148 destination_port=3389 raw_log: {'Username': 'Matthew', 'EventID': '4624(An account was successfully...


Hide Fields
INTERESTING FIELDS
a type
a source_address
source_port
a destination_address
destination_port
a raw_log
Event
type OS
source_address 218.92.0.56
source_port 31245
destination_address 172.16.17.148
destination_port 3389
time Mar, 07, 2024, 11:44 AM
Raw Log
Username Matthew
EventID 4624(An account was successfully logged on.)
Logon Type 10(RemoteInteractive)
Source IP 218.92.0.56
1 row selected


Matthew
172.16.17.148
OS: Windows 10
Primary User: Matthew
Client/Server: Client
Last Login: Mar, 07, 2024, 04:00 AM
Processes 268
Network Action 28
Terminal History 5
Browser History 0
Results: 10
EVENT TIME
COMMAND LINE
Mar 7 2024 11:45:18
"C:\Windows\system32\cmd.exe"
Mar 7 2024 11:45:51
whoami
Mar 7 2024 11:45:58
net user letsdefend
Mar 7 2024 11:46:34
net localgroup administrators
Mar 7 2024 11:46:53
netstat -ano


Endpoint Information
Host Information
Hostname: Matthew
IP Address: 172.16.17.148
OS: Windows 10
Client/Server: Client
Domain: LetsDefend
Bit Level: 64
Primary User: Matthew
Last Login: Mar, 07, 2024, 04:00 AM
Action
Containment:
Host Contained