

 **ONE IDENTITY™**

# Syslog-ng 101 part 1: introduction

Peter Czanik

# About me

- Peter Czanik from Hungary
- Syslog-ng user for 20+ years
- Open Source Evangelist at One Identity: syslog-ng upstream
- syslog-ng packaging, support, advocacy
- syslog-ng originally developed by Balabit, now part of One Identity

# Overview

- What is syslog-ng / logging concepts
- The four roles of syslog-ng
- Configuration, testing
- Networking, relays
- Filters, parsers
- Logging to Elasticsearch

# What you need

- Linux / FreeBSD
- syslog-ng 3.37+ (but at least 3.23+)

Optionally:

- GeoIP, Elasticsearch & Kibana 7+ or OpenSearch
- You can download slides, sample data and configurations from: TBD

# What is syslog-ng?

- Logging: recording events, for example:

```
Jan 14 11:38:48 linux-0jbu sshd[7716]: Accepted  
publickey for root from 127.0.0.1 port 48806 ssh2
```

- syslog-ng: an enhanced logging daemon with a focus on portability and high-performance central log collection. Originally developed in C.

 **ONE IDENTITY™**