Elevating Security Intelligence

Incorporating uSIEM for Comprehensive Monitoring and Proactive Risk Management

Kostas Kalevras, DevOps Engineer, GUNet

Agenda

- SIEM
- Business as Usual
- uSIEM
- Loki / Grafana Stack
- Live Demo

SIEM

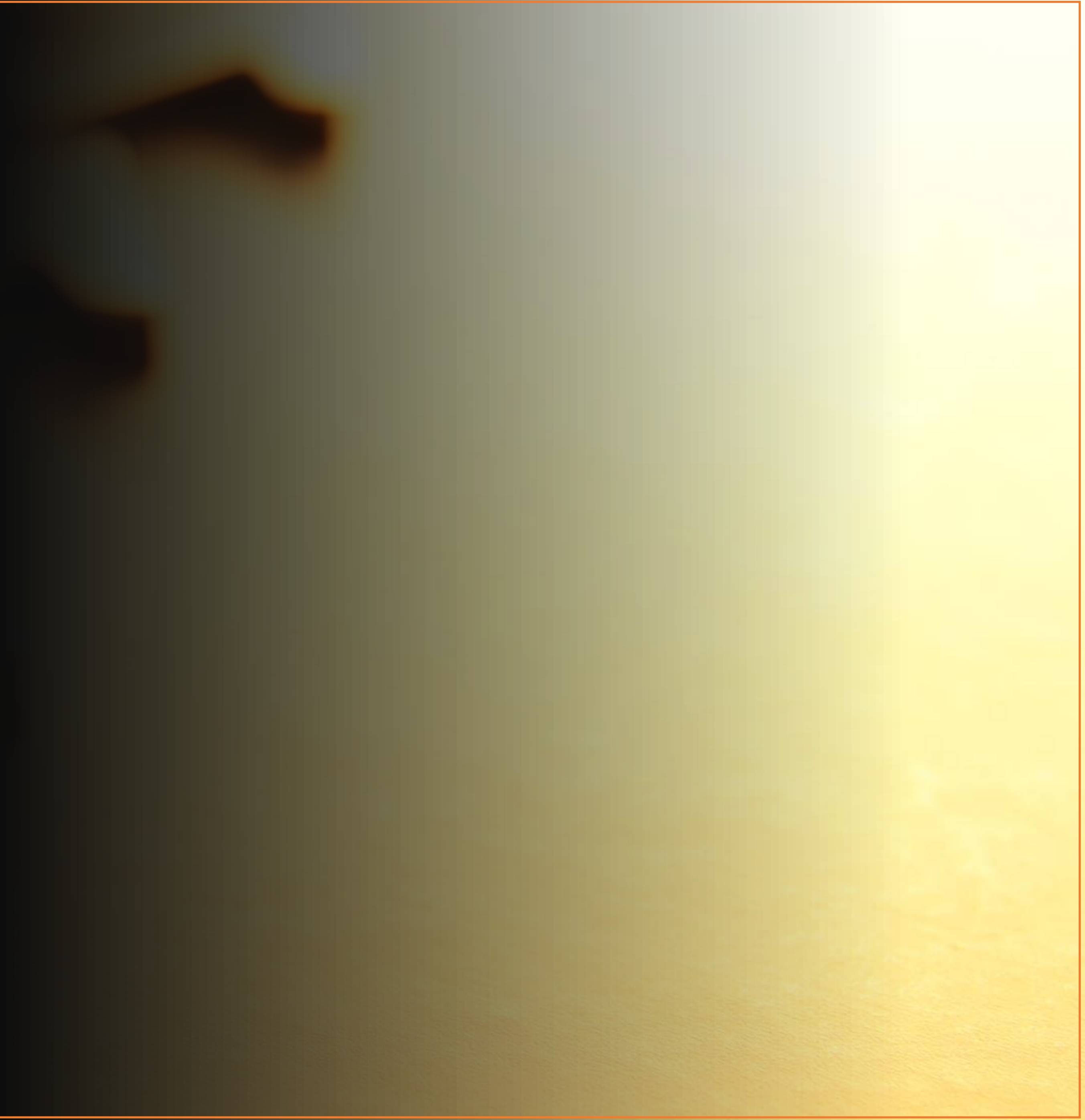
- Security Information
  - Log Aggregation + Storage (TSDB)
  - Log Visualization
  - Dashboards
- Event Management
  - Anomaly Detection
    - Predefined rules
    - Machine Learning
  - Event Visualization
  - Alerting
  - Notification
    - E-mail
    - SMS
    - Slack
- RBAC Access

Business as Usual

- GUNet – Identity stack
  - IDM
  - SSO / MFA
  - RADIUS / uGuest
- Security Monitoring
  - Log files, Syslog
  - No Visualizations
- Event Management

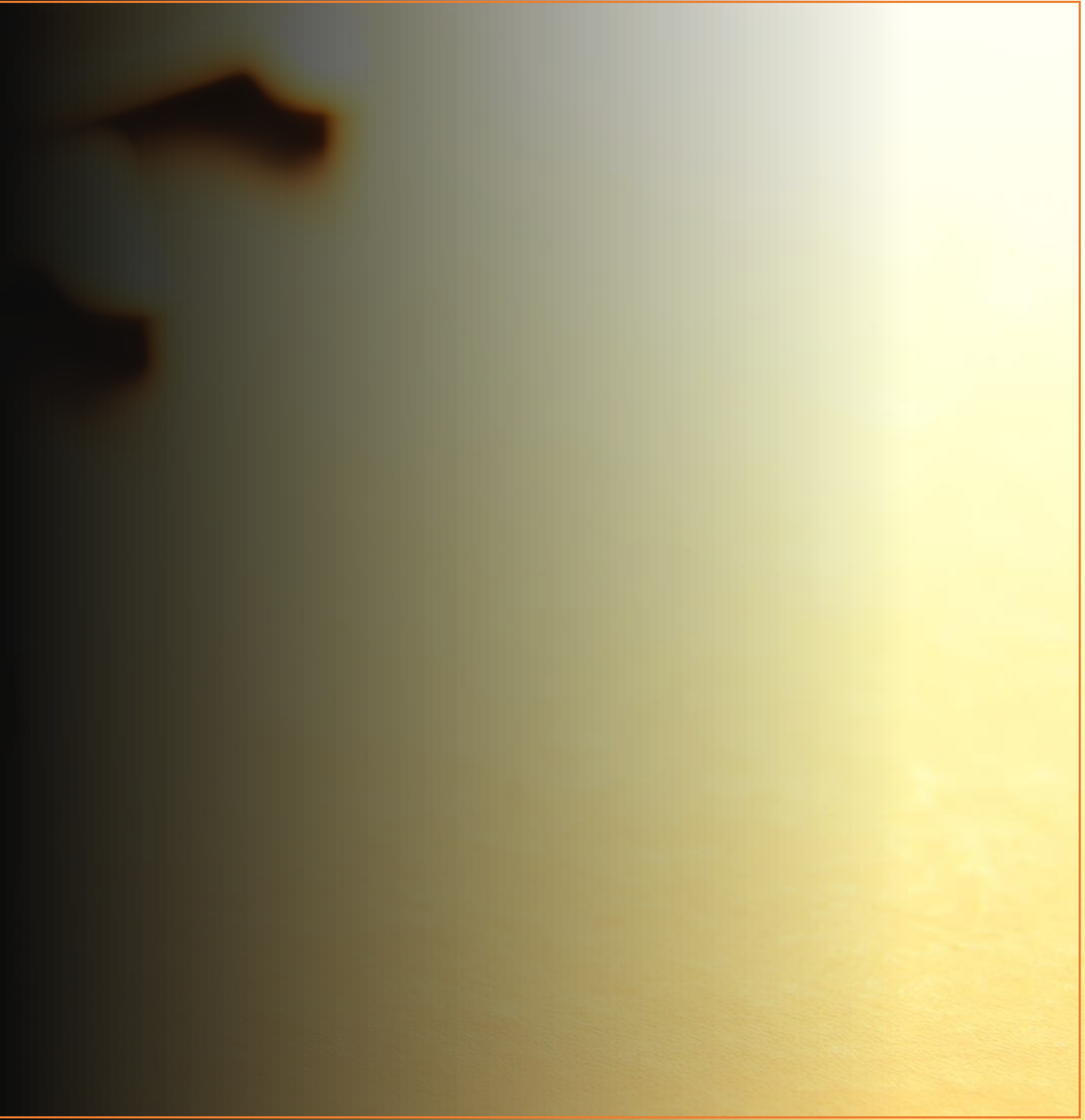
uSIEM

- Software as a Service
  - Based on Loki + Grafana (Docker)
- Security Information
  - Log Aggregation for GUNet services
    - SSO
    - MFA
    - RADIUS
    - uGuest
  - Log Visualization
  - Pre-Provisioned Dashboards
- Future
  - More GUNet Services
  - Event Management
    - Anomaly Detection
    - Alerting - Notifications
- RBAC Access
  - oAuth + MFA
  - Roles based on eduPersonEntitlement



Why Grafana?

- Open Source / Large Community
- Lightweight, Dockerized
- Easy integration
  - Docker Loki Logging Driver
  - Promtail tool for log processing
  - Integration with syslog
- Small footprint
  - 200MB RAM
  - 600MB Docker image stack
- Low disk requirements
  - Label indexing, not full indexing
  - Compression
  - GUNet stack: ~15MB/day



uSIEM Live Demo