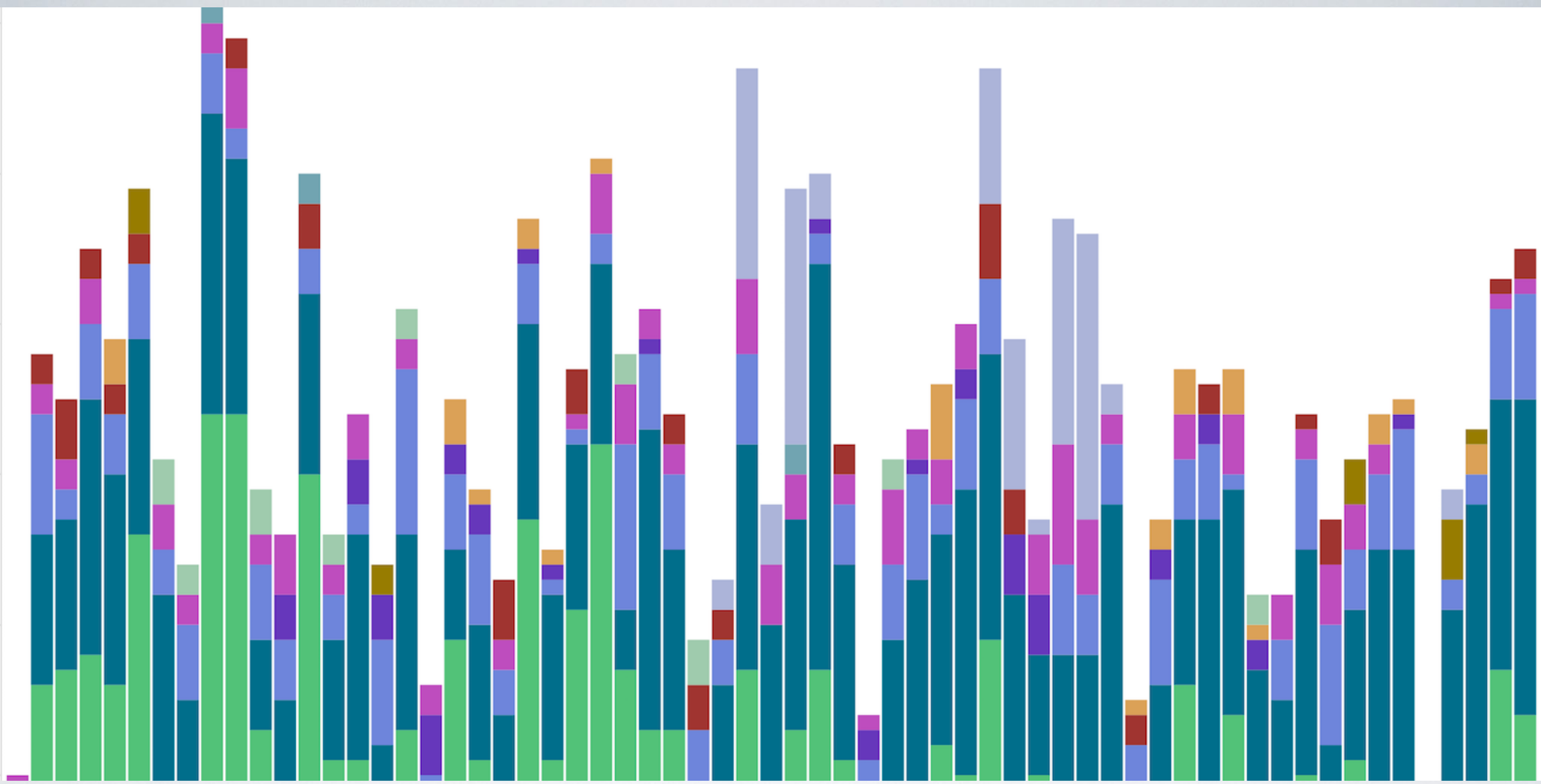


SECURITY-FOCUSED ELK STACK

UCLA Information Security Office

UCLA: Security-Focused ELK Stack

Ross Bollens, Ph.D.

Director of Information Security/CISO | UCLA

Alex Podobas

DevOps/Senior InfoSec Analyst | UCLA Information Security Office

2017 Juris Doctor Candidate | UC Irvine School of Law

A DECEPTIVELY SIMPLE PROBLEM

Servers we use write countless log entries. Buried in those logs are security events that **every** sysadmin, developer, or security professional should be paying attention to, but very likely isn't.

FRAMEWORK OF A SOLUTION

A better approach is to have logs automatically parsed for security events, and those events presented clearly in a human-readable format.

DISADVANTAGES OF NOT USING AN AUTOMATED LOG PARSER

1. Day-to-day, logs are rarely examined;

2. Discovered security issues might be days or weeks old. Slow and reactive response;

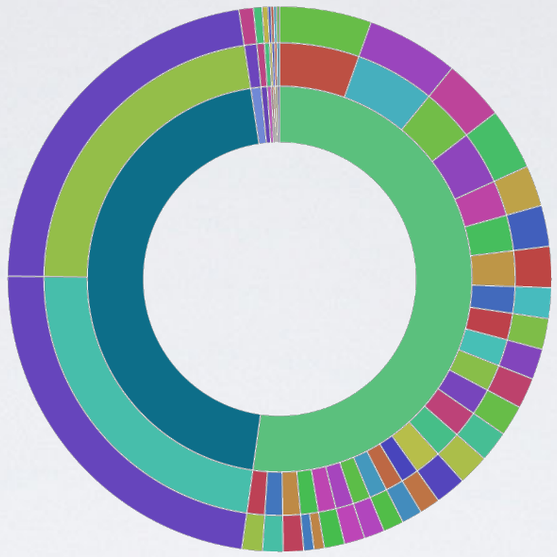
3. Trends cannot be discerned from single, discrete log entries.

UCLA: Security-Focused ELK Stack

elastic

Logstash Forwarder	→	Forwards logs
Logstash	→	Collects/parses logs
Elasticsearch	→	Stores log data
Kibana	→	Visualizes Elasticsearch

UCLA: Security-Focused ELK Stack



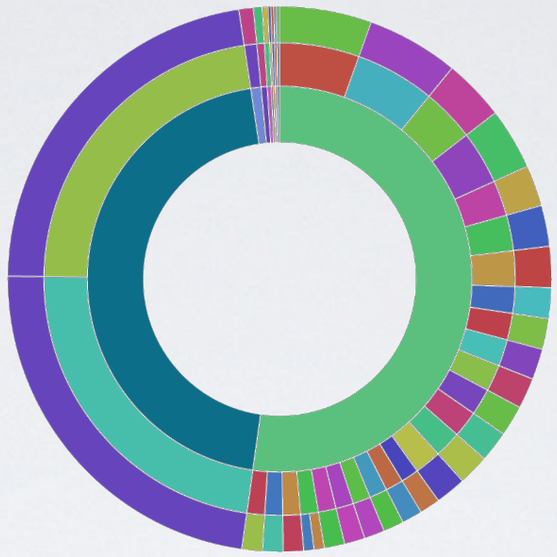
UCLA'S ELK STACK

Configured out of the box

Specific to InfoSec log events

Useful for legal/forensic investigations

UCLA: Security-Focused ELK Stack

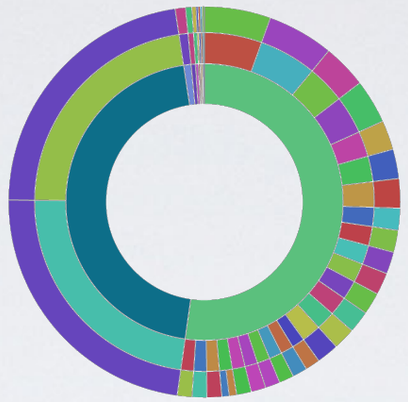


CONFIGURED OUT OF THE BOX

Well-documented, step-by-step installation provided

Our production logstash.conf, logstash-forwarder.conf, and Kibana dashboards posted to Github. Incredibly easy to import and update.

UCLA: Security-Focused ELK Stack



SPECIFIC TO INFOSEC LOG EVENTS

Authentication attempts (SSH, MySQL, Basic Auth, Google 2FA);

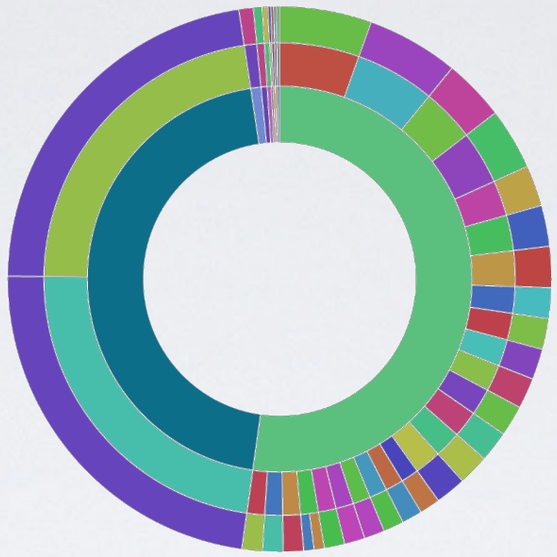
When new users and/or new groups are added or removed;

Password changes and privilege elevation attempts;

SQL injection attempts;

Successful + failed Shibboleth logins (pertinent to University of California campuses).

UCLA: Security-Focused ELK Stack



LEGAL FORENSICS/INVESTIGATIONS

Information security is deeply connected to legal investigations and forensics. Our security-focused ELK stack has reduced the time and effort involved in gathering log-based evidence.

UCLA: Security-Focused ELK Stack

SUMMER 2015 ROADMAP

[Linux: audit.d]

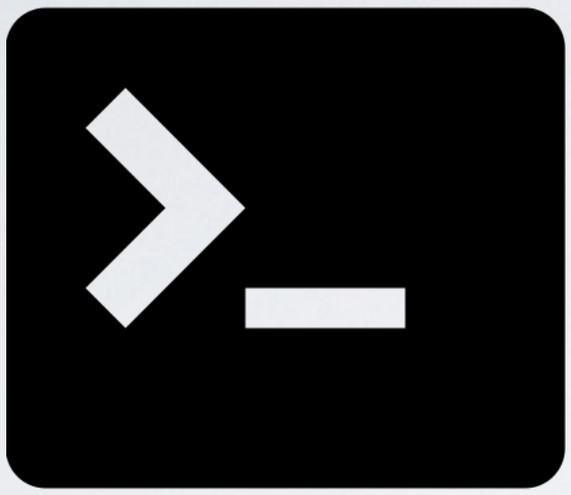
[Windows Server: logstash-forwarder]

[Linux: privileges on watched files/directories]

[Major Databases: MSSQL, MariaDB, Percona, etc.]

[Netflow: [D]DOS attacks] [Netflow: Outbound/Inbound]

UCLA: Security-Focused ELK Stack



NEXT UP: LIVE DEMO