BCNET

Shared IT Services for Higher Education & Research

Conference 2018

Infrastructure for Security, Infrastructure for Agility

Jeff Albert

University of Victoria

Hi, I'm Jeff

- Senior System Administrator, UVic Systems

Hi, I'm Jeff

- Senior System Administrator, UVic Systems

- 11 years with the Enterprise IT side of the shop

Hi, I'm Jeff

- Senior System Administrator, UVic Systems

- 11 years with the Enterprise IT side of the shop

- Made the jump to Research Computing in Nov 2017

Hi, I'm Jeff

- Senior System Administrator, UVic Systems

- 11 years with the Enterprise IT side of the shop

- Made the jump to Research Computing in Nov 2017

- Fortunate to have worked on many of UVic's IT infrastructure projects: asset management, configuration management, logging and alerting, web application platforms, and now cloud computing
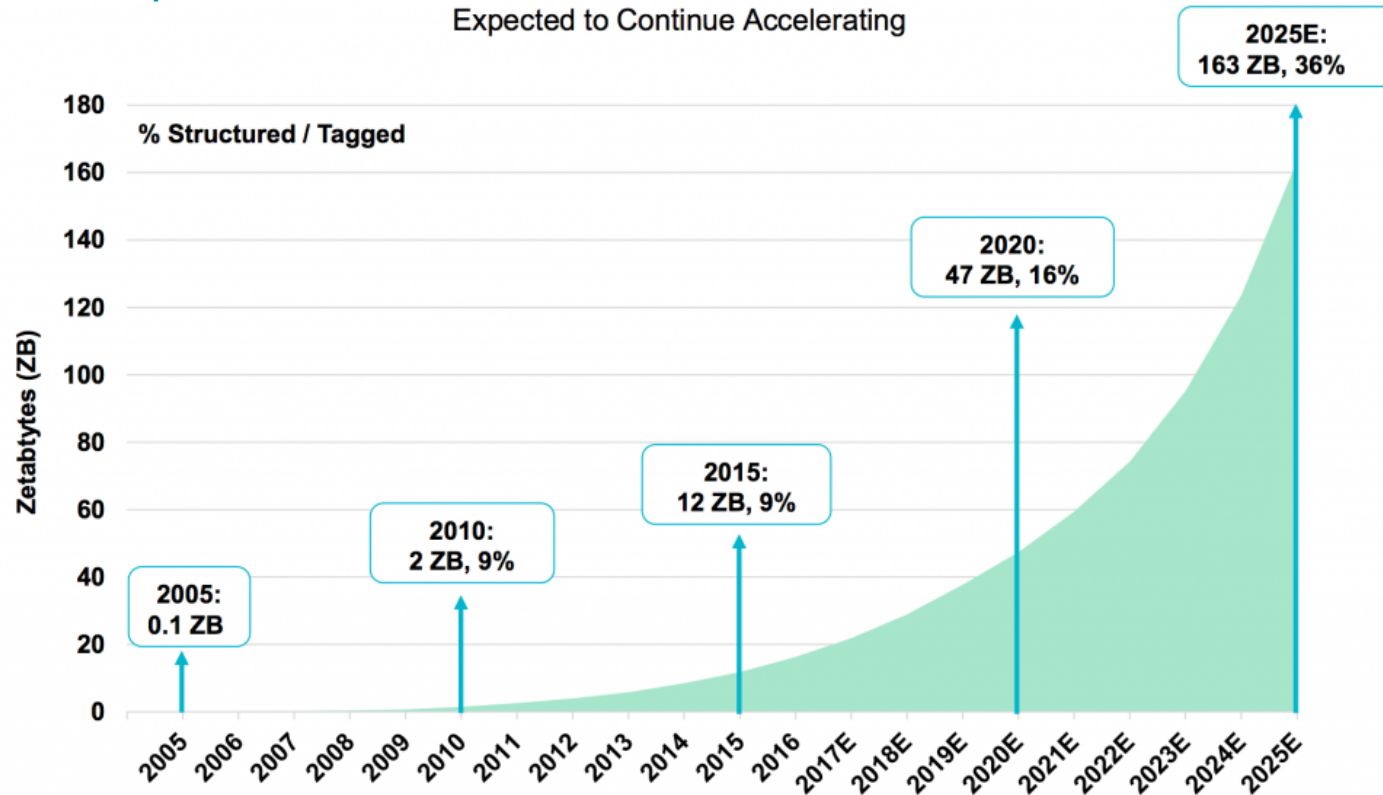
Scope and Scale of IT Ops: It's Getting Out of Hand

…in software complexity:
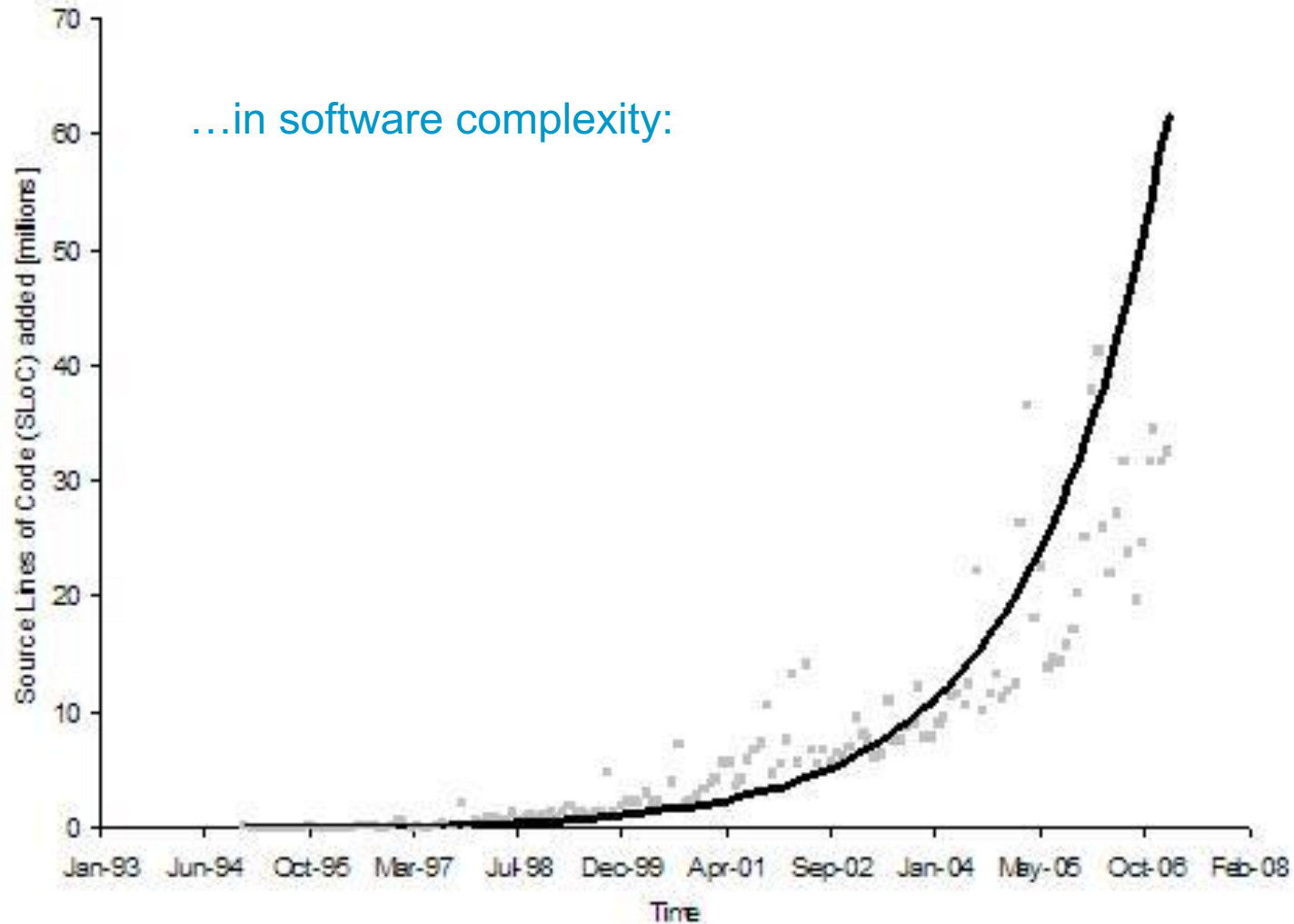
Scope and Scale of IT Ops: It's Getting Out of Hand

...in data footprint:

Information Created Worldwide =
Expected to Continue Accelerating

2025E:
163 ZB, 36%

2020:
47 ZB, 16%

2015:
12 ZB, 9%

2010:
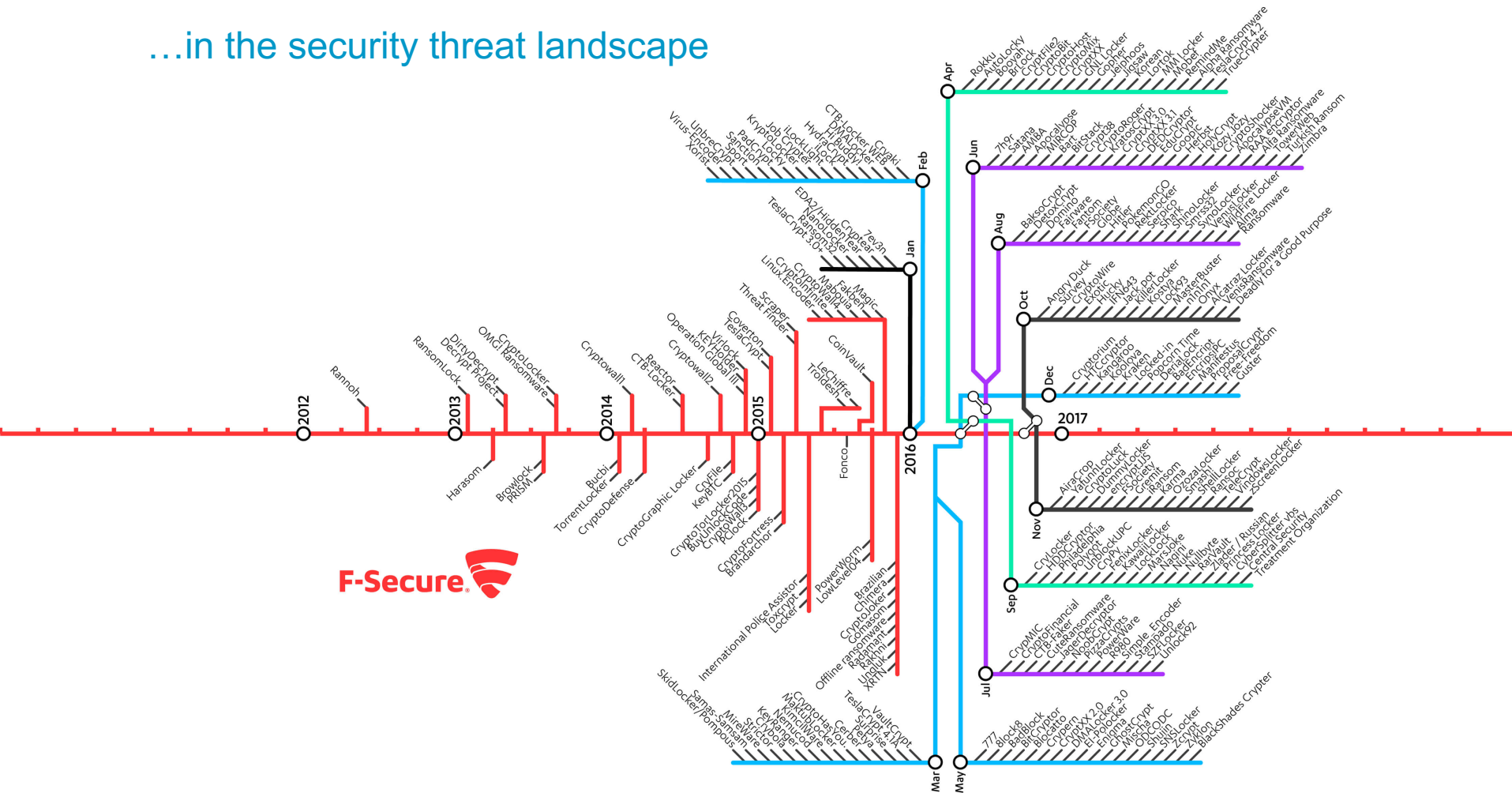2 ZB, 9%

2005:
0.1 ZB

% Structured / Tagged

Zetabytes (ZB)

KLEINER PERKINS

Source: IDC DataAge 2025 Study, sponsored by Seagate (3/17)
Note: 1 petabyte = 1MM gigabytes, 1 zeta byte = 1MM petabytes

BCNET Conference 2018

Scope and Scale of IT Ops: It's Getting Out of Hand

…in the security threat landscape

F-Secure

2018-level IT Complexity

↑

200m

How Can We Climb Up a Curve That Steep?

How Can We Climb Up a Curve That Steep?

By Not Starting At The Bottom!

Case Study

Automated Linux Updates

Requirement:

"Our systems must be up to date with security fixes"

Easy, right?

```
sudo mesh all "yum -y update"
```

Wait…

- Did some of those updates need restarts?

- Did all of those updates succeed?

- Did we communicate to all our stakeholders?

- Did we establish compliance with client requirements?

- Did we document what was updated and when?

- Are we gonna have to do this by hand every time?

Wait…we need infrastructure around this

- Did some of those updates need restarts?

- Did all of those updates succeed?

- Did we communicate to all our stakeholders?

- Did we establish compliance with client requirements?

- Did we document what was updated and when?

- Are we gonna have to do this by hand every time?

Wait…we need infrastructure around this

- Configuration Management

- Did all of those updates succeed?

- Did we communicate to all our stakeholders?

- Did we establish compliance with client requirements?

- Did we document what was updated and when?

- Are we gonna have to do this by hand every time?

Wait…we need infrastructure around this

- Configuration Management

- Monitoring

- Did we communicate to all our stakeholders?

- Did we establish compliance with client requirements?

- Did we document what was updated and when?

- Are we gonna have to do this by hand every time?

Wait…we need infrastructure around this

- Configuration Management

- Monitoring

- Alerting

- Did we establish compliance with client requirements?

- Did we document what was updated and when?

- Are we gonna have to do this by hand every time?

Wait…we need infrastructure around this

- Configuration Management

- Monitoring

- Alerting

- Service Management

- Did we document what was updated and when?

- Are we gonna have to do this by hand every time?

Wait…we need infrastructure around this

- Configuration Management

- Monitoring

- Alerting

- Service Management

- Asset Management

- Are we gonna have to do this by hand every time?

Wait…we need infrastructure around this

- Configuration Management

- Monitoring

- Alerting

- Service Management

- Asset Management

- Automation

Easy, right?

```
sudo mesh all "yum -y update"
```

Easy, right?

```
sudo mesh* all "yum -y update"
```

* Mesh is an infrastructure component developed in-house
to enable parallel cross-environment command execution

HIGH RISK LIVE DEMO

Asset / Service Management

ConfigManager – in-house web application

- 6 years of active development and testing in the UVic environment

- Inventory metadata on every managed asset

- Service and stakeholder metadata including contacts

- Provides inventory as an infrastructure service

Configuration Management / Automation

Ansible

- 2 years development and testing in the UVic environment

- Sources inventory directly from ConfigManager

- Provides desired-state and operational playbook execution as an infrastructure service
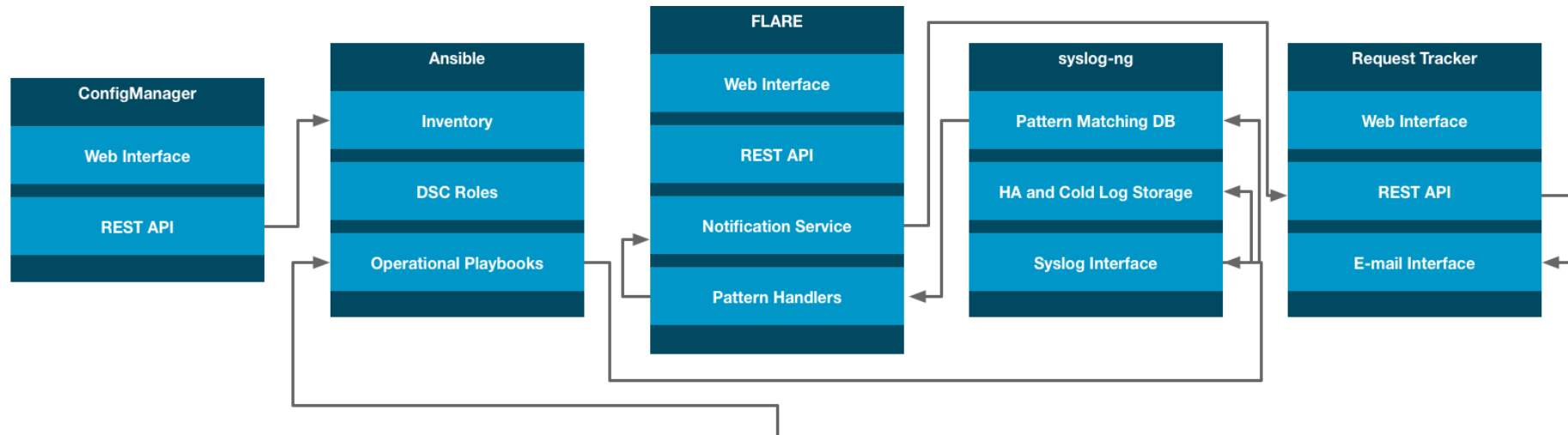
Monitoring / Alerting

Syslog-ng / FLARE

- 5 years development and testing in the UVic environment

- Combines syslog from all managed assets, internal pattern database, and ConfigManager inventory

- Provides event transport, logging, pattern-based monitoring and inventory-informed alerting as infrastructure services

Monitoring / Alerting

Request Tracker

- 10 years development and testing in the UVic environment

- Web UI, API, and e-mail interfaces to a live archival record of ongoing and historical issues

- Provides collaborative issue tracking, triage, and notification as infrastructure services

Automated Updates Leveraging Infrastructure

ConfigManager
- Web Interface
- REST API

Ansible
- Inventory
- DSC Roles
- Operational Playbooks

FLARE
- Web Interface
- REST API
- Notification Service
- Pattern Handlers

syslog-ng
- Pattern Matching DB
- HA and Cold Log Storage
- Syslog Interface

Request Tracker
- Web Interface
- REST API
- E-mail Interface

Automated Updates Process

1. Check for Scheduled Updates
2. Notify Stakeholders About Pending Updates
3. Kick Off Update Process
4. Monitor Update Process and Alert on any Failures
5. Document Completion of Updates and Notify Stakeholders

BCNET Conference 2018

HIGH RISK LIVE DEMO
...did it work?

Infrastructure Produces Agility

Total development time:
- Automated Linux Updates: ~1 month
- Supporting Infrastructure: ~10 years

Stretch goals came "for free" from infrastructure:
- Audit accountability
- Issue tracking on update failures
- Web UI and API access to update scheduling
- Ad-hoc / out-of-band scheduling

So how do you get to this infrastructure foundation?

So how do you get to this infrastructure foundation?

- Survey your existing IT infrastructure

So how do you get to this infrastructure foundation?

- Survey your existing IT infrastructure

- Commit to using and improving what's in place

So how do you get to this infrastructure foundation?

- Survey your existing IT infrastructure

- Commit to using and improving what's in place

- Identify the gaps

So how do you get to this infrastructure foundation?

- Survey your existing IT infrastructure

- Commit to using and improving what's in place

- Identify the gaps

- Attach infrastructure development to business-driven projects

Thanks!

Thanks!

Questions?