```
FTP BF Chain-of-Event
=====================
10.75.7.167 (host: ctsagent01, MAC: b0:5c:da:3b:31:1f = HP maskine, OS: Windows)

03/14/2022 11:42:15 AM    ARP scan detected. AP:1
  10.75.7.167 made 200 or more ARP requests within 1.0 min. Sender's MAC address: b0:5c:da:3b:31:1f.
Targets: [00:50:56:9e:18:77 (10.75.7.109), 00:50:56:9e:52:2d (10.75.2.11),
0c:37:96:52:e1:6c (10.75.6.139), 10.75.7.66, 10.75.7.86, 10.75.8.32,
10.75.8.33, 10.75.8.34, 10.75.8.35, 10.75.8.36, 10.75.8.37, 10.75.8.38,
10.75.8.39, 10.75.8.41, 10.75.8.42, 10.75.8.43, 10.75.8.

03/16/2022 11:45:12 AM    Selective Port Scan. AP:1
  The local host 10.75.7.167 scanned at least 10 unique ports on host 10.76.8.59
in 0m5s Sample of scanned ports: 8080/tcp, 23/tcp, 22/tcp, 21/tcp,
443/tcp, 135/tcp, 80/tcp, 25/tcp, 139/tcp, 53/tcp

03/22/2022 11:56:44 AM    FTP brute force login detected. AP: 4
  10.75.7.167 had 20 failed logins on FTP server in 5m19s -

Højeste attack phase: AP 4 (Exploit)
Source IP: <client IP>
Source port: <random port number>
Destination IP: <server IP>
Destination port: <server port>

Flags: SYN = 1, ACK = 0
Sequence number: <random initial sequence number>
Acknowledgement number: 0 <We See>
<We Act>
Source IP: <server IP>
Source port: <server port>
Destination IP: <client IP>
Destination port: <          number>

Flags: RST
```

Muninn

We See. We Act.

Why choose Muninn AI Detect

- ✓ Full visibility of all activity within your network.
- ✓ Helps you to identify and fix potential vulnerabilities.
- ✓ Detects known and unknow threats in the earliest stage.
- ✓ Reduces time spent on threat investigation.
- ✓ Minimizes the alerts for false positives

AI Detect

Relying solely on basic security tools such as firewalls, endpoint security agents, and other legacy technologies is no longer adequate to detect and prevent today's sophisticated cyberattacks.

Muninn takes you to the next level of network security. Through advanced machine learning, Muninn adapts to your changing network environment, including home offices and production sites, and effectively identifies genuine threats while minimizing false positives.

AI Prevent

The lack of cybersecurity staff and the growing complexity of digital networks do not allow SOC teams to stay alert 24/7 and to act fast enough in case of an attack happening.

Muninn AI Prevent instantly mounts the most effective response to cyberthreats. Based on highly developed understanding of your organization's legitimate traffic patterns, Muninn AI Prevent can respond to novel threats that have never been seen before – buying your security teams the time they need to catch up.

Why choose Muninn AI Prevent

- ✓ Blocks attacks immediately within seconds
- ✓ No interruption of your business operations
- ✓ Able to respond around the clock and on weekends.
- ✓ Email and dashboard alerts when Muninn identifies and stops an attack
- ✓ Easy set up and configuration

Get in touch with us

www.muninn.ai

sales@muninn.ai

+45 70 60 59 08