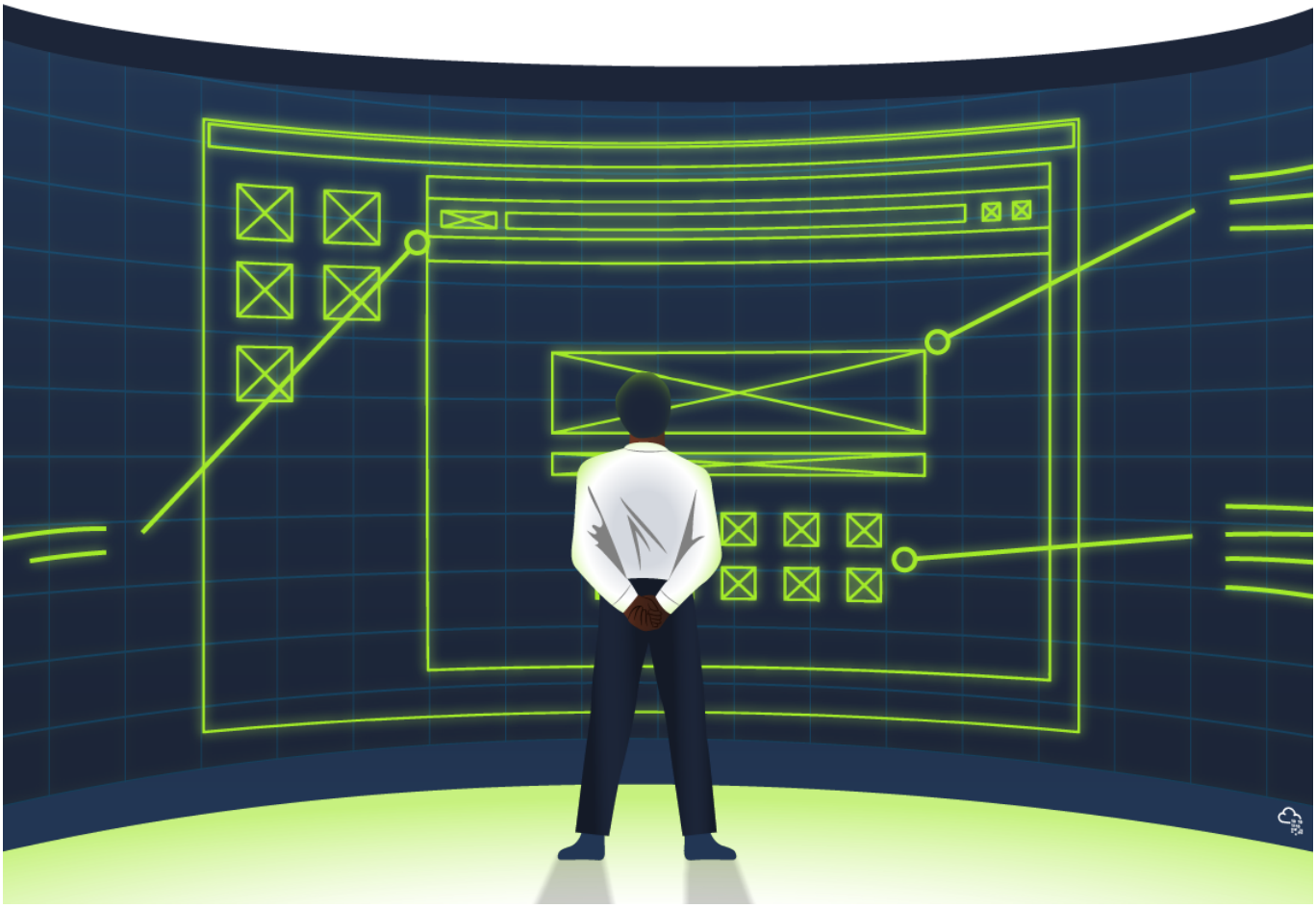
Security Engineer Log Analysis



Roles

- Security Policies
- Secure by Design
- Asset invetory, recovery, assesment and insuarance
- Awareness creation, phishing campaigns
- Managing risks, data leakage and law suits
- Change management
- Vulnerability Assesment
- Audits and compliance

Log Analysis

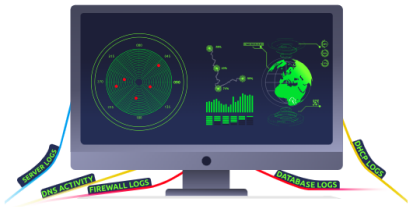
Question	Answer
What happened?	An adversary was **confirmed** to have accessed SwiftSpend Financial's GitLab instance.
When did it happen?	Access started at 22:10 on Wednesday, September 8th, 2023.
Where did it happen?	The event originated from a device with an IP address of 10.10.133.168 within the VPN Users' segment (10.10.133.0/24).
Who is responsible?	Upon examining the network logs, it was observed that the device, identified by the User-Agent "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0", was allocated the IP address 10.10.133.168.
Were they successful?	Yes, since an API Key was found to be publicly exposed on the GitLab instance. Moreover, the web proxy logs confirm that the adversary device reached *gitlab.swiftspend.finance* and maintained access through their uploaded web shell.
What is the result of their action?	The adversary achieved remote code execution on *gitlab.swiftspend.finance* and performed post-exploitation activities.

The example above emphasises how logs are instrumental in piecing together a complete picture of an event, thereby enhancing our understanding and ability to respond effectively.

Log Types

Specific log types can offer a unique perspective on a system's operation, performance, and security. While there are various log types, we will focus on the most common ones that cover approximately 80% of the typical use cases.

Below is a list of some of the most common log types:



- **Application Logs:** Messages about specific applications, including status, errors, warnings, etc.
- **Audit Logs:** Activities related to operational procedures crucial for regulatory compliance.
- **Security Logs:** Security events such as logins, permissions changes, firewall activity, etc.
- **Server Logs:** Various logs a server generates, including system, event, error, and access logs.
- **System Logs:** Kernel activities, system errors, boot sequences, and hardware status.
- **Network Logs:** Network traffic, connections, and other network-related events.
- **Database Logs:** Activities within a database system, such as queries and updates.
- **Web Server Logs:** Requests processed by a web server, including URLs, response codes, etc.

Understanding the various log types, formats, and standards is critical for practical log analysis. It enables an analyst to effectively parse, interpret, and gain insights from log data, facilitating troubleshooting, performance optimisation, incident response, and threat hunting.

Log Formats

- Semi-structured Logs
  - syslog
  - windows Event log
- Structured Logs
  - CSV,TSV,JSON,XML
- Unstructured
  - NCSA Common Log Format (CLF)
  - NCSA Combined Log Format (Combined)

Log Standards

A log standard is a set of guidelines or specifications that define how logs should be generated, transmitted, and stored. Log standards may specify the use of particular log formats, but they also cover other aspects of logging, such as what events should be logged, how logs should be transmitted securely, and how long logs should be retained. Examples of log standards include:

- **Common Event Expression (CEE):** This standard, developed by MITRE, provides a common structure for log data, making it easier to generate, transmit, store, and analyse logs.
- **OWASP Logging Cheat Sheet:** A guide for developers on building application logging mechanisms, especially related to security logging.
- **Syslog Protocol:** Syslog is a standard for message logging, allowing separation of the software that generates messages from the system that stores them and the software that reports and analyses them.
- **NIST Special Publication 800-92:** This publication guides computer security log management.
- **Azure Monitor Logs:** Guidelines for log monitoring on Microsoft Azure.
- **Google Cloud Logging:** Guidelines for logging on the Google Cloud Platform (GCP).
- **Oracle Cloud Infrastructure Logging:** Guidelines for logging on the Oracle Cloud Infrastructure (OCI).
- **Virginia Tech - Standard for Information Technology Logging:** Sample log review and compliance guideline.

Answer the questions below

- Log Collection - Involves collection from multiple sources. Configuring NTP is crucial for co-related time.

  > ntpdate pool.ntp.org

  - Identify sources
  - Choose a log collector
  - Collection parameters
  - Test collection

- Log management - securely storing, organising, and easy retrival.

  - Storage
  - Organisation
  - Backup
  - Review

- Log centralisation - its crucial for in-depth analysis and incidence response.

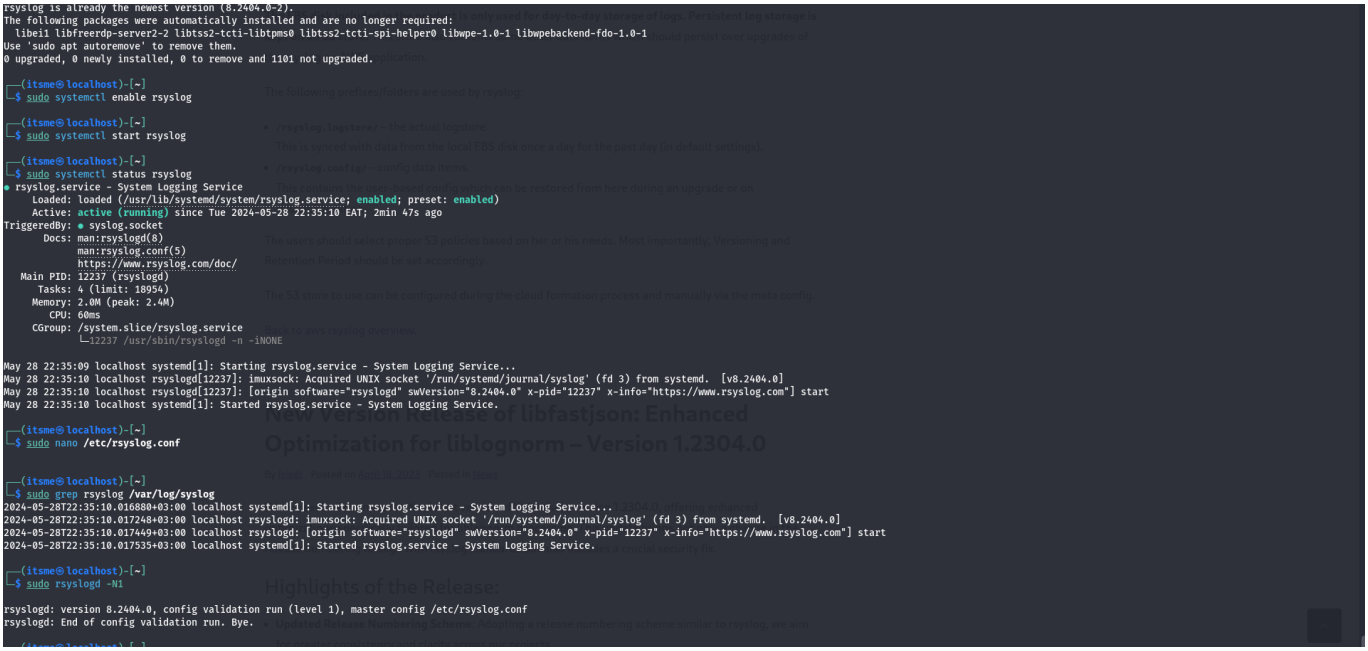
  - A centralised system
  - Integrate sources
  - Set up monitoring
  - Integration with Incident management

Rsyslog

Its a centralised logging sys.

```
Lets use it log all sshd logs to view when we log in.

> sudo systemctl enable rsyslog
> sudo systemctl start rsyslog
> sudo systemctl status rsyslog

configuration file
> sudo nano /etc/rsyslog.conf

checking logs
```

```
> sudo rsyslogd -N1

combining all logs in one file
> *.*                                           /var/log/combined.log
```



Log Management

- Storage
    - Security requirements
    - Accessibility needs
    - Storage capacity
    - Cost consideration
    - Compliance regulations
    - Retention policies
    - Disaster recovery plans
- Retention
    - Hot storage 3-6 months
    - Warm Storage 6months - 2yrs
    - Cold Storage 2-5yrs
- Deletion
    - size/cost capacity
    - Regulatuins

Logrotate

```
Logrotate is a utility for managing log files on Unix-like operating
systems. It is used to ensure that log files do not consume too much disk
space, and to allow log files to be rotated and compressed, making it
easier to manage and analyze them.

> sudo nano /etc/logrotate.d/98-websrv-02_sshd.conf
> sudo logrotate -f /etc/logrotate.d/98-websrv-02_sshd.conf
```

```
/var/log/websrv-02/rsyslog_sshd.log {
    daily
    rotate 30
    compress
    lastaction
        DATE=$(date +"%Y-%m-%d")
        echo "$(date)" >> "/var/log/websrv-
02/hashes_"$DATE"_rsyslog_sshd.txt"
        for i in $(seq 1 30); do
            FILE="/var/log/websrv-02/rsyslog_sshd.log.$i.gz"
            if [ -f "$FILE" ]; then
                HASH=$(/usr/bin/sha256sum "$FILE" | awk '{ print $1 }')
                echo "rsyslog_sshd.log.$i.gz "$HASH"" >> "/var/log/websrv-
02/hashes_"$DATE"_rsyslog_sshd.txt"
            fi
        done
        systemctl restart rsyslog
    endscript
}
```

Log Analysis

- data sources
- parsing
- normalisation
- sorting
- classification
- enrichment
- correlation
- visualisation
- reporting

- Tools
    - cat
    - grep
    - sed
    - sort
    - uniq
    - awk

log viewer

```
```