راهنمای جامع کوئری‌های Splunk برای تحلیلگران SOC

این مجموعه شامل بیش از 100 ها کوئری تخصصی Splunk است که برای تحلیلگران مرکز عملیات امنیتی (SOC) طراحی شده تا تهدیدات امنیتی را شناسایی و تحلیل کنند .پارت اول تقدیم شما می گردد

نویسنده :ابوالفضل رضی پور

hellodigi.ir

www.linkedin.com

نویسنده :ابوالفضل رضی پور

شناسایی تلاش‌های ورود ناموفق و تهدیدات احراز هویت

تلاش‌های ورود ناموفق

```
sourcetype=auth× "authentication failure" | stats count by user | sort -count
```

شناسایی کاربرانی که بیشترین تلاش‌های ورود ناموفق را داشته‌اند

تهدیدات امنیتی احتمالی

```
sourcetype=access_× method=POST status=200 | rex field=_raw
"password=(?<password>[^&]+)" | eval password_length=length(password) | where
password_length>= 8
```

بررسی درخواست‌های POSTبا رمزهای عبور طولانی

نظارت بر تلاش‌های ورود ناموفق یکی از اولین خطوط دفاعی در برابر حملات brute forceو تلاش‌های نفوذ غیرمجاز است.

نویسنده :ابوالفضل رضی پور hellodigi.ir

تشخیص تلاش‌های افزایش سطح دسترسی

1

سیستم‌های Linux

```
sourcetype=linux_secure su× | where user!=root AND user!=""
```

شناسایی تلاش‌های تغییر کاربر در سیستم‌های لینوکس

2

سیستم‌های Windows

```
sourcetype="WinEventLog:Security" EventCode=4672 | eval user_account=mvindex(Account_Name،1) | search "Security ID" NOT IN ("SYSTEM"،"LOCAL SERVICE"،"NETWORK SERVICE")
```

نظارت بر رویدادهای امنیتی ویندوز برای تشخیص افزایش دسترسی

3

استفاده از Sudo

```
sourcetype=linux_secure "sudo:" | where user!="root" AND user!=""
```

بررسی استفاده از دستورات sudoتوسط کاربران غیر root

نویسنده :ابوالفضل رضی پور hellodigi.ir

نظارت بر اتصالات SSH و تحلیل ترافیک شبکه

تلاش‌های SSH ناموفق

```
sourcetype=linux_secure "Failed password for" | stats count by src_ip | sort -count
```

شناسایی IPهایی که بیشترین تلاش‌های ورود ناموفق SSH را داشته‌اند

اتصالات SSH موفق

```
sourcetype=linux_secure "Accepted publickey for" | stats count by src_ip | sort -count
```

نظارت بر اتصالات SSH موفق از IPهای مختلف

ترافیک شبکه غیرعادی

```
sourcetype=network_traffic | stats sum(bytes) as total_bytes by src_ip, dest_ip | where total_bytes > 1000000
```

نویسنده :ابوالفضل رضی پور hellodigi.ir

شناسایی فرآیندهای مشکوک و حملات Brute Force

فرآیندهای مشکوک

```
sourcetype=processes | search "lsass.exe" OR "svchost.exe" OR "explorer.exe" | stats count by user | sort -count
```

نظارت بر فرآیندهای حساس سیستم

1

Brute Force حملات

```
sourcetype=access_* | stats count by clientip، action | where action="failure" AND count>=5
```

تشخیص تلاش‌های متعدد ورود ناموفق

2

فعالیت کاربری غیرعادی

```
sourcetype=access_* action=purchase | stats count by clientip، user | where count > 50
```

شناسایی الگوهای خرید غیرعادی

3

نویسنده :ابوالفضل رضی پور hellodigi.ir

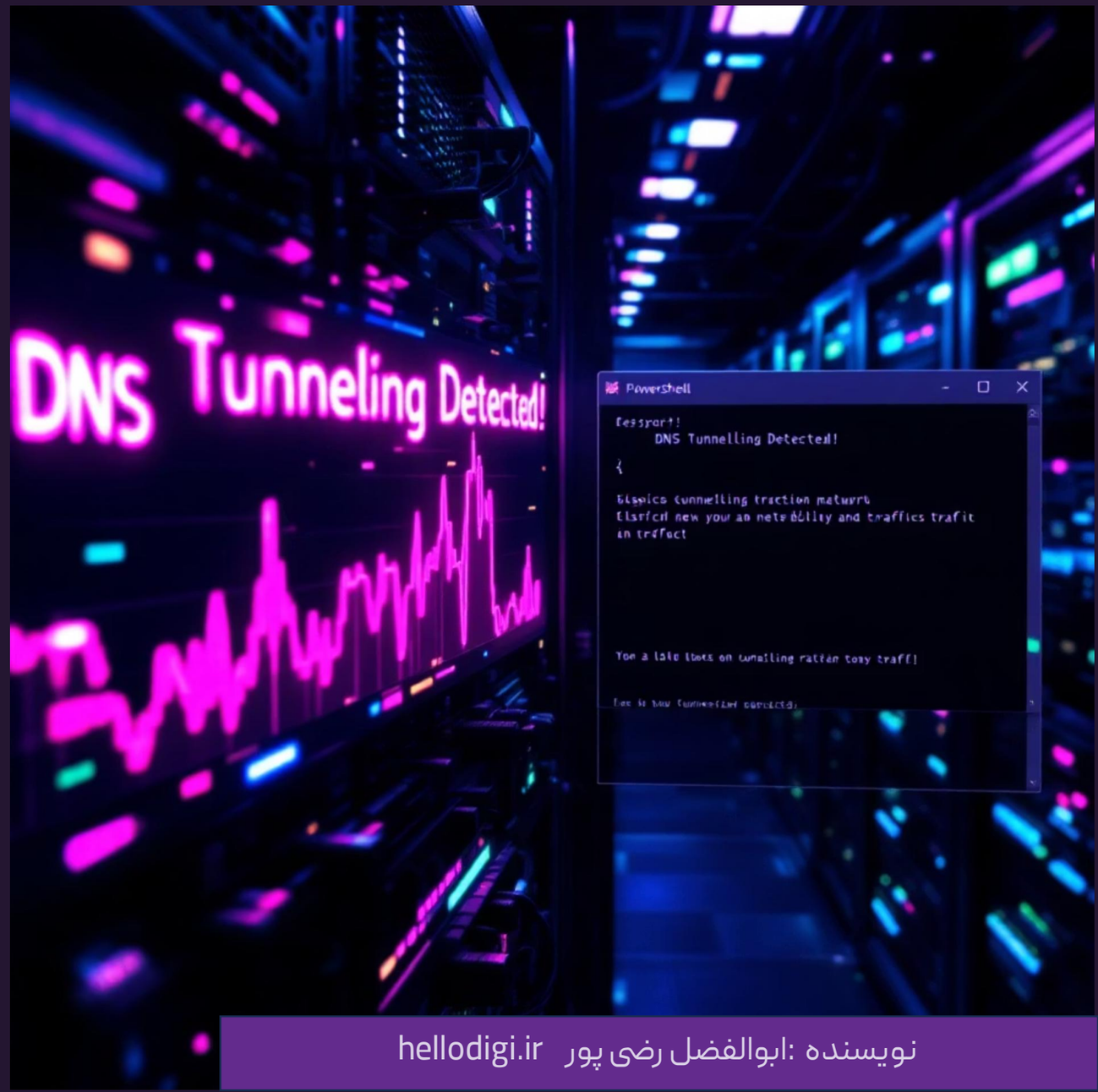
تحلیل فعالیت‌های DNS و PowerShell

DNS Tunneling

```
sourcetype=dns | rex field=answer "data"\s×:\s×"(?<data>[^"]+)"" | eval
data_length=len(data) | where data_length > 32 AND (data_length % 4) == 0
```

PowerShell مشکوک

```
sourcetype="WinEventLog:Microsoft-Windows-PowerShell/Operational"
EventCode=4103 | eval script_block=mvindex(Message، 3) | search
script_block="×Start-Process×"
```



نویسنده :ابوالفضل رضی پور hellodigi.ir

نظارت بر Port Scan و فعالیت‌های ایمیل

شبکه Port Scan

```
sourcetype=network_traffic | stats count by src_ip، dest_port | where count > 100
```

شناسایی تلاش‌های اسکن پورت

ایمیل‌های مشکوک

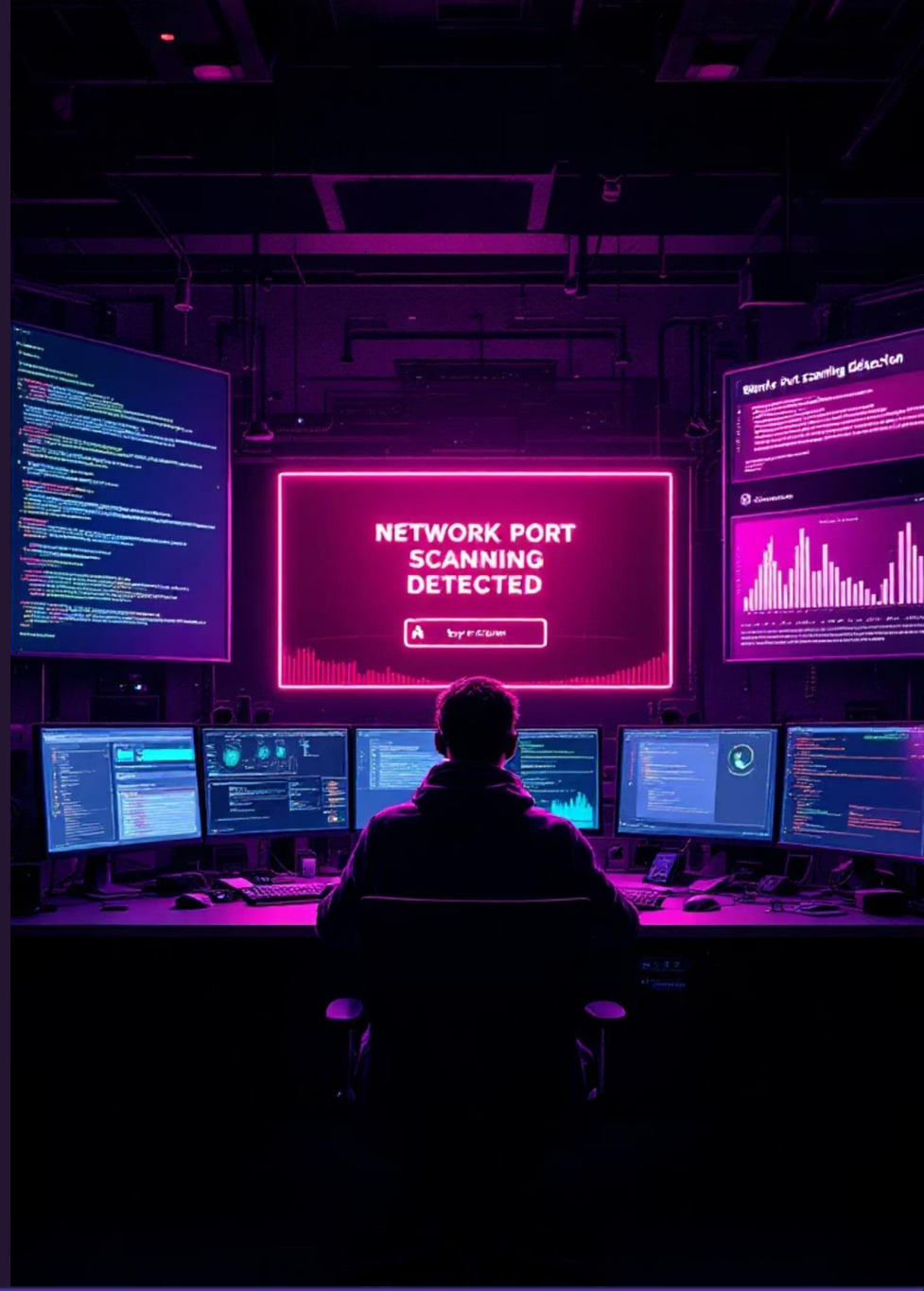
```
sourcetype=email | search "phishing" OR "malware" OR "suspicious link"
```

تشخیص ایمیل‌های فیشینگ

نشت داده احتمالی

```
sourcetype=access_* action=file_download | stats count by user، dest_ip، dest_port | where count > 10
```

نظارت بر دانلودهای مشکوک



نویسنده :ابوالفضل رضی پور hellodigi.ir

تحلیل اتصالات VPNو IPهای جدید

اتصالات VPN

- تلاش‌های VPNناموفق
- اتصالات VPNموفق
- نظارت بر IPهای جدید

```
sourcetype=access_* VPN AND action="failure"
```

```
sourcetype=access_* VPN AND action="success"
```

نویسنده :ابوالفضل رضی پور hellodigi.ir

تشخیص حملات SQL Injection و فیشینگ

SQL Injection

```
sourcetype=access_* method=POST | rex field=_raw "SELECT\s+(?<query>[^;]+)" | eval query_length=length(query) | where query_length > 50 AND query_length < 100
```

حملات فیشینگ

```
sourcetype=email | search "password" OR "reset" OR "verify" OR "login"
```

های مخرب IP

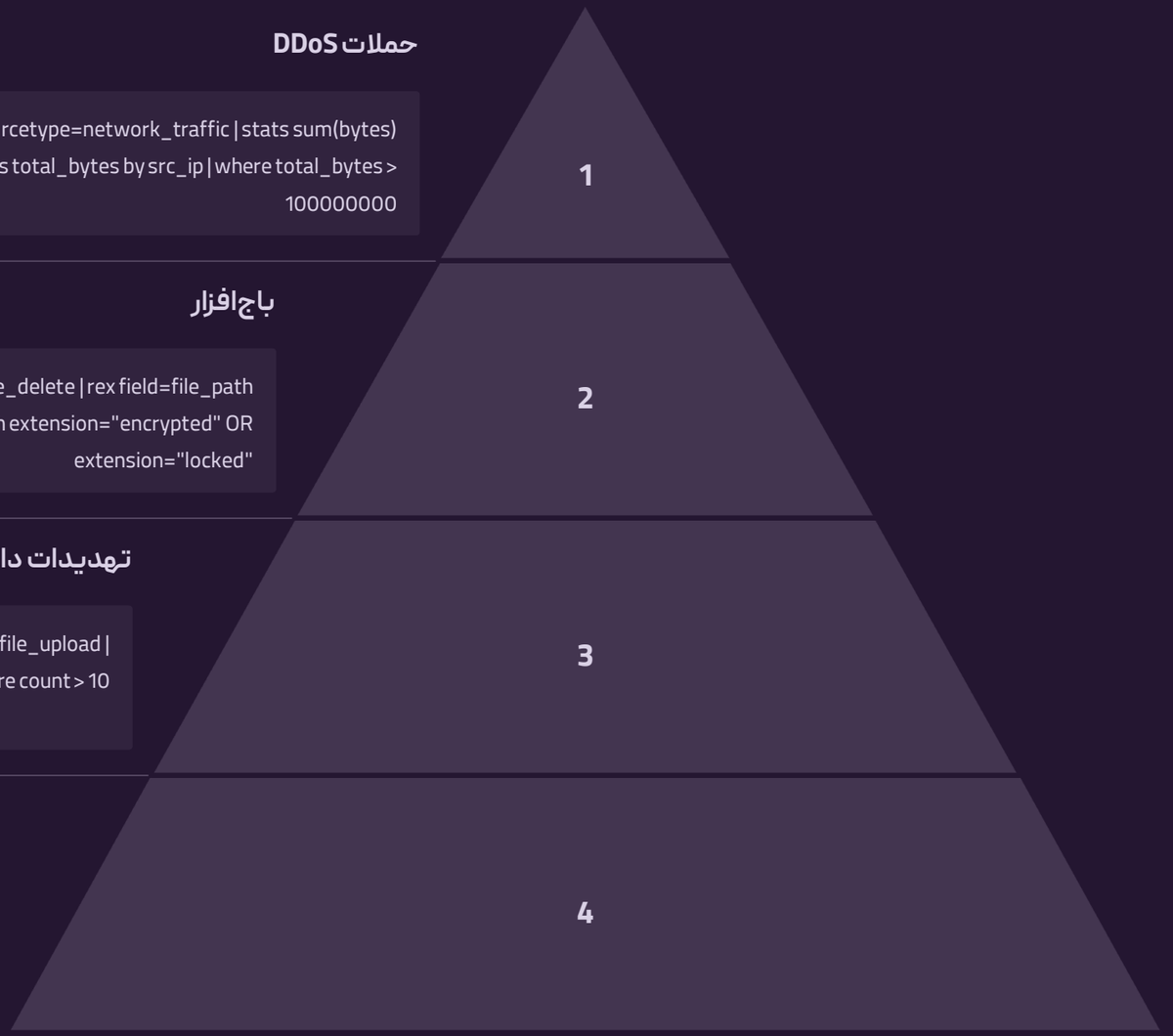
```
sourcetype=network_traffic dest_ip=malicious_ip
```

پسوندهای غیرعادی

```
sourcetype=access_* action=file_upload | rex field=file_path ".*\.(?<extension>[^.]+)" | stats count by extension | where count > 10
```

نویسنده :ابوالفضل رضی پور hellodigi.ir

حملات پیشرفته و تهدیدات داخلی



حملات DDoS

```
sourcetype=network_traffic | stats sum(bytes) as total_bytes by src_ip | where total_bytes > 100000000
```

باج‌افزار

```
sourcetype=access_* action=file_delete | rex field=file_path ".*\.(?<extension>[^.]+)" | search extension="encrypted" OR extension="locked"
```

تهدیدات داخلی

```
sourcetype=access_* action=file_upload | stats count by user، file_path | where count > 10
```

حملات Man-in-the-Middle

```
sourcetype=network_traffic protocol=tcp | stats count by dest_ip | where count > 100
```

این مجموعه کوئری‌ها ابزاری قدرتمند برای تحلیلگران SOCفراهم می‌کند تا تهدیدات امنیتی را به‌موقع شناسایی و واکنش مناسب نشان دهند .استفاده منظم از این کوئری‌ها می‌تواند سطح امنیت سازمان را به‌طور قابل‌توجهی افزایش دهد.

نویسنده :ابوالفضل رضی پور hellodigi.ir