Splunk!

splunk>

Agenda

- Welcome & introductions
- IT Security, Brisbane and us….
- What is Splunk?
- Splunk for Security
- Demo time!
- Wrap up & questions

whoami - Amanda

- Studied at QUT – musician by trade
- Career so far…
- Worst job
- Best Job
- What do you want to do?

whoami - Amanda

whoami - Amanda

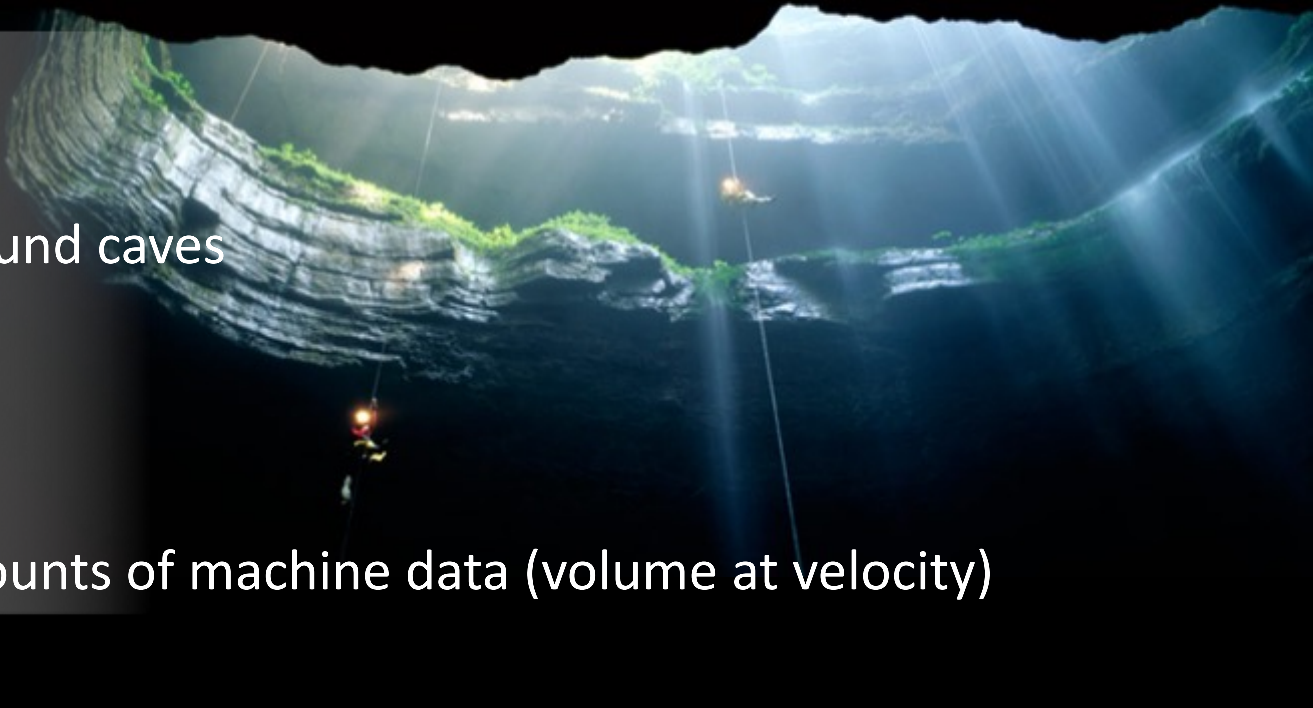
whoami - Simon

- UQ student – graduated from USC via QUT
- Career so far…
- Worst job
- Best Job
- What do you want to do?

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk



Spelunking:

to explore underground caves

Splunking:

to explore large amounts of machine data (volume at velocity)

The Accelerating Pace of Data

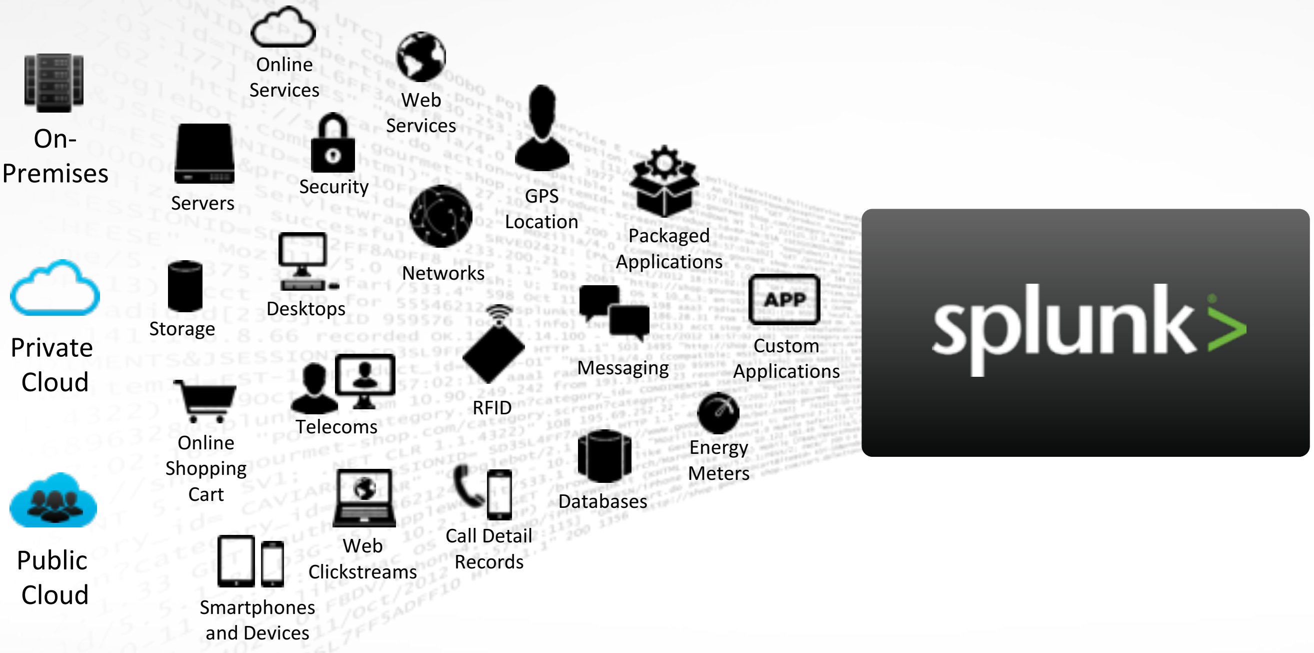
Volume | Velocity | Variety | Variability

Machine data is the fastest growing, most complex, most valuable area of 'big data'

GPS,
RFID,
Hypervisor,
Web Servers,
Email, Messaging,
Clickstreams, Mobile,
Telephony, IVR, Databases,
Sensors, Telematics, Storage,
Servers, Security Devices, Desktops

Turning Machine Data Into Business Value

Index Untapped Data: Any Source, Type, Volume


On-Premises

Private Cloud

Public Cloud

Servers

Storage

Online Shopping Cart

Smartphones and Devices

Online Services

Security

Desktops

Telecoms

Web Clickstreams

Web Services

Networks

GPS Location

RFID

Call Detail Records

Packaged Applications

Messaging

Databases

Custom Applications

Energy Meters

splunk>

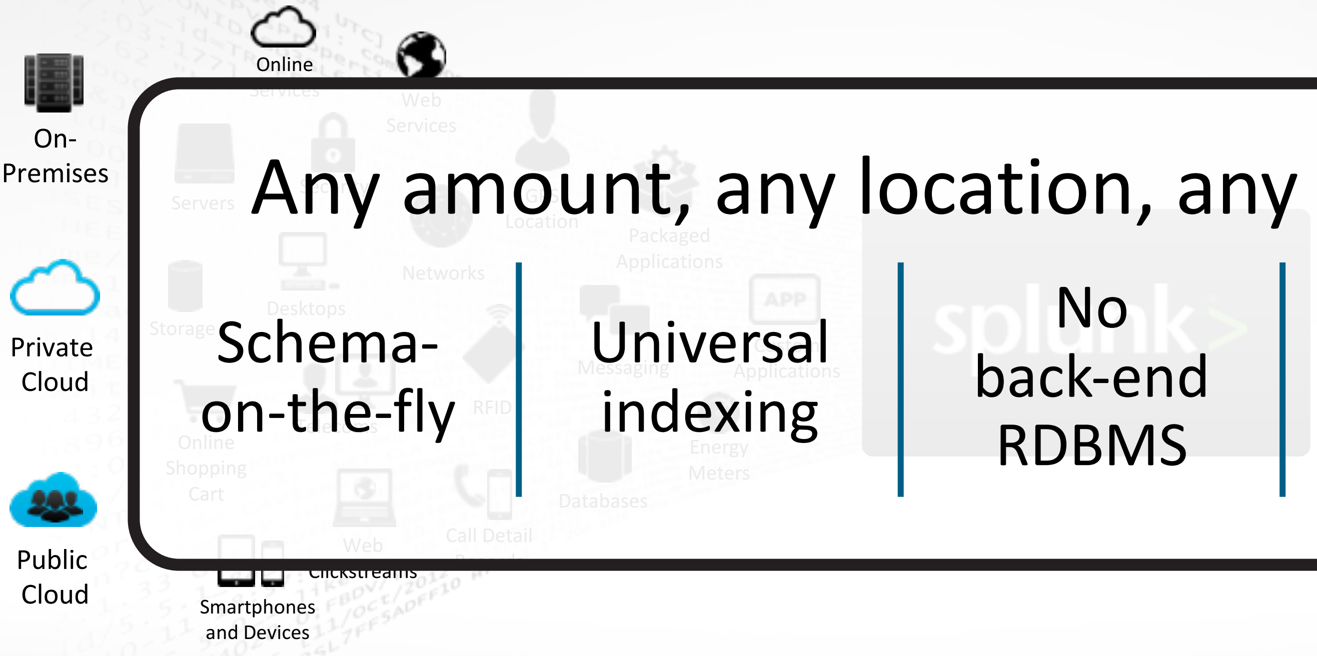
Ask Any Question

- Application Delivery
- IT Operations
- Security, Compliance and Fraud
- Business Analytics
- Industrial Data and the Internet of Things

Industry Leading Platform for Machine Data

Index Untapped Data: Any Source, Type, Volume

Ask Any Question



Any amount, any location, any source

Schema-on-the-fly	Universal indexing	No back-end RDBMS	No need to filter data

Application Delivery

IT Operations

Security, Compliance and Fraud

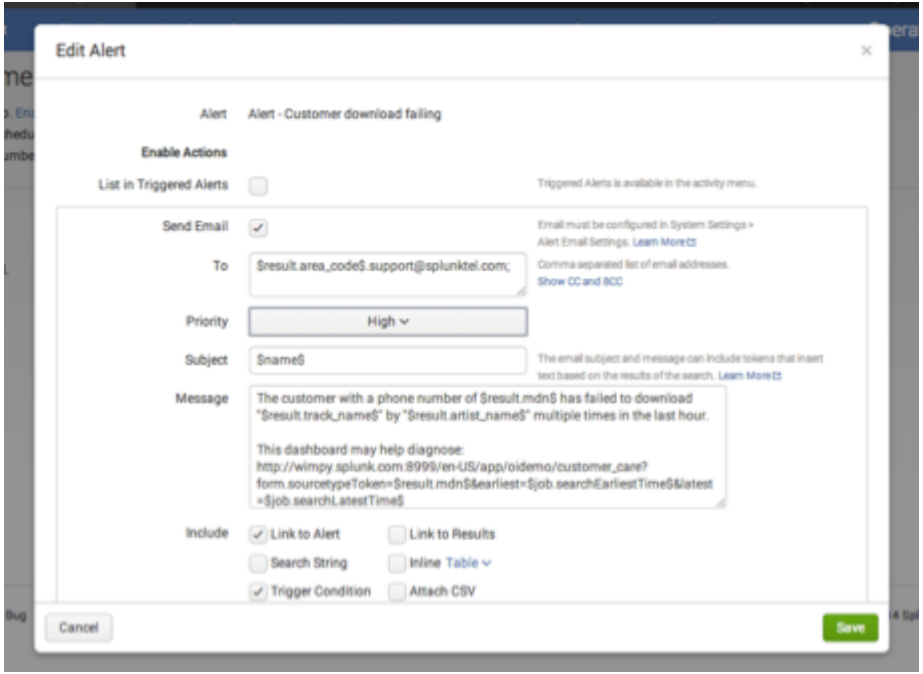
Business Analytics

Industrial Data and the Internet of Things

Actionable Alerting

Alerts

- Create alerts based on any search
- Customize content and format of email alerts
  - Provide context
  - Highlight next steps
  - Enable custom workflows
- Trigger a script
  - SMS alert
  - SNMP trap
  - Other



Alert: Alert - Customer download failing

Enable Actions

List in Triggered Alerts □ — Triggered Alerts is available in the activity menu.

Send Email ☑ — Email must be configured in System Settings > Alert Email Settings. Learn More

To: $result.area_code$.support@splunktel.com; — Comma separated list of email addresses. Show CC and BCC

Priority: High

Subject: $name$ — The email subject and message can include tokens that insert text based on the results of the search. Learn More

Message:

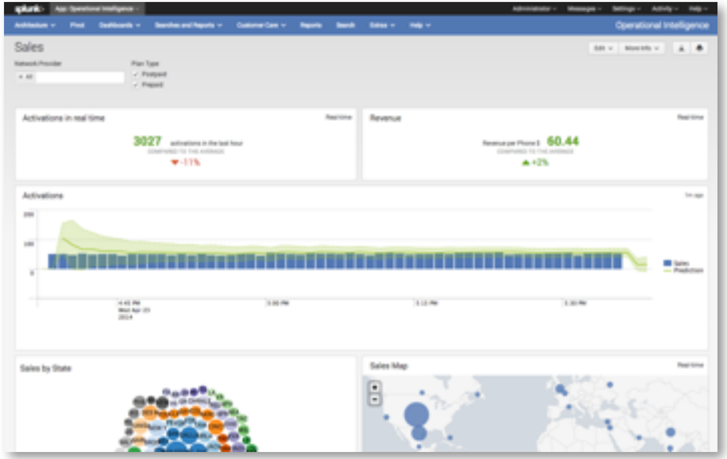
The customer with a phone number of $result.mdn$ has failed to download "$result.track_name$" by "$result.artist_name$" multiple times in the last hour.

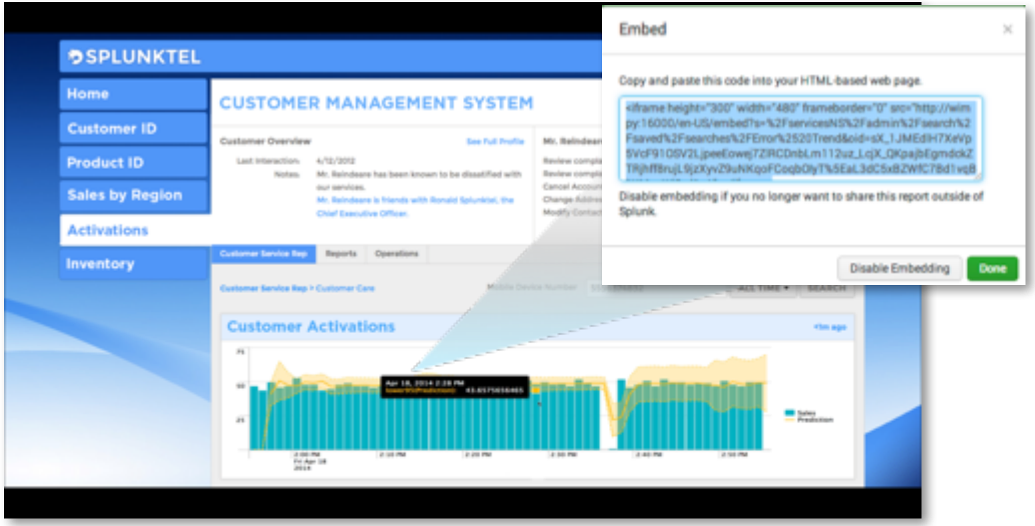
This dashboard may help diagnose:
http://wimpy.splunk.com:8999/en-US/app/oidemo/customer_care?form.sourcetypeToken=$result.mdn$&earliest=$job.searchEarliestTime$&latest=$job.searchLatestTime$

Include: ☑ Link to Alert □ Link to Results □ Search String □ Inline Table ☑ Trigger Condition □ Attach CSV

Combine Reports to Create Dashboards

Use the built-in dashboard editor





Customer Overview

Last Interaction: 4/12/2012

Notes: Mr. Reindeare has been known to be dissatisfied with our services.

Mr. Reindeare is friends with Ronald Splunktel, the Chief Executive Officer.

Embed

Copy and paste this code into your HTML-based web page.

```
<iframe height="300" width="480" frameborder="0" src="http://wim
py:16000/en-US/embed?s=%2FservicesNS%2Fadmin%2Fsearch%2
Fsaved%2Fsearches%2FError%2520Trend&oid=sX_1JMEdlH7XeVp
5VcF91OSV2LjpeeEowej7ZIRCDnbLm112uz_LqX_QKpajbEgmdckZ
TRjhff8rujL9jzXyvZ9uNKqoFCoqbOlyT%5EaL3dC5xBZWfC78d1vqB
```

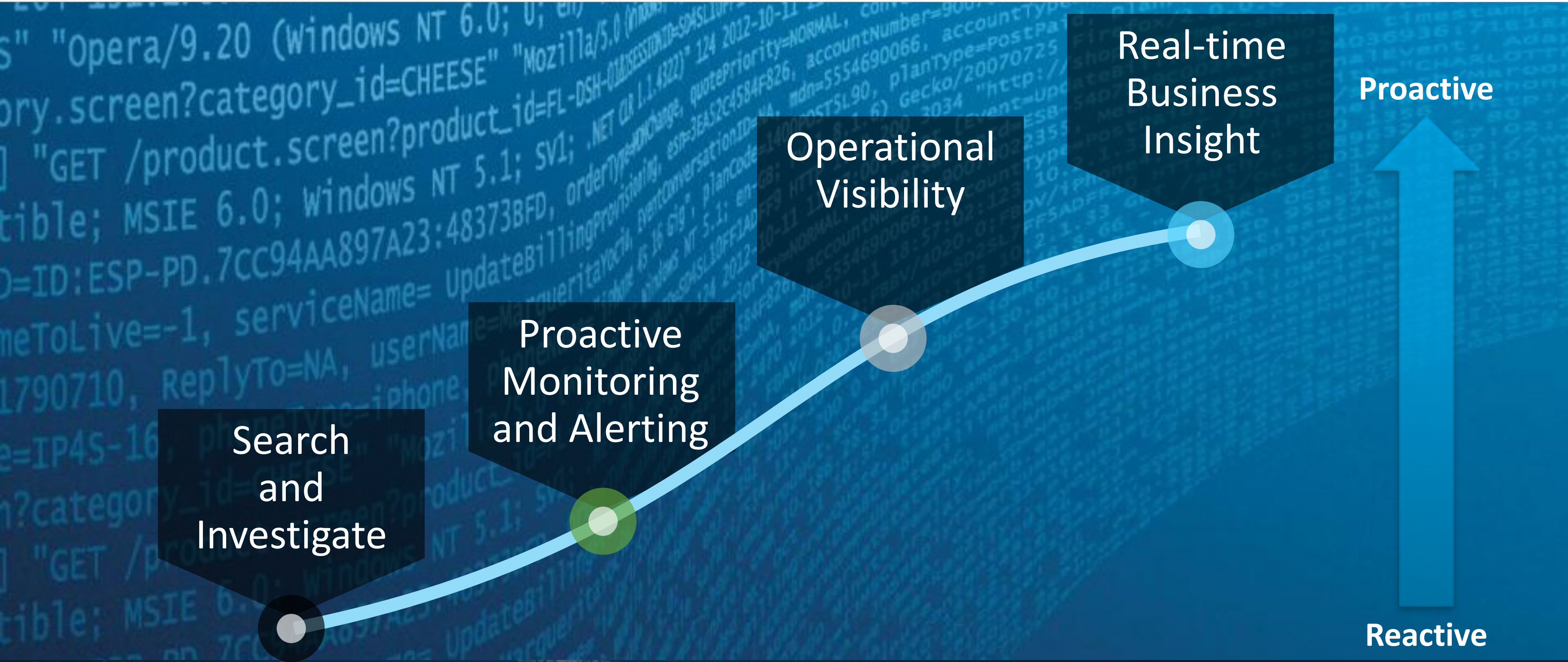
Disable embedding if you no longer want to share this report outside of Splunk.

Disable Embedding

Done

Or embed the reports into external sites like a wiki

Turning Machine Data Into Operational Intelligence



Search and Investigate

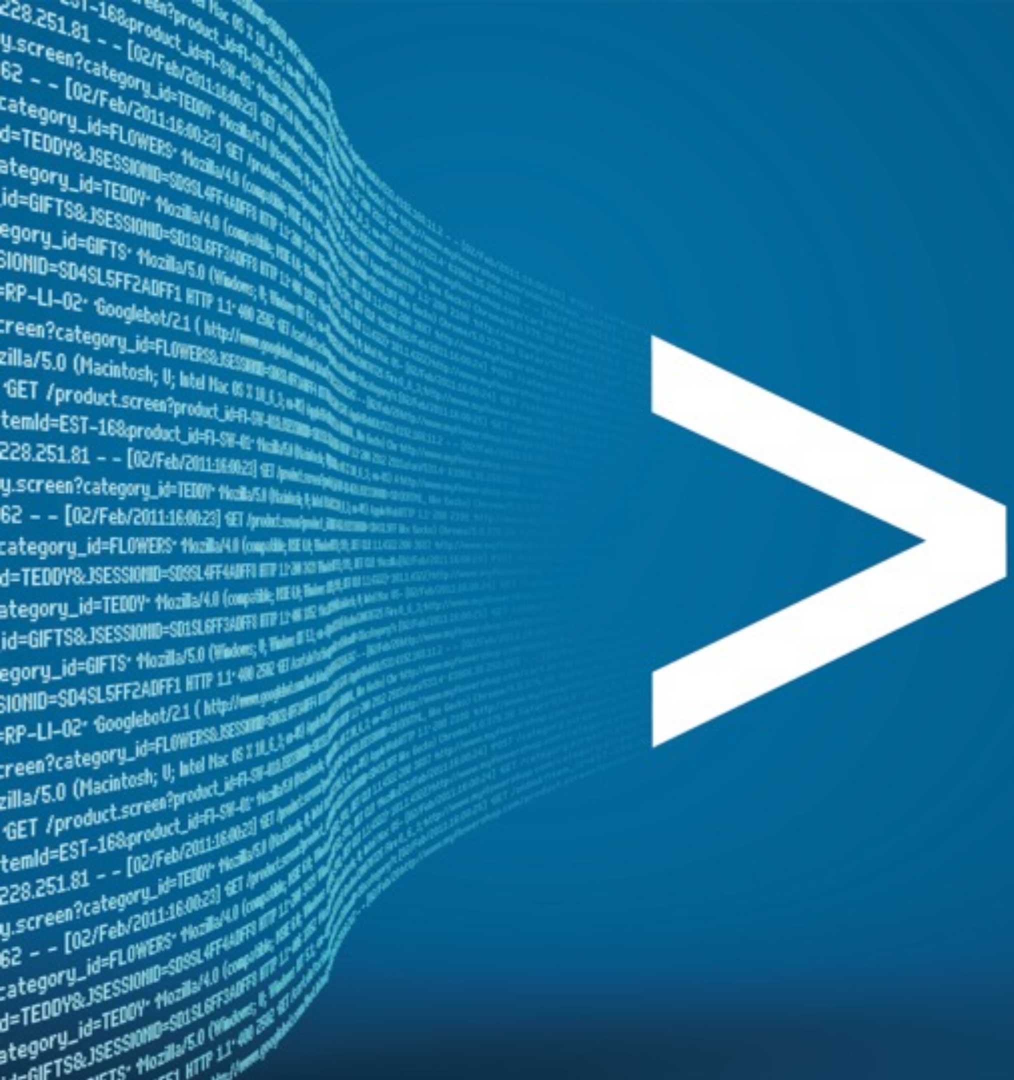
Proactive Monitoring and Alerting

Operational Visibility

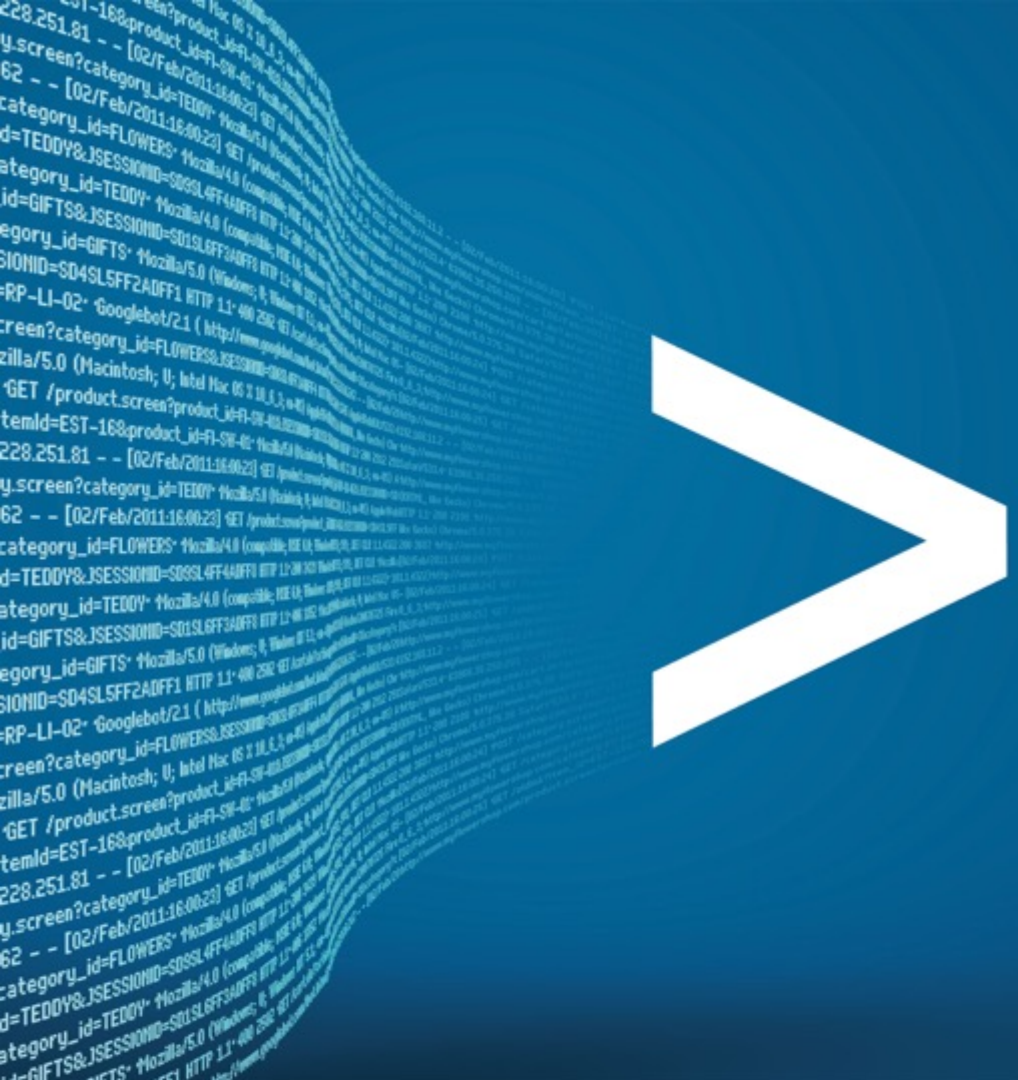
Real-time Business Insight

Proactive

Reactive



Demo Time!



Splunk for security

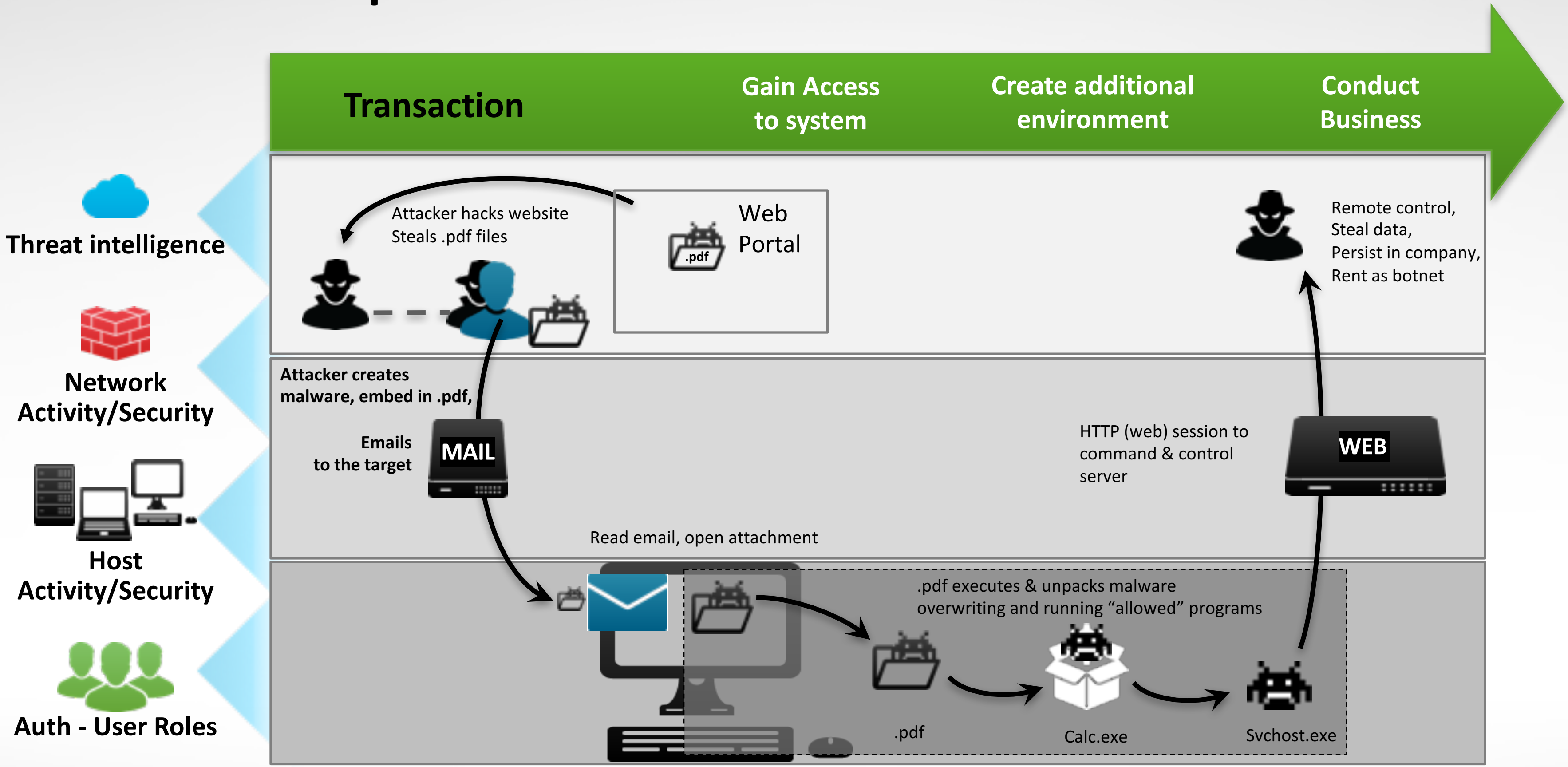
All Data is Security Relevant = Big Data

- Threat Intelligence
- Email
- Web
- Desktops
- Servers
- DHCP/ DNS
- CMDB
- Hypervisor
- Badges
- Custom Apps
- Network Flows
- Storage
- Mobile
- Physical Access
- Transaction Records

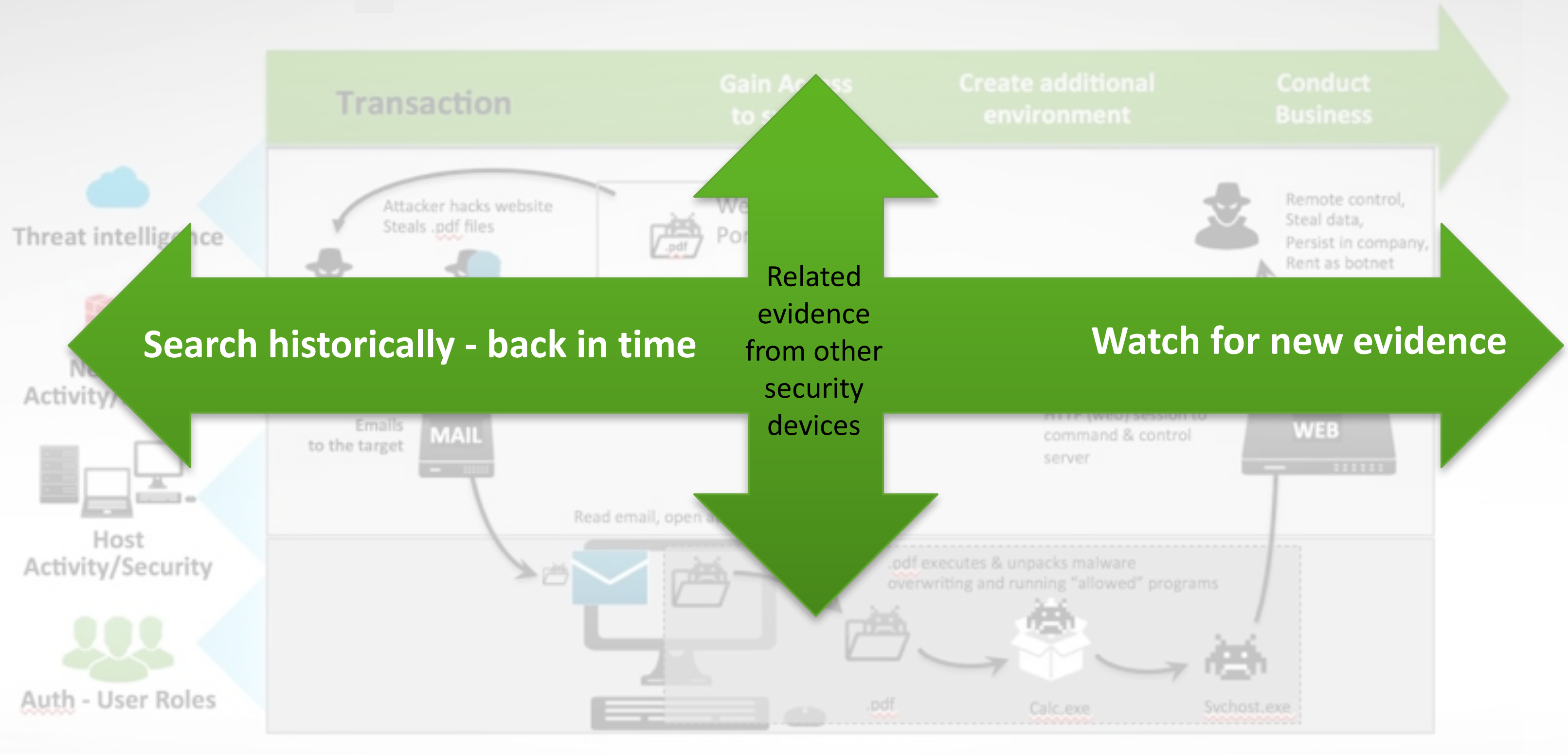
Traditional

- Firewall
- Authentication
- Vulnerability Scans
- Intrusion Detection
- Data Loss Prevention
- Anti-Malware

Example of Advanced Threat Activities



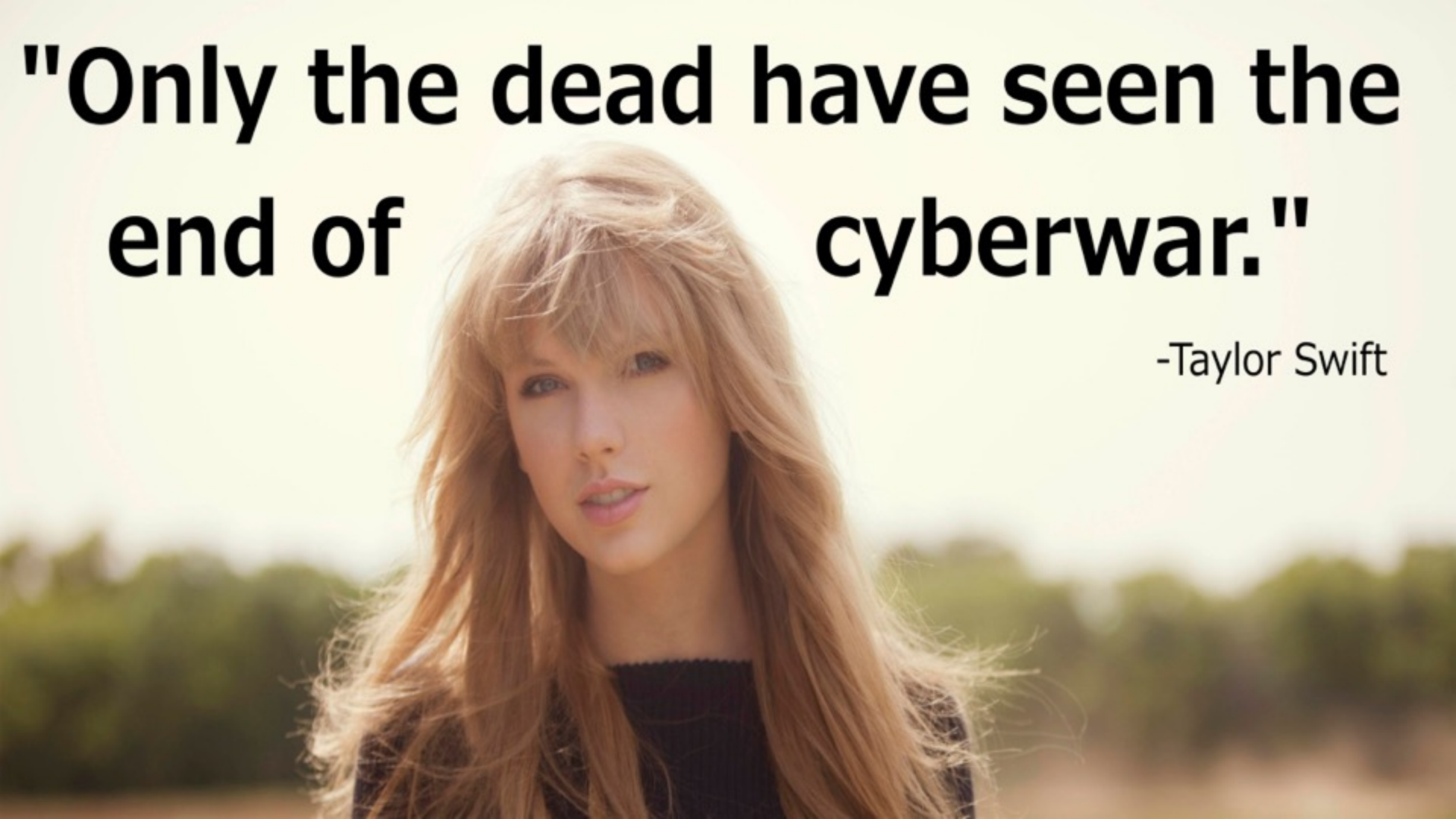
Use Splunk to Find Evidence



Search historically - back in time

Related evidence from other security devices

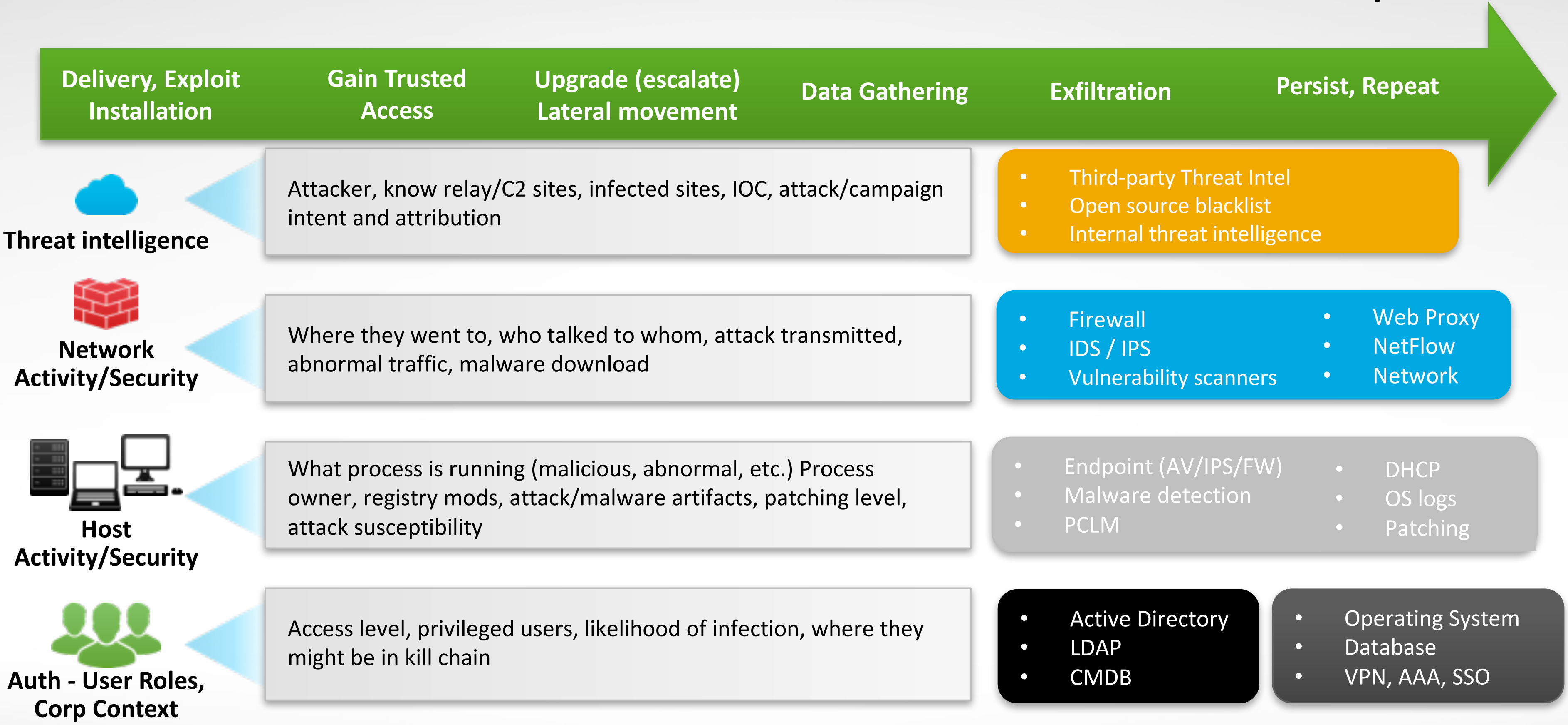
Watch for new evidence



"Only the dead have seen the end of cyberwar."

-Taylor Swift

Connect the "Data-Dots" to See the Whole Story



Delivery, Exploit Installation → Gain Trusted Access → Upgrade (escalate) Lateral movement → Data Gathering → Exfiltration → Persist, Repeat

Threat intelligence

Attacker, know relay/C2 sites, infected sites, IOC, attack/campaign intent and attribution

- Third-party Threat Intel
- Open source blacklist
- Internal threat intelligence

Network Activity/Security

Where they went to, who talked to whom, attack transmitted, abnormal traffic, malware download

- Firewall
- IDS / IPS
- Vulnerability scanners
- Web Proxy
- NetFlow
- Network

Host Activity/Security

What process is running (malicious, abnormal, etc.) Process owner, registry mods, attack/malware artifacts, patching level, attack susceptibility

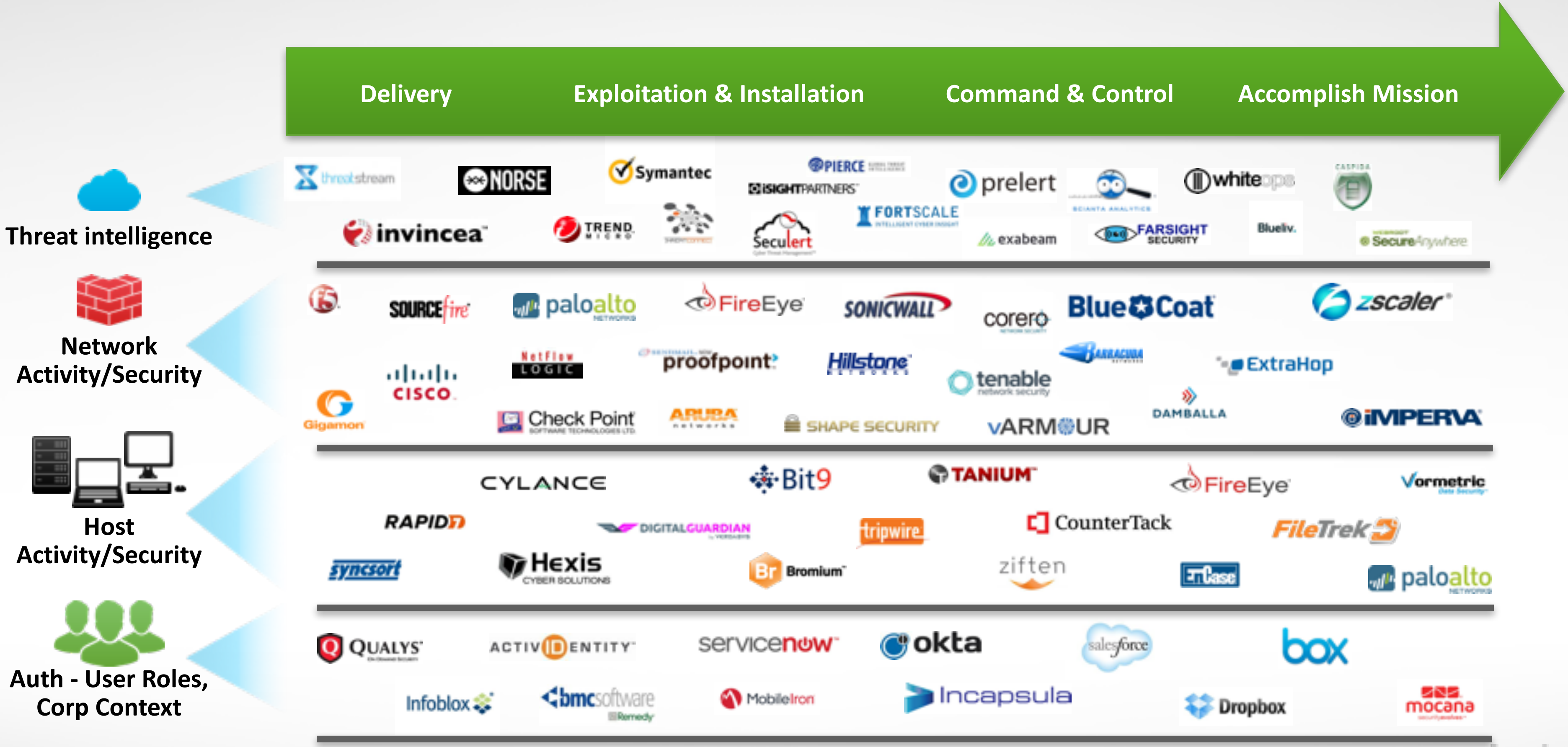
- Endpoint (AV/IPS/FW)
- Malware detection
- PCLM
- DHCP
- OS logs
- Patching

Auth - User Roles, Corp Context

Access level, privileged users, likelihood of infection, where they might be in kill chain

- Active Directory
- LDAP
- CMDB
- Operating System
- Database
- VPN, AAA, SSO

Security Ecosystem for Coverage and Protection



Delivery | Exploitation & Installation | Command & Control | Accomplish Mission

Threat intelligence

Network Activity/Security

Host Activity/Security

Auth - User Roles, Corp Context

Example Patterns of Fraud in Machine Data

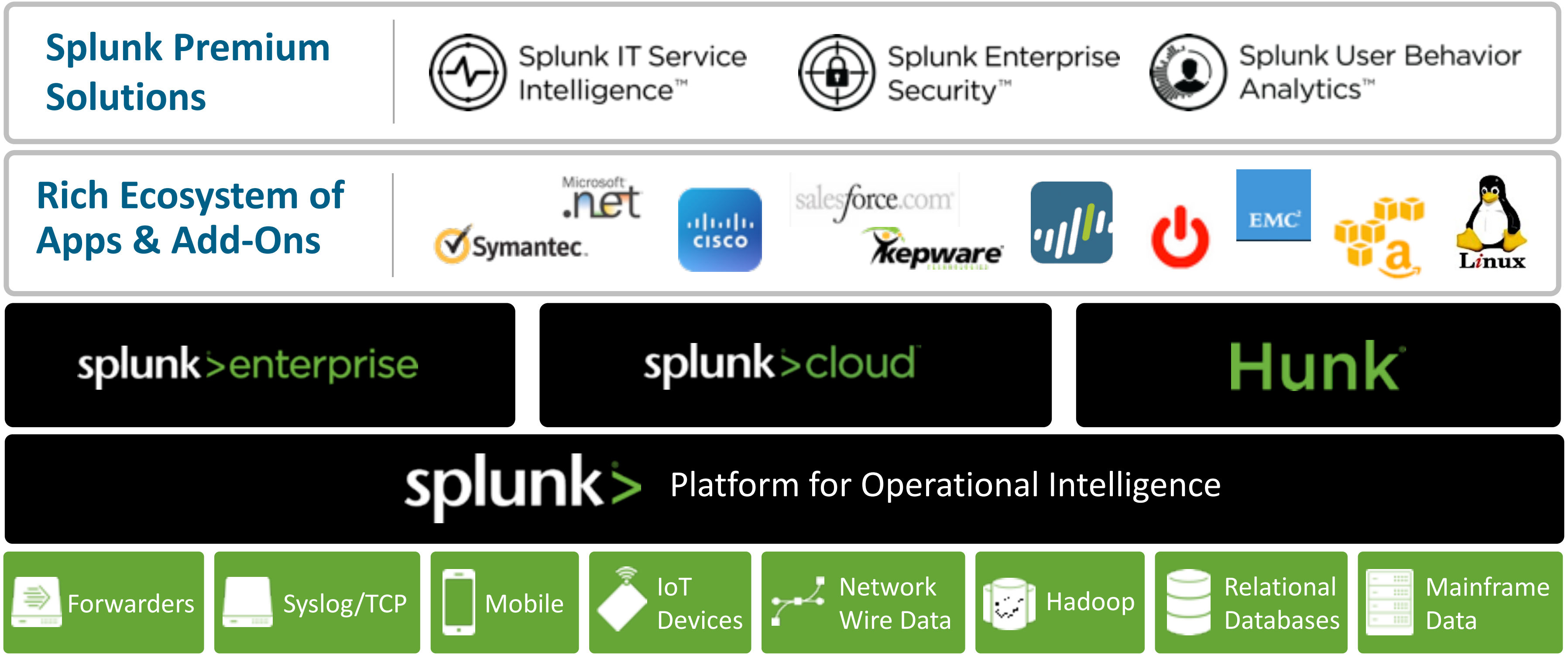
Industry	Type of Fraud/Theft/Abuse	Pattern
Financial Services	Account takeover	Abnormally high number or dollar amounts of wire transfer withdrawals
Healthcare	Physician billing	Physician billing for drugs outside their expertise area
E-Tailing	Account takeover	Many accounts accessed from one IP
Telecoms	Calling plan abuse	Customer making excessive amount of international calls on an unlimited plan
Online Education	Student loan fraud	Student receiving federal loan has IP in “high-risk” overseas country and is absent from online classrooms and forums

Insider Threat

What To Look For	Data Source
Abnormally high number of file transfers to USB or CD/DVD	**OS**
Abnormally large amount of data going to personal webmail account or uploaded to external file hosting site	**Email / web server**
Unusual physical access attempts (after hours, accessing unauthorized area, etc)	**Physical badge records / AD**
Above actions + employee is on an internal watchlist as result of transfer / demotion / poor review / impending layoff	**HR systems / above**
User name of terminated employee accessing internal system	**AD / HR systems**

Demo Time!

The Splunk Portfolio



Splunk Premium Solutions

Splunk IT Service Intelligence™

Splunk Enterprise Security™

Splunk User Behavior Analytics™

Rich Ecosystem of Apps & Add-Ons

splunk>enterprise

splunk>cloud

Hunk

splunk> Platform for Operational Intelligence

Forwarders

Syslog/TCP

Mobile

IoT Devices

Network Wire Data

Hadoop

Relational Databases

Mainframe Data

Summary

- Universal Machine Data Platform
- Real Time Architecture
- Schema on the Fly
- Agile Reporting and Analytics
- Scales from Desktop to Enterprise
- Fast Time to Value
- Passionate and Vibrant Community

Q&A