Padrões de ataque que devem ser priorizados, no SIEM – por exemplo:

IP: 116.254.36.200 (US)

- Padrões de Ataque:
  - Path Traversal: `/../../../../windows/system32/cmd.exe`
  - Tentativas de login admin: `/admin.php?user=admin&password=admin`
- Características:
  - Múltiplos métodos (GET, POST, PATCH)
  - Alterna entre desktop e tablet

2. IP: 192.88.206.163 (US)

- Padrões de Ataque:
  - Path Traversal: `/../../../etc/passwd`, `/../../boot.ini`
  - XSS Injection: `/script.php?=<script>window.location='http://evil.com'</script>`
  - SQL Injection: `/login.jsp?user=admin'--`
  - WordPress Admin: `/wp-admin/setup-config.php`
  - Git Exposure: `/.git/config`
- Características:
  - Usa todos os tipos de dispositivos
  - Variedade de métodos HTTP

3. IP: 118.20.187.50 (US)

- Padrões de Ataque:
  - XSS: `/<img src='x' onerror='alert(1)'>`
  - Shell Command: `/shell.php?cmd=cat%20/etc/passwd`
- Características:
  - Alterna entre desktop e tablet
  - Múltiplos métodos HTTP

4. IP: 163.242.39.161 (IN)

- Padrões de Ataque:
  - XSS via PATCH: `/<img src='x' onerror='alert(1)'>`
- Características:
  - Uso incomum do método PATCH
  - Consistente no uso de desktop

5. IP: 26.158.117.152 (US)

- Padrões de Ataque:
  - XSS complexo: `/<marquee><img src=1 onerror=alert(1)></marquee>`
  - Path Traversal: `/../../../windows/win.ini`
  - Backup Files: `/config.php.bak`
- Características:
  - Usa todos os tipos de dispositivos
  - Múltiplos métodos HTTP

Estes IPs demonstram padrões mais sofisticados de ataque, incluindo:

1. Combinação de diferentes técnicas
2. Tentativas de exploração de múltiplas vulnerabilidades
3. Uso de diferentes métodos HTTP
4. Alternância entre dispositivos
5. Payloads mais elaborados