



Securing a global investment fund using Splunk Cloud and Enterprise Security

Grant Slender | CISO & Head of Security, Cloud and Support

Simon O'Brien | Principal Sales Engineer



Grant Slender

CISO & Head of Security, Cloud and Support |
QIC



Simon O'Brien

Principal Sales Engineer | Splunk

Forward-Looking Statements



During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. 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, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

Content Overview

Security, and some not-so-security focused content

People



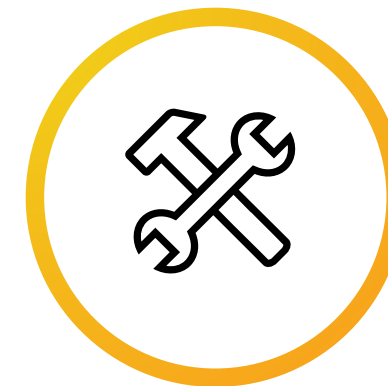
- Operational model
- Skills
- Services

Process



- Security journey
- Data onboarding
- Use case definition

Technology



- Splunk Cloud
- Enterprise Security
- Data sources

WE ARE A LONG-TERM SPECIALIST MANAGER IN ALTERNATIVES

A longstanding heritage with an established platform enabling us to become the visionary asset manager we are today.

- \$80 billion in funds under management ¹
- Over 110 clients including government, pension plans, sovereign wealth funds, universities and insurers. Spanning Australia, Europe, UK, Asia, Middle East and US
- Established in 1991 by the Queensland Government to serve its long-term investment responsibilities
- Over 1000 employees with offices in Brisbane, Sydney, Melbourne, New York, Los Angeles, Cleveland, San Francisco, London and Copenhagen



● GLOBAL INFRASTRUCTURE

● GLOBAL REAL ESTATE

● GLOBAL PRIVATE CAPITAL

● GLOBAL LIQUID STRATEGIES

● GLOBAL MULTI-ASSET

¹ As at 30 June 2019. All figures in AUD.



QIC & Splunk

The Journey so far

QIC's expectations and requirements

People



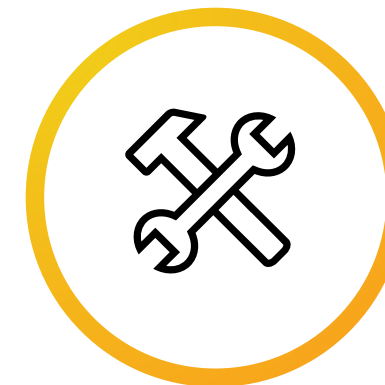
- 24x7 security capability
- Retention and skill gaps

Process



- Repeatable, consistent
- Good fit with our processes

Technology



- Integrated tooling
- Flexible and adaptable

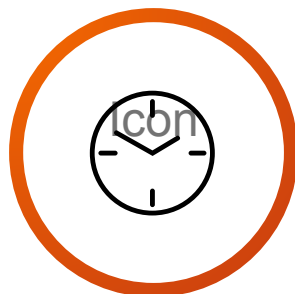
QIC's expectations and requirements

People



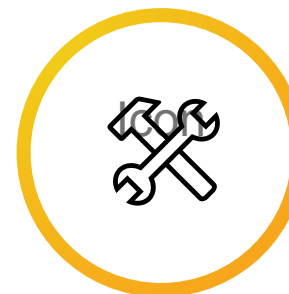
- 24x7 security capability
- Retention and skill gaps

Process



- Repeatable, consistent
- Good fit with our processes

Technology



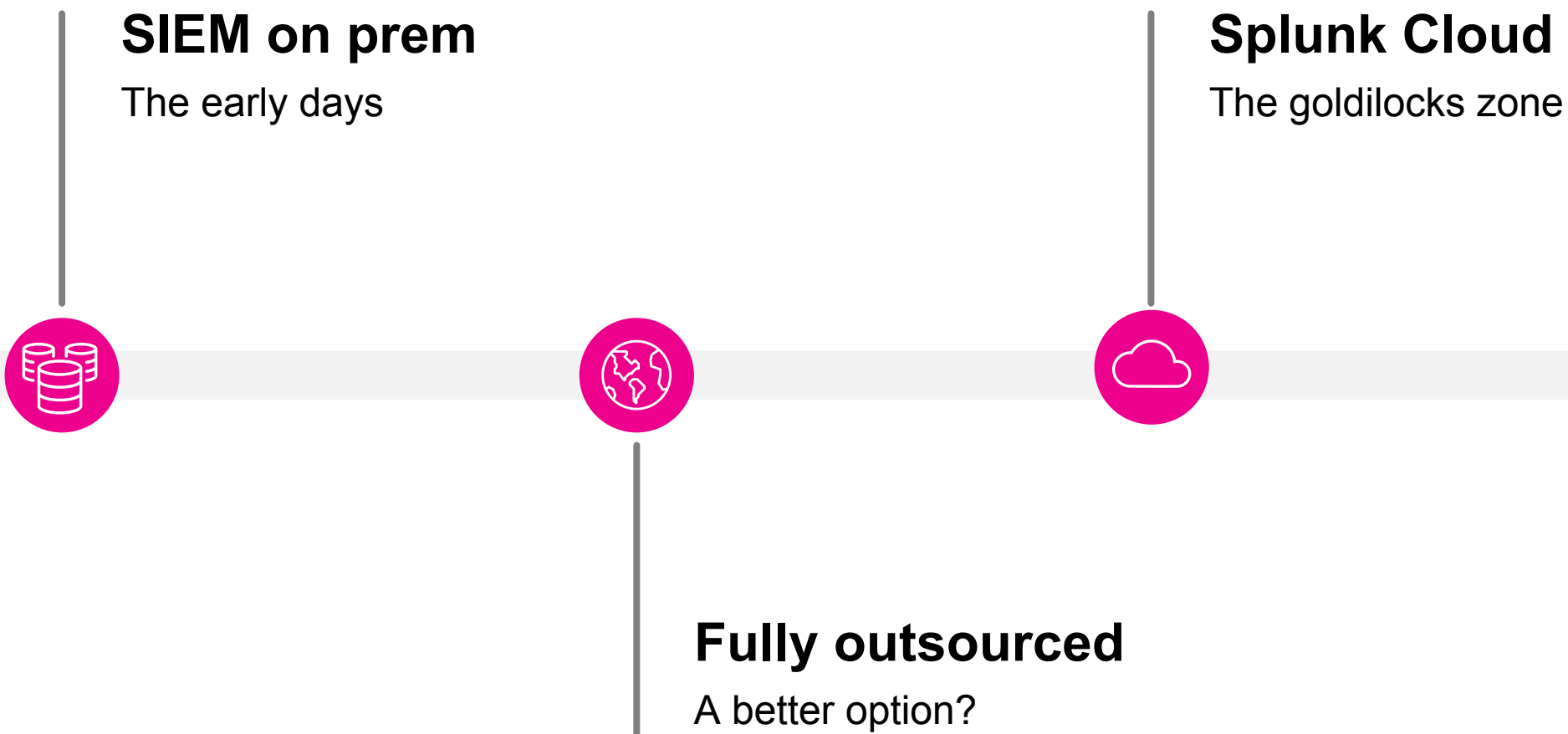
- Integrated tooling
- Flexible and adaptable



SECURE!

The journey

How QIC came to use Splunk Enterprise Security in Splunk Cloud

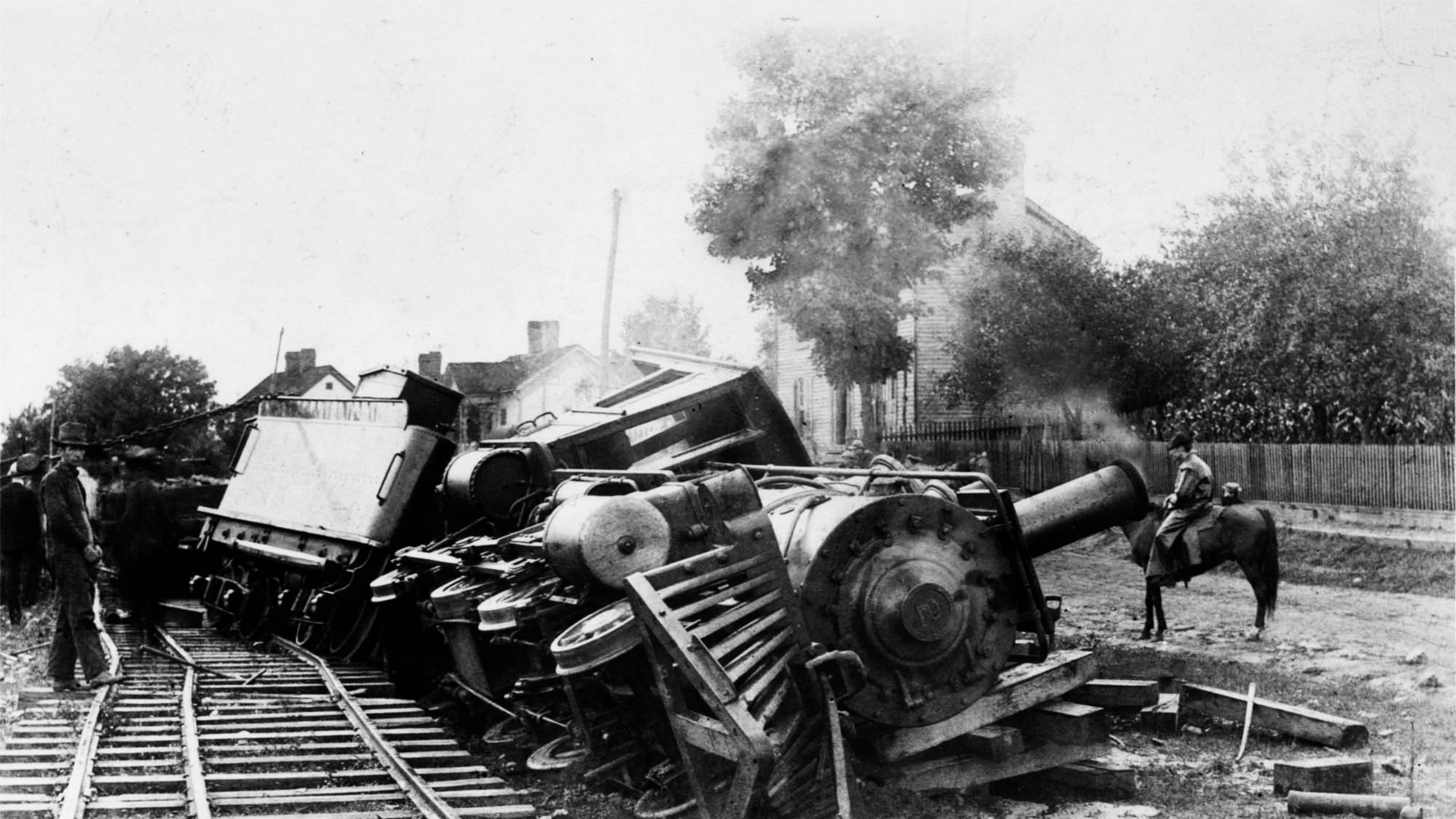


I think we have found our
goldilocks architecture.”

Grant Slender



The operational model





Operational Model

QIC personnel

Highly experienced professionals



Specialist 3rd parties

Splunk IT ops and security skillsets



External MSSP

Specialist security triage and support skillsets



Splunk Cloud

Splunk architecture, design and operations



```

      "product_id=RP-SN-01&JSESSIONID=
      F4 HTTP 1.1" 200 3739 "http://bu
      /cup-shopping.com/product.screen?produc
      t=1" "Mozilla/5.0 (Macintosh; U; Intel Mac
      /cup-shopping.com/product.screen?product_id=K9-
      -26" "Opera/9.01 (Windows NT 5.1; U; en)" 513 12,
      jows NT 5.1; U; en)" 539 10.2.1.44 - [07/Jan 18:10
      -01" "Opera/9.20 (Windows NT 6.0; U; en)" 559 128.241.220.82
      .1)" 317 27.160.0.0 - [07/Jan 18:10:56:156] "GET /oldlink?item_id
      d 125.17.14.100 - [07/Jan 18:10:56:147] "POST /category.screen?category
      18:10:55:189] "GET /cart.do?action=changequantity&item_id=EST-18&product_id
      item_id=EST-6&JSESSIONID=SD10SL8FF2ADFF9 HTTP 1.1" 200 3865 "http://buttcru
      IADFFG HTTP 1.1" 200 3971 "http://buttcru-shopping.com/cart.do?action=remov
      outtcru-shopping.com/oldlink?item_id=EST-21" "Mozilla/4.0 (compatible; MSIE 6.0; Window
      action=remove&item_id=EST-15&product_id=AV-58-20" "Mozilla/4.0 (compatible; MSIE 6.0; Windows
      id=EST-17&product_id=K9-CW-01" "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_3; en-US) App
      iL3FF1ADFF4 HTTP 1.1" 404 2258 "http://buttcru-shopping.com/cart.do?action=addtocart&item_id=EST-
      FP 1.1" 200 488 "http://buttcru-shopping.com/cart.do?action=purchase&item_id=EST-27&product_id=FL-
      product_id=RP-SN-01&JSESSIONID=SD7SL8FF3ADFF2 HTTP 1.1" 200 1901 "http://buttcru-shopping.com/car
      IQUETS&JSESSIONID=SD10SL1FF4ADFF10 HTTP 1.1" 406 1437 "http://buttcru-shopping.com/cart.do?action=
      6 - - [07/Jan 18:10:53:118] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD7SL3FF9ADFF10 H
      tory.screen?category_id=BOUQUETS&JSESSIONID=SD3SL1FF7ADFF2 HTTP 1.1" 200 2567 "http://buttcru-sho
      id=SD8SL2FF5ADFF2 HTTP 1.1" 200 1649 "http://buttcru-shopping.com/category.screen?category_id=TE
      200 223 "http://buttcru-shopping.com/category.screen?category_id=BOUQUETS" "Mozilla/5.0 (Maci
      0&JSESSIONID=SD6SL2FF3ADFF4 HTTP 1.1" 200 363 "http://buttcru-shopping.com/product.screen?
      9 3326 "http://buttcru-shopping.com/product.screen?product_id=FL-DLH-02" "Mozilla/4.0 (co
      oduct.screen?product_id=RP-SN-01" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
      -illa/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 790 128.241.220.82 - [07/Jan 1
      ble; MSIE 6.0; Windows NT 5.1; SV:1 .NET CLR 1.1.4322) 380 195.80.144.77

```

Maximizes value
from limited
resources

Managing Splunk Is More Than Just Software

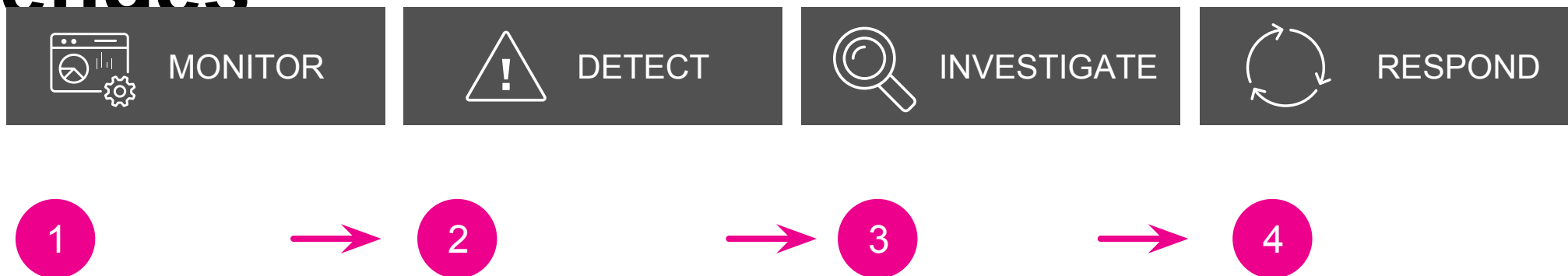
© 2019 SPLUNK INC.

	Responsibility	Splunk Ent Deployed On-Premises	Splunk Cloud
Admin Tasks: One-time Setup	Purchase/rent HW	QIC	Splunk
	Rack and stack, cable, network all HW	QIC	Splunk
	Install Splunk	QIC	Splunk
	Install OS	QIC	Splunk
	Configure Splunk (create users, load apps, configure)	QIC	Splunk
	Configure indexes	QIC	Splunk
	Setup HA/clustering	QIC	Splunk
	Setup disaster and recovery	QIC	Splunk
	Configure forwarders	QIC	Joint
	Onboard data	QIC	QIC/MSSP
	Integrate with LDAP/AD	QIC	Joint
Admin Tasks: Ongoing	Scale up HW	QIC	Splunk
	Install Splunk patches / upgrades	QIC	Splunk
	Install OS patches / upgrades	QIC	Splunk
	Monitor deployment / health checks	QIC	Splunk
	Manage forwarders	QIC	QIC
	Create users / roles	QIC	QIC/MSSP
	Manage indexes	QIC	QIC/MSSP
	Onboard additional data	QIC	QIC/MSSP
	Load search head only apps	QIC	Splunk
	Load distributed apps	QIC	Splunk
	Load premium apps	QIC	Splunk
	Export data	QIC	Splunk
User Tasks	Search, alerts, reports, dashboards	QIC	MSSP/QIC/3 rd Parties

Managing a Splunk deployment involves 12 on-going admin tasks, 8 of which are conducted by Splunk for a Cloud based deployment



Splunk Enterprise Security Addresses Security Operations Challenges



KEY FEATURES



Splunk Enterprise
Security™

SECURITY WORKFLOW

Notable Event Framework

EVENT CORRELATIONS

Search Management

**SECURITY
ENRICHED CONTEXT**
Asset, Identity Framework

THREAT INTELLIGENCE

Threat Intel Framework

RISK BASED ANALYTICS

Risk Scoring Framework

ADAPTIVE RESPONSE

Adaptive Response Framework



Data onboarding process

What Your Executives Want



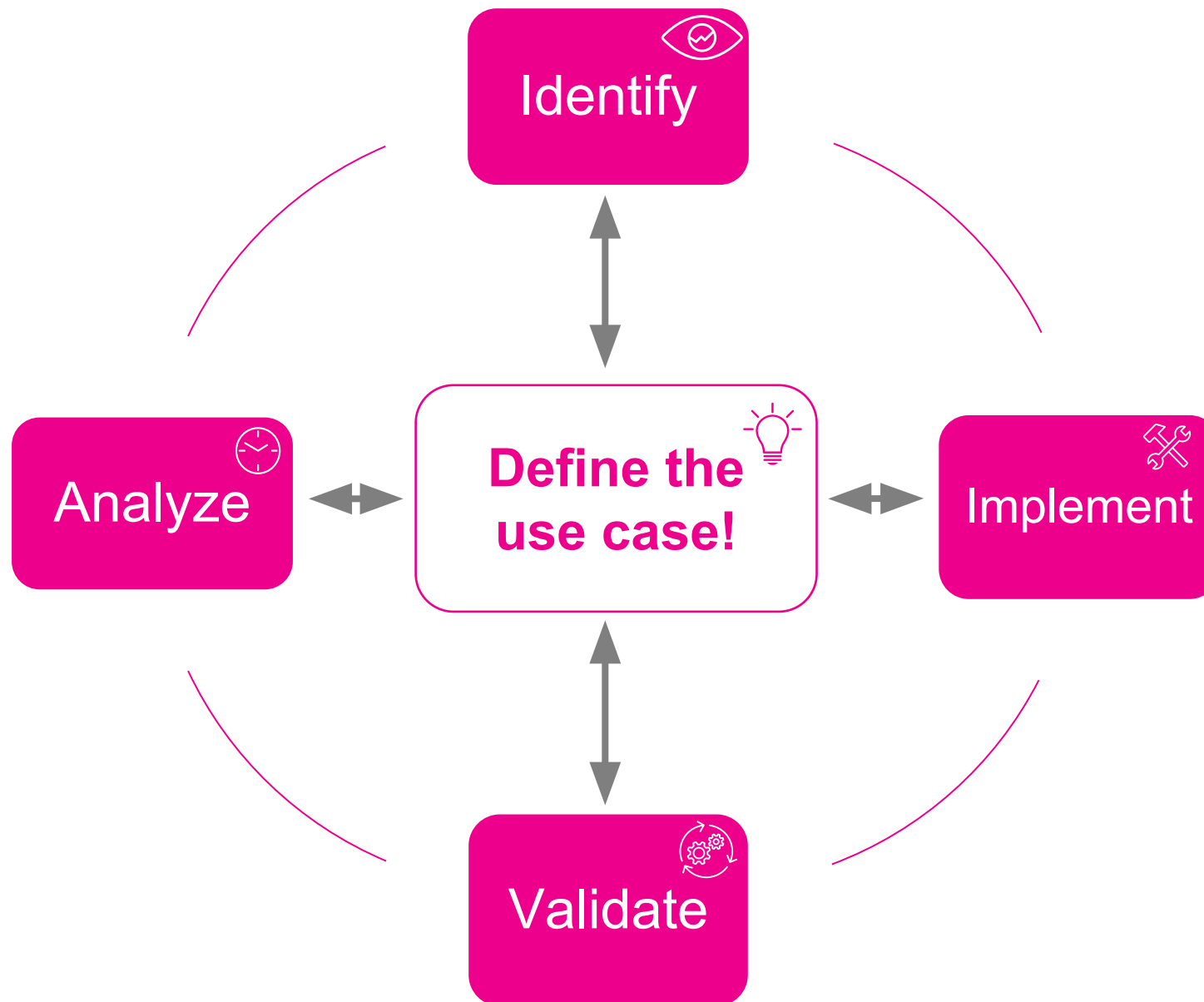
Splunk is not expensive.
People are just **lazy.**”

Grant Slender

Don't just throw data into
Splunk. Define your **use case**
first!”

Grant Slender

Data onboarding process



What Can Splunk Ingest?

Agent-Less and Forwarder Approach for Flexibility and Optimization

Aggregated/API Data Sources

Heavy Forwarder



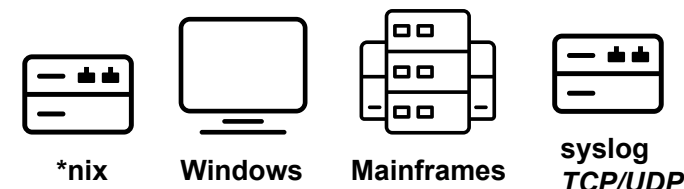
Event Logs, Active Directory, OS Stats
Unix, Linux and Windows hosts

Universal Forwarder



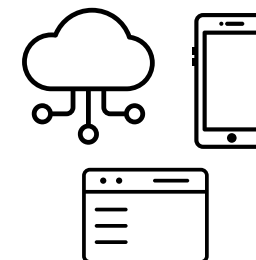
Local File Monitoring

Universal Forwarder

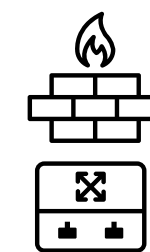


DevOps, IoT, Containers

HTTP Event Collector
(Agentless)



Wire Data
Splunk Stream
Universal Forwarder or
HTTP Event Collector



splunk> .conf19

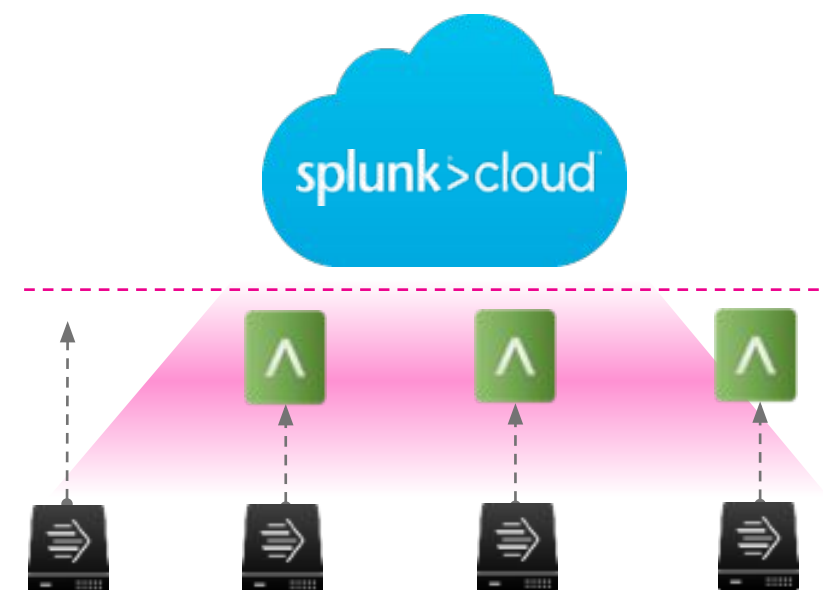


Use case overview

Endpoint security posture improvements

Detection of brute force RDP connection attempts

- User working from home using a bridged connection to the Internet. UF deployed to ALL hosts.
- Target of brute force attacks from an IP in Europe.
- Attackers trying to authenticate to RDP with multiple usernames.
- WinEventLogs sent in almost real time from anywhere to Splunk allowed a use case to trigger an alert on the activity.
- The unusual activity prompted an investigation that helped uncover a misconfiguration on the endpoint firewall.



Custom threat intelligence

Provided through managed security services provider

- Custom TA deployed by SOC team to integrate threat feed into ES framework
- Mapped into Threat Framework to provide actionable insights to analysts based on trusted intel
- Generating hits against multiple data sources
- Tracking in excess of 9000 threats
- Has prompted action against vulnerability analysis

Most Active Threat Collections		
threat_collection ▾	search ▾	sparkline ▾
ip_intel	Source And Destination Matches	

Cisco device change monitoring

Detection of changes on critical devices

Notable deployed to identify changes to critical devices within the environment.

Custom notable developed and deployed through use case development process.

Adaptive response includes forwarding event to outsource SOC provider, via custom TA with actions.

Detected the cutover to new outsource network provider within short timeframe.

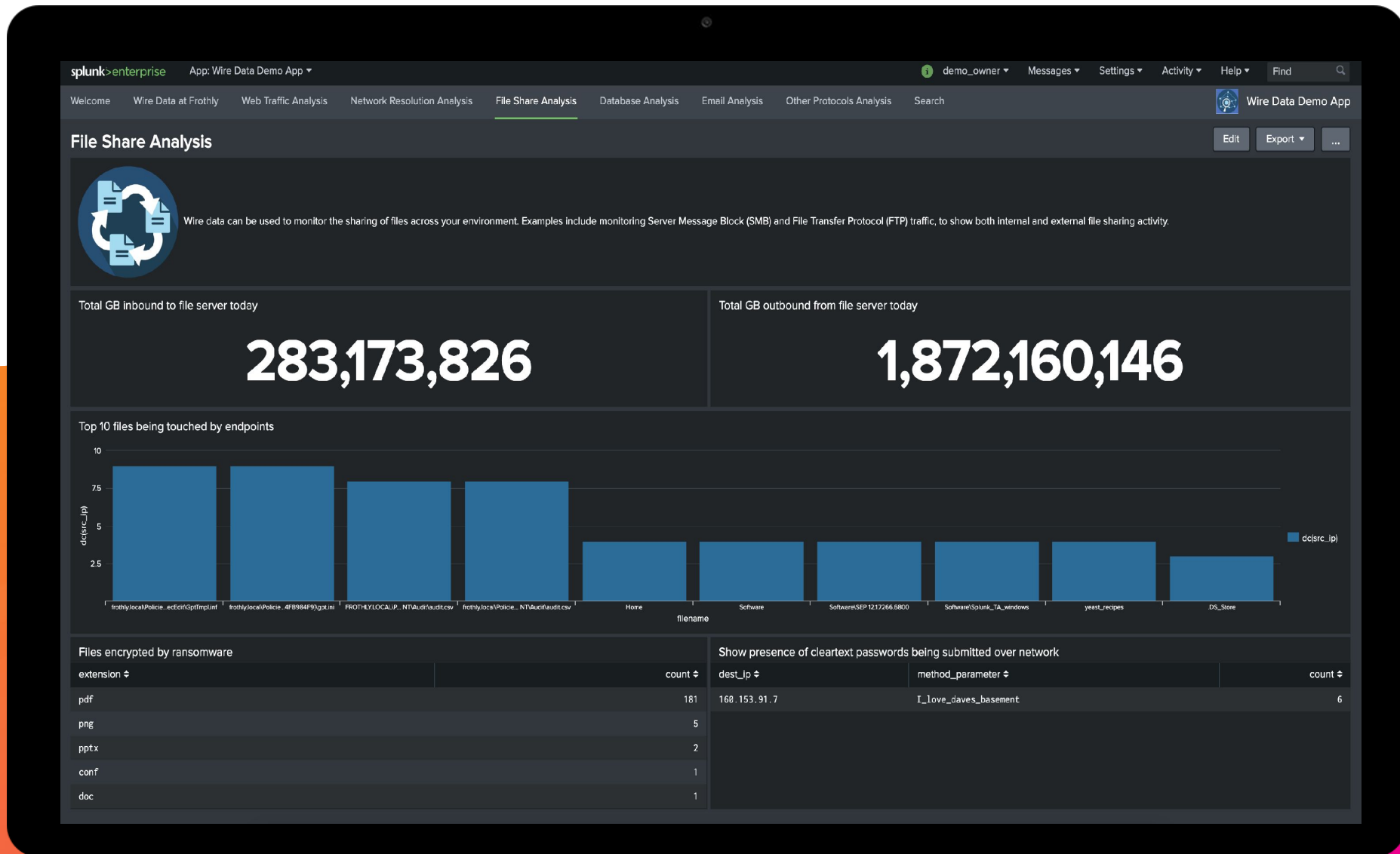
The screenshot shows the 'Adaptive Response Actions' configuration interface in Splunk. At the top, a 'Correlation Search' section is visible with a search name of 'Cisco Router Configuration Modification Detecte' and an application of 'Enterprise Security'. Below this, the 'Adaptive Response Actions' section is expanded, showing a 'Notable' event. Under the 'Notable' event, a 'Data Forwarder' action is configured. The configuration includes the following fields:

- Category:** Security (selected)
- Type:** Alert (selected)
- Action Type:** SOC
- Urgency:** Medium
- Impact:** Medium
- Title:** ProSOC Alert Notification - \$result.alert
- Message:** QIC Team, Proficio has detected a Cisco Router configuration change. Details of the event are as follows:



Business focussed outcomes

What we achieved outside the security world

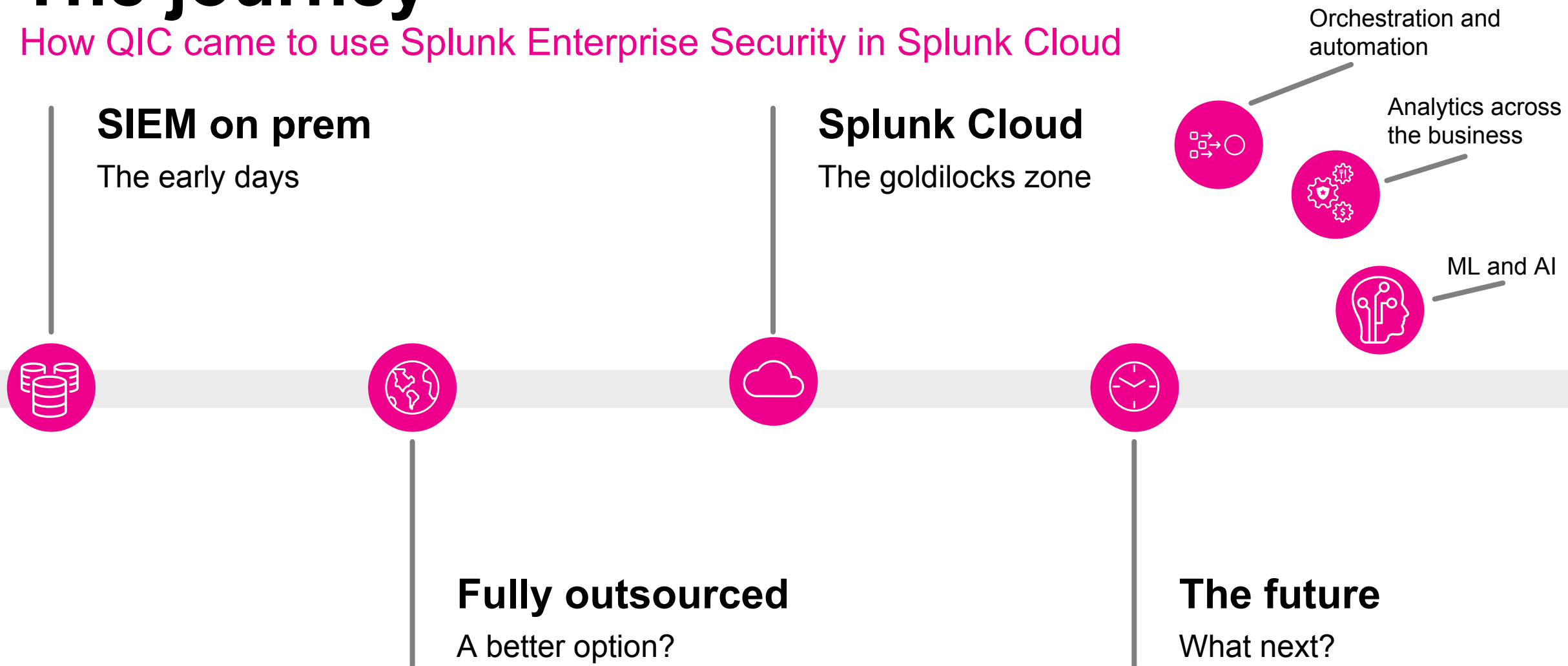




The future

The journey

How QIC came to use Splunk Enterprise Security in Splunk Cloud



Key Takeaways

1. Consider the people, process and technology aspects of your organizational requirements
2. Define use cases and security visibility requirements first, then on board data!
3. Iterate. You (probably) won't get this all right the first time around!



Q&A

Grant Slender |
CISO & Head of Security, Cloud and Support |
QIC

Simon O'Brien |
Principal Sales Engineer | Splunk



Thank

You



Go to the .conf19 mobile app to

RATE THIS SESSION

