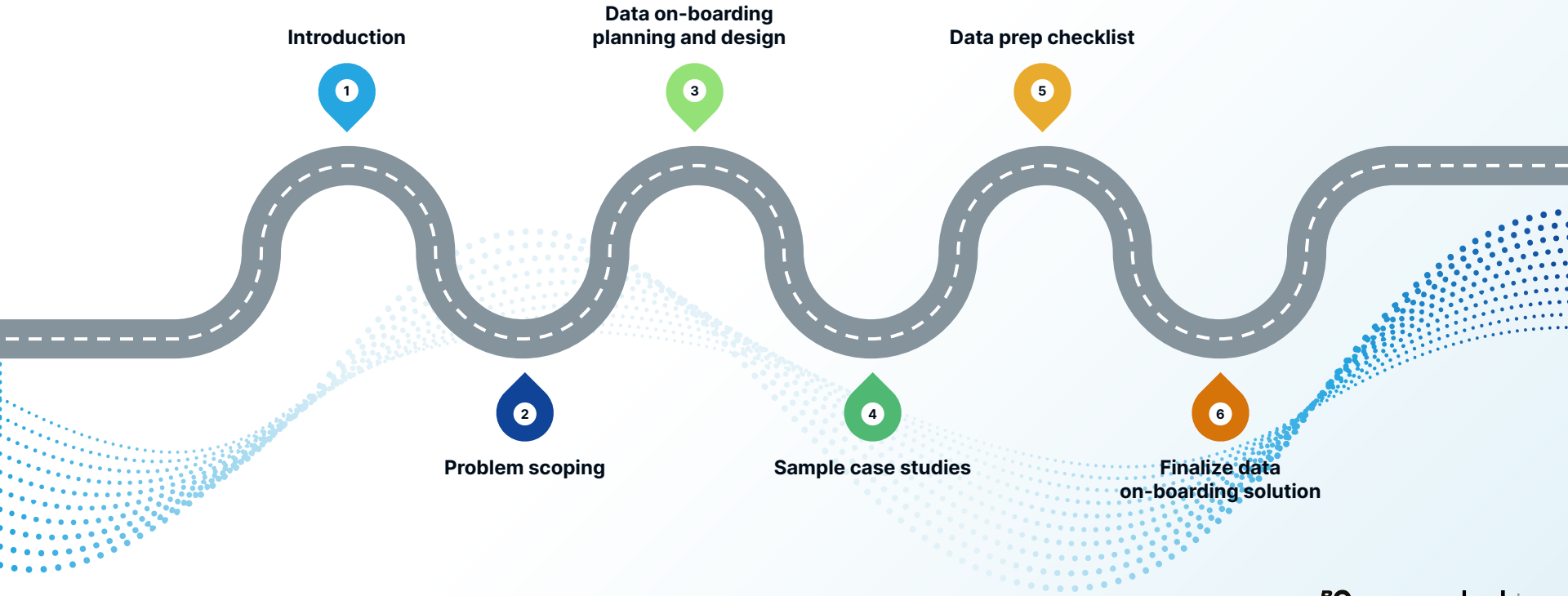
CYBERSECURITY RECIPES FOR MATURE AND EFFECTIVE SECURITY CONTENT

Henry Canivel

Roadmap


Introduction
1
Problem scoping
2
Data on-boarding planning and design
3
Sample case studies
4
Data prep checklist
5
Finalize data on-boarding solution
6

whoami

Henry Canivel

- Security Architect splunk>
- Key Words: Security, Data Science, Automation, Software Development, Data Engineering, Python, Cloud Security
- Splunking since 2009!
  - Customer
  - PS Consultant
  - App Developer
  - Admin
  - Architect

Things we will learn + cover

What are we going to do today?

- Framework for building technical requirements for security use cases
- Deep dive for discovery of data visibility
- Walkthrough for performing data engineering due diligence

Security Keyword Bingo

Make your head spin

- Monitoring and Triaging
- Incident Response
- Threat Hunting
- SOC
- Compliance
- Automation
- Security Analytics
- Machine Learning
- Behavioral Analytics
- Malware Analysis
- Network Security
- Endpoint Telemetry
- Threat Intelligence
- Cloud

BSIDES splunk>

What are we trying to do?

What are we trying to *deliver?*

BSIDES splunk>

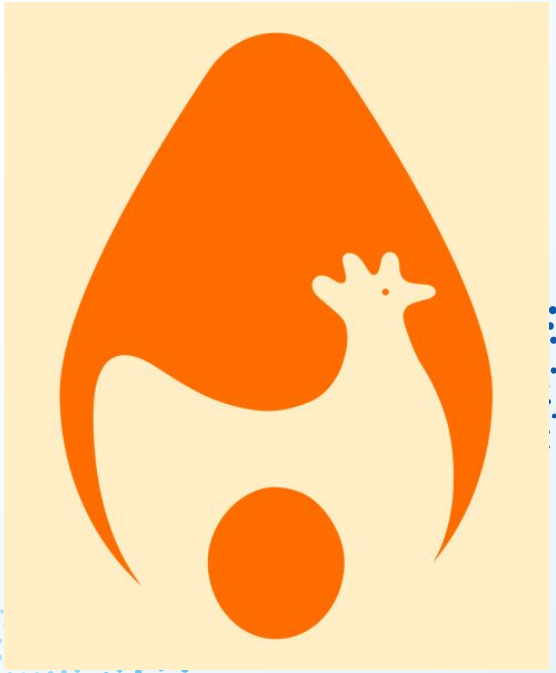
Data onboarding drivers

- Real-time monitoring
- Threat intelligence
- Behavior profiling
- Data and user monitoring
- Application Monitoring
- Analytics
- Log management and reporting
- Operational and compliance reporting

Problem Statement

What are you trying to address?

- I have a *SOC use case* with missing data, need to fix the **data gap**.
- I have **data**, need to figure out what *SOC use cases* can benefit.



But what's the **REAL** problem?

“

I don’t know where to **start**.

It’s too **hard**.

I don’t know what to **do**.

I don’t **not an expert** in (X).

Common delivery roadblocks

What are reasons you'd hesitate from engaging this task?

- Not a security specialist
- Not the data SME
- Not a SOC engineer
- Not a Splunk app developer

Don’t worry.

Let’s just take it **one** step at a time.

Scope

- Data engineering implementation focused
- Most data requirements already established
  - E.g., I need <this> data in Splunk to {analyze, populate into dashboard, populate into alert}
- SOC use case OR data source has already been identified
- Design a data engineering implementation plan

Why **this** way?

Focus

- On what you can do (within Splunk + data source)
- Clear deliverables and implementation tasks
  - Read: Splunk engineering tasks
- Rely on defined use cases for foundation
- Discover and define data engineering requirements

Perspective … *preview*

What we want to cover today!

Will do:

- Help you design data collection solution
- Identify areas of consideration from data source, use case
- Identify what will be needed for Splunk app development

Won't do:

- Design entire SOC use case
- Integrate SOC use case within your monitoring portfolio

Goals
Takeaways
Expectations

assert(this.talk == “useful”)

Goals

What if I told you ...

You can take on the world

Set realistic expectations

Empower New Splunk Champions!

#SessionGoals

- Share experience, knowledge of working with Splunk for the *security* domain
  - As a Splunk admin
  - As a developer
  - As a security professional
  - As a data engineer
- Showcase a real world workflow/checklist for data on-boarding
- Enable **YOU** with new tools and techniques

Attendee Takeaways

- More effectively draw security value from any data source
- Possess knowledge to deploy optimized integrated Splunk solutions
- Know where to start building custom content, apps

Recommended Skill sets and Aptitude

Know who you are

- Basic comprehension of IT/infrastructure architecture
  - [ideal] knowledge of Splunk deployment
- Saved a Splunk search
- Curiosity to tackle technical challenges
- Involved with security projects or monitoring
  - Design, implementation, or even request
- Basic idea of what you want to do!

So, what's involved?


People
Process
Technology

People

- Stakeholders
  - Leadership
  - Audit
  - Non-security teams
- SOC
  - Analysts
  - Engineers

Processes

- Threat modeling
- SOC use case SDLC
- Intrusion analysis
  - Diamond model
  - Cyber Kill Chain
  - MITRE ATT&CK
- Data on-boarding

Technology

- ...

People

NOPE,

Won’t go into this one

Processes

Only some of it

Processes

- ~~Threat modeling~~
- SOC use case SDLC
- Intrusion analysis
  - Diamond model
  - Cyber Kill Chain
  - MITRE ATT&CK
  - Pyramid of Pain
- Data on-boarding

Where/how does data on-boarding fit into these processes?

Data onboarding

Traditionally to address marketing needs in delivering offline data to online platforms, in our scenario, the delivery of data sources into Splunk environment to enable operational and security needs.

How does the SOC benefit?

Mainly: service, environment visibility

- Analysis
- Detection and Monitoring
- Investigation/incident response

Intrusion Analysis

- US Dept of Defense Diamond Model
  - Adversary, Capability, Victim, Infrastructure
- Lockheed Martin Cyber Kill Chain
  - Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control (C2), Actions on Objectives
- MITRE ATT&CK
  - Adversarial Tactics, Techniques, and Common Knowledge
- Pyramid of Pain
  - Note: Not really a process for intrusion analysis, but certainly still helps provide context to defending against an adversary through your organization's technology

Intrusion Analysis

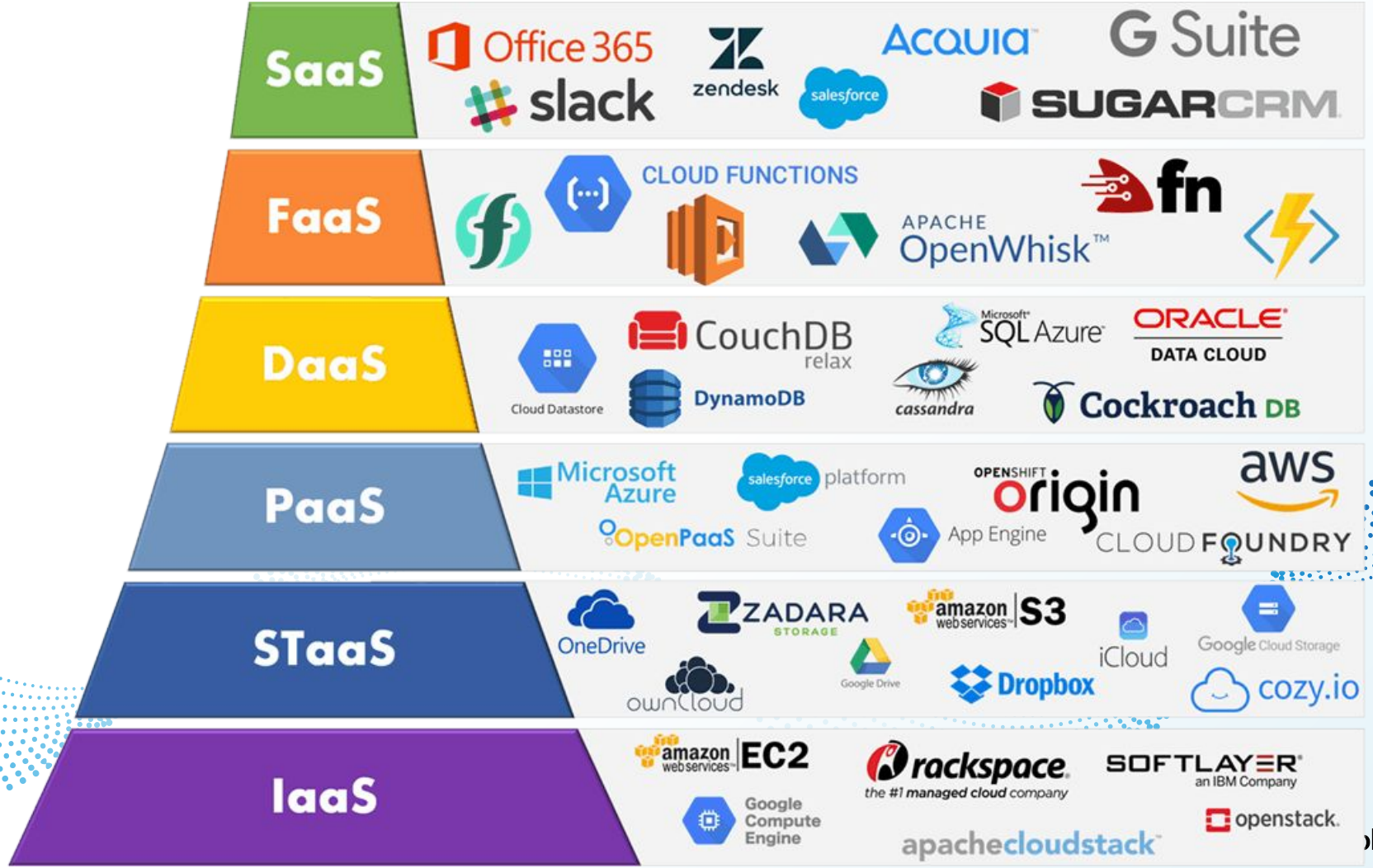
Bottom line

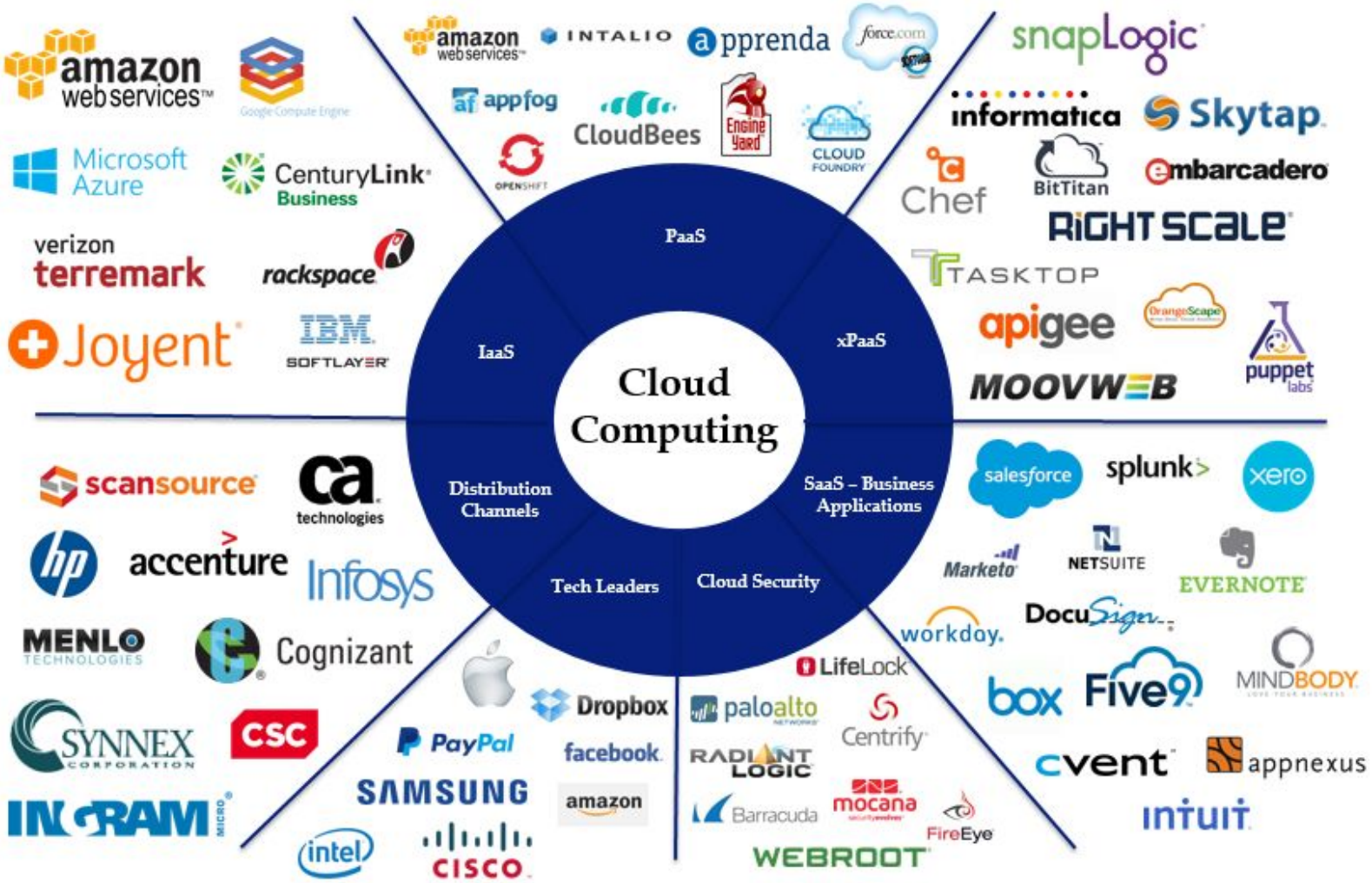
- All intrusion analysis models require the capability to capture:
  - Action event that happened
  - Who triggered this action
  - If applicable, onto what object or process was the action exacted
  - When did it happen
- Can we identify severity of the event activity? Why is this important?
  - Implicitly, inferred from the use case and analytic request for this data
  - Explicitly indicated within the data itself
- Need to validate if this event data can be captured

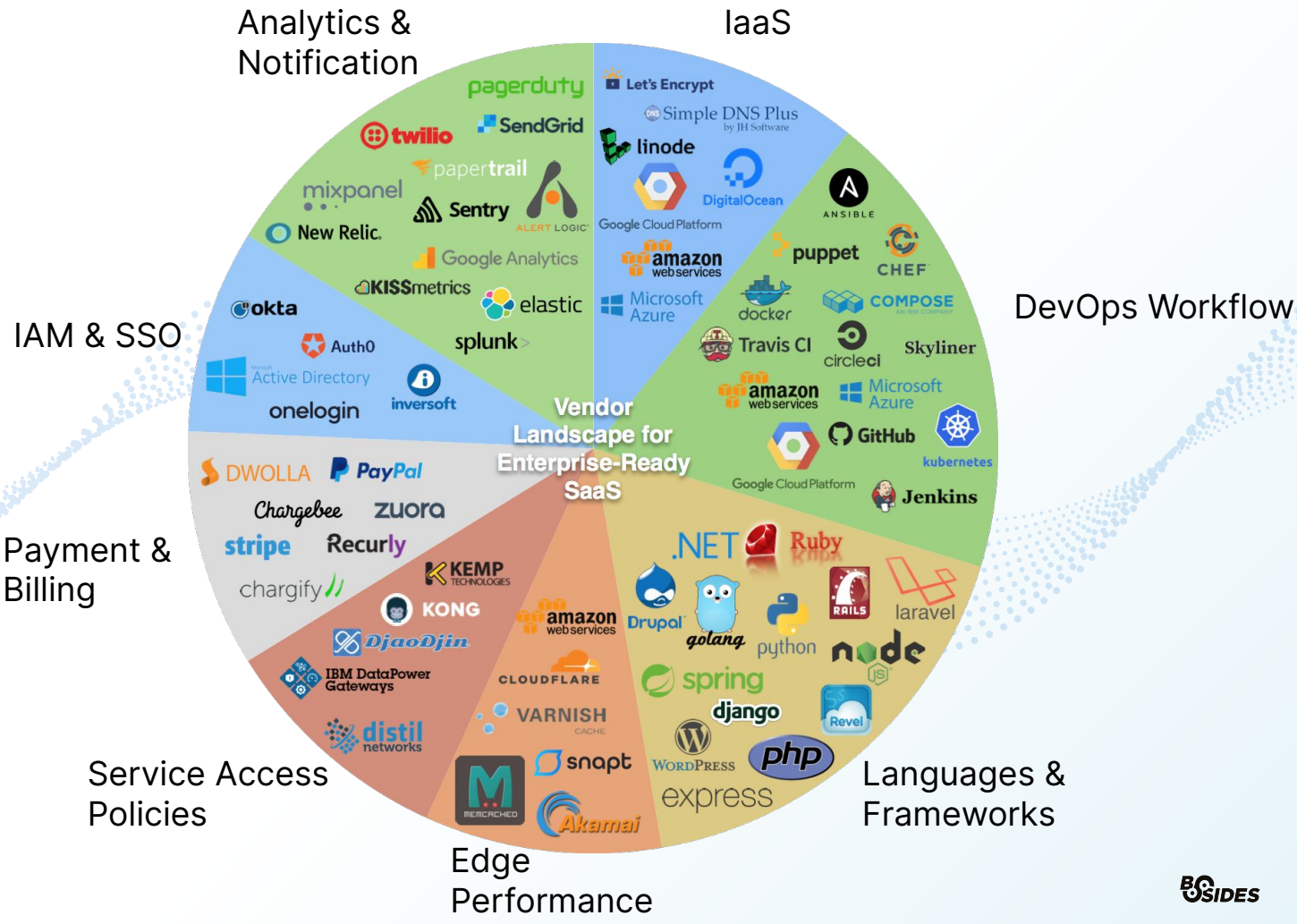
Perspective on SOC use case

How do we supply the event data for this visibility?

Technologies

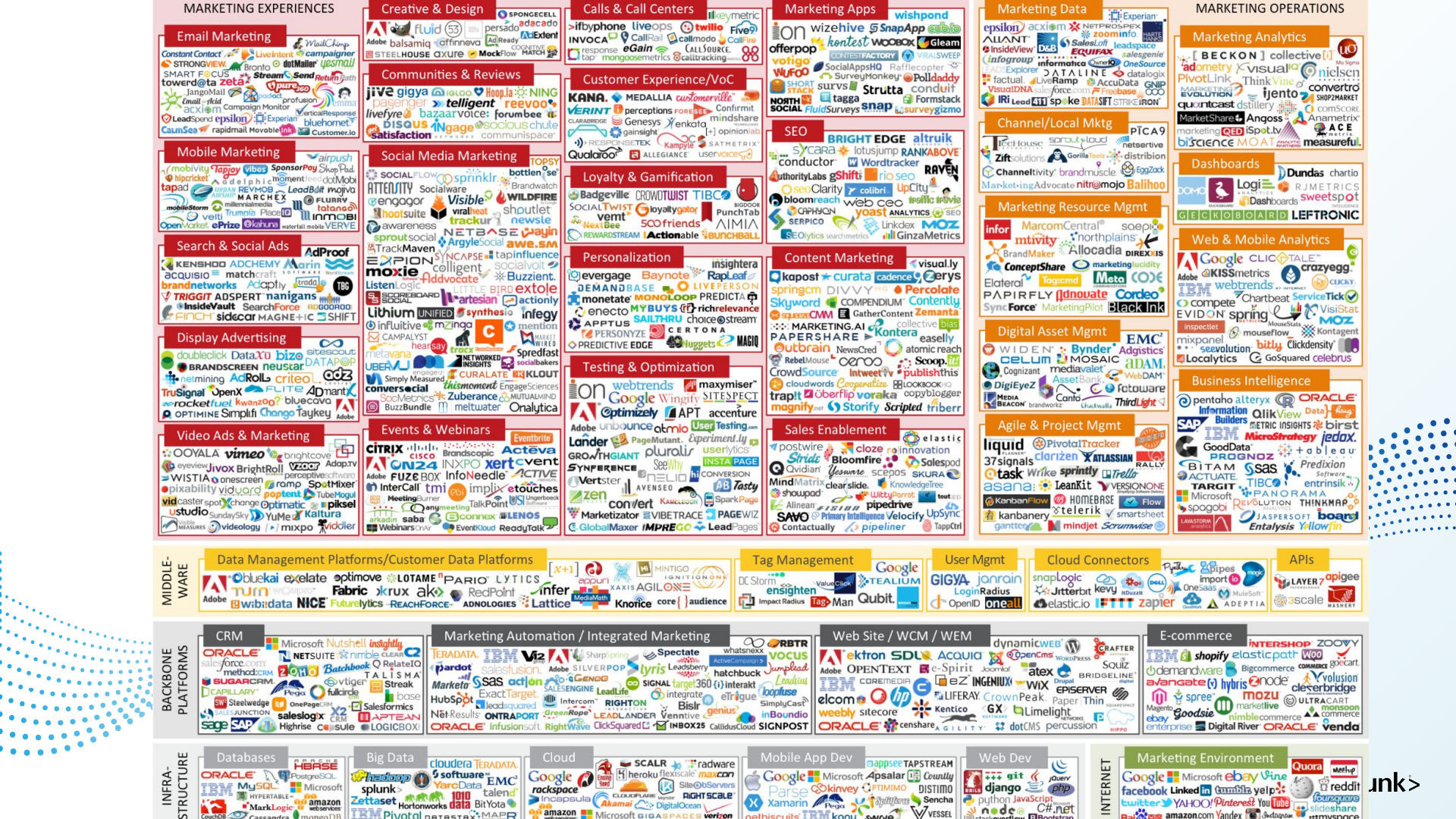

SaaS
Office 365
slack
zendesk
salesforce
Acquia
G Suite
SUGARCRM
FaaS
CLOUD FUNCTIONS
APACHE
OpenWhisk™
fn
DaaS
Cloud Datastore
CouchDB
relax
DynamoDB
Microsoft SQL Azure
cassandra
ORACLE
DATA CLOUD
Cockroach DB
PaaS
Microsoft Azure
salesforce platform
OpenPaaS Suite
App Engine
OPENSHIFT
origin
CLOUD FOUNDRY
aws
STaaS
OneDrive
ZADARA
STORAGE
owncloud
Google Drive
amazon web services S3
Dropbox
iCloud
Google Cloud Storage
cozy.io
IaaS
amazon web services EC2
Google Compute Engine
rackspace
the #1 managed cloud company
SOFTLAYER
an IBM Company
openstack
apachecloudstack


Cloud Computing
PaaS
xPaaS
SaaS – Business Applications
Cloud Security
Tech Leaders
Distribution Channels
IaaS
amazon web services
Google Compute Engine
Microsoft Azure
CenturyLink Business
verizon terremark
rackspace
Joyent
IBM SOFTLAYER
amazon web services
INTALIO
apprenda
force.com
appfog
CloudBees
Engine Yard
OPENSHIFT
CLOUD FOUNDRY
snapLogic
informatica
Skytap
Chef
BitTitan
embarcadero
RIGHTSCALE
TASKTOP
apigee
OrangeScape
puppet labs
MOOVWEB
scansource
ca technologies
hp
accenture
Infosys
MENLO TECHNOLOGIES
Cognizant
SYNNEX CORPORATION
CSC
INGRAM MICRO
PayPal
Dropbox
facebook
SAMSUNG
amazon
intel
CISCO
LifeLock
paloalto
Centrify
RADIANT LOGIC
Barracuda
mocana
FireEye
WEBROOT
salesforce
splunk>
xero
Marketo
NETSUITE
EVERNOTE
workday.
DocuSign
box
Five9
MINDBODY
cvent
appnexus
INTUIT



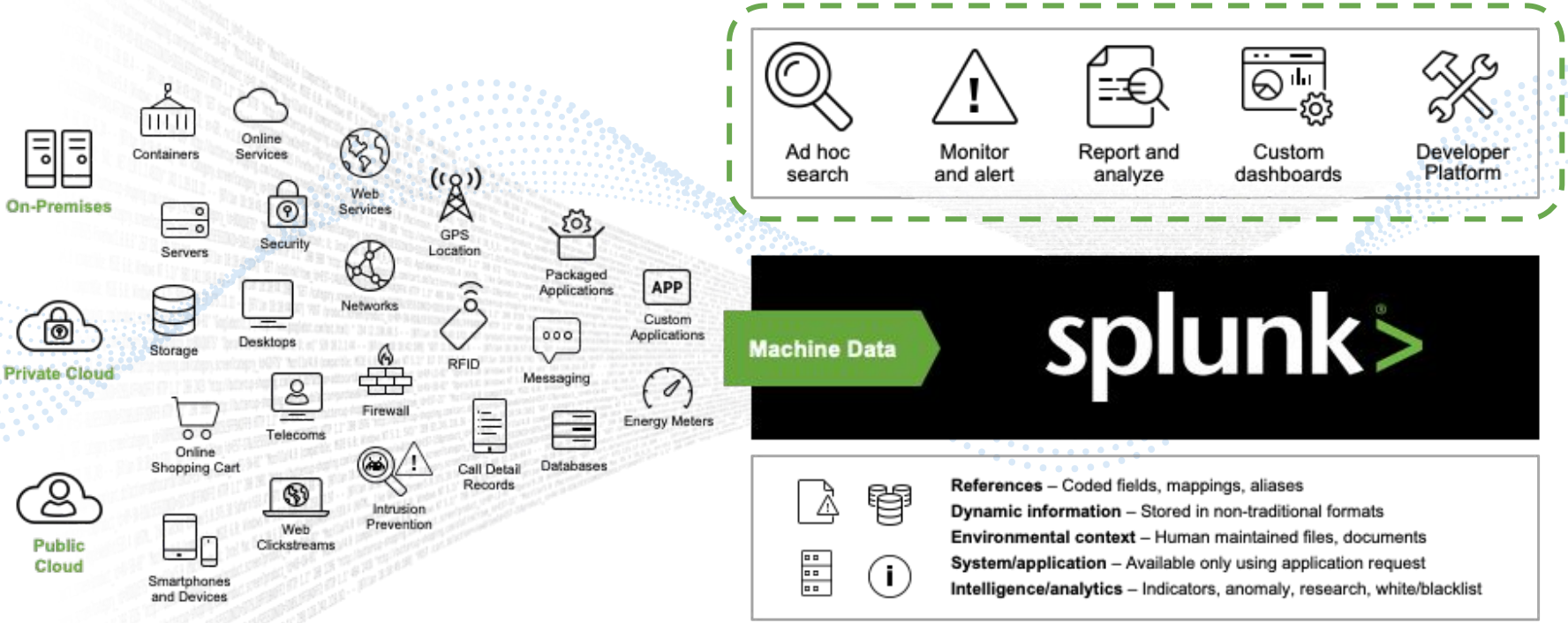
BSIDES splunk>


Predict & Prevent
Enrich data input and detection
Detect
Respond
and protect
Network Traffic Analysis (NTA) & Anomaly detection
User and Entity Behavior Analytics (UEBA/UBA)
Vulnerability Assess. (VA) Config audits and Compliance
Risk Intelligence (IRMS) & prioritization
Deception Based Detection
Threat Intelligence Automation and Sharing
Offensive Security
Code Testing
Cyber Situational Awareness
LOG , SIEM and Big Data Platforms
Integrity Based Assurance and Detection
Sandbox Analysis
Threat Intelligence Platforms (TIPS)
Endpoint Detection & Response (EDR) & Malware
Hunting
Machine Data Analytics & Big Data / Security Operations, Analytics and Reporting (SOAR)
Data Analytics and Visualization
Exfiltration detection, DLP
Endpoint Protection (EPP)
Content Disarm & Reconstruction CDR
DLP for the Cloud
IAG – Identity and Access Governance
Incident Response Orchestration and Automation & Situational Awareness
MSSP Content Security Web and Mail
IDaaS and CASB - Cloud Access Security Broker
IoT Security
Encryption and Key Management
Security Automation and DevOps
Threat Protection for SaaS
Cloud based CDN, DDoS, WAF, ADC
Tokenization, DLP, Monitoring, Encryption
Mobile Device Security
OT/SCADA Security
App Segmentation & Hardening
Micro Segmentation of Docker Containers
Backup into the Cloud


MARKETING EXPERIENCES
Email Marketing
Mobile Marketing
Search & Social Ads
Display Advertising
Video Ads & Marketing
Creative & Design
Communities & Reviews
Social Media Marketing
Events & Webinars
Calls & Call Centers
Customer Experience/VoC
Loyalty & Gamification
Personalization
Testing & Optimization
Marketing Apps
SEO
Content Marketing
Sales Enablement
Marketing Data
Channel/Local Mktg
Marketing Resource Mgmt
Digital Asset Mgmt
Agile & Project Mgmt
MARKETING OPERATIONS
Marketing Analytics
Dashboards
Web & Mobile Analytics
Business Intelligence
MIDDLE-WARE
Data Management Platforms/Customer Data Platforms
Tag Management
User Mgmt
Cloud Connectors
APIs
BACKBONE PLATFORMS
CRM
Marketing Automation / Integrated Marketing
Web Site / WCM / WEM
E-commerce
INFRA-STRUCTURE
Databases
Big Data
Cloud
Mobile App Dev
Web Dev
INTERNET
Marketing Environment

Simplify

Focus on what you want to enable



Lean on established success paths for security

Frameworks are a great place to start

- NIST
- **OWASP**
  - OWASP Top 10
  - Logging Cheat Sheet
- SANS Critical Security Controls
- AAA
  - Authentication, authorization, and accounting

Quick summary for OWASP logging cheat sheet

Capture the following recommended types of events

- Access & authentication
  - Data access
  - Service access
- Authorization (access control)
- Session management
- System/process events
  - e.g., start-up/shut-down
- Admin/service change management
- User activities: action x object
  - Data export/downloading
  - Scheduled job configuration

Prioritize your desired data quality

Based on level of effort and visibility requirements

Minimal

- Access & authentication
- Admin/service change management
- Session management
  - Depends on service

Ideal

- Access & authentication
- Authorization (access control)
- Session management
- System events
  - e.g., start-up/shut-down
- Admin/service change management
- User activities: action x object
  - Data export/downloading
  - Scheduled job configuration

Collection methods

- API / webhooks
- 3rd party tools, integrations
  - closed
  - open source
- Native tools and capabilities
  - E.g., syslog, file writing

Resources

How can you discover what is available?

- Product documentation
  - Administrator guides
  - API specifications
  - Community resources (e.g., blogs, solution guides)
- Google/OSINT
  - 3rd party tools
  - Github
- Splunk!
  - Splunkbase
  - Documentation
  - Blogs
- Partners/community
  - Splunk User Slack

Data Engineering

Bring it back into Splunk for tie-in

- Collect into Splunk
  - Add-On Builder
  - Splunk developer
  - Splunk file monitoring inputs
- Splunk content
  - Searches / ES Correlation Searches
  - Field extractions
  - Macros
  - Dashboards
  - Lookups
- Data mapping
  - CIM
  - ES Threat Intel Framework
  - Add-On Builder

Data onboarding process

1. Target use case(s)
   - Identify visibility gaps to activity/event or IOC if possible
2. Technologies/applications
   - Identify and review product resources
3. Data requirements
   - Scope for level of effort
   - Qualify data quality
     - minimum
     - ideal
4. Data engineering
   - Methodologies for data collection
   - Data analysis and quality
   - Map data into Splunk

Security data onboarding checklist

- Planning
  - Verify motivation
  - Validate and quantify visibility gaps
  - Resource allocation
  - Timing and alignment of partnering teams
- Analysis
  - Scope requirements, limitations
  - Discover options for collection methods
  - Identify LOE for logging data quality
  - Identify service owners and other partners
- Design
  - Prioritize deliverables for MVP (minimal viable product)
  - Requirements validation
  - Data collection solution
- Implementation
  - Data Sourcing
  - Technology Integration
- Content Engineering
- Testing & Integration
  - Stage collection setup
  - Stage data indexing, Splunk apps
- Maintenance
  - Deployment
  - Production Rollout
  - Operational Process Refinement
  - Content Delivery
    - Measureable
  - SLA Enforcement
  - Feedback Loop Enablement
  - Gap Collection

Data on-boarding R&D

BSIDES splunk>

Sample case studies for security data onboarding

	LastPass	GCP
Type	Application product	Cloud Service Platform
Description	Application for password management. Can be used to manage shared or service account credentials.	Platform to deploying cloud infrastructure to support a company's scalable compute and storage demands
Target data	• Login activities • Admin/service change management • User activity: shared credential access and permission management	• Login activities • Admin/service change management • Service and system events

Recipe for data discovery: LastPass

LastPass

What do we need?

- Target delivery:
  - Track sharing activities and credential exposure
- Validate methods of collection
- Scope for available resources to collect into Splunk
- Identify any “gotchas”
- Develop implementation plan

Recipe: data on-boarding LastPass

Let's use our framework and start with what we know

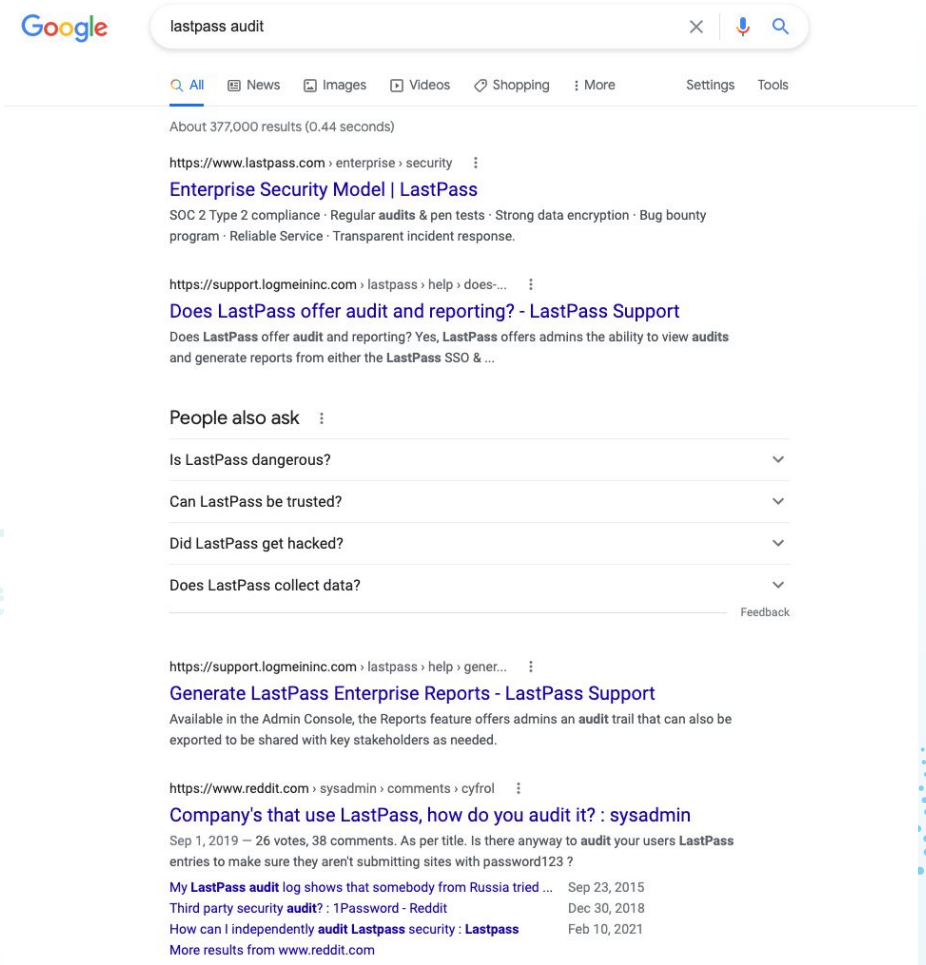
What we have

- Ingredients:
  - Requirement for capturing credential sharing user activity (did user enable sharing?)
  - Requirement for configurations to indicate potential credential exposure (is sharing enabled?)
  - Requirement for enabling user attribution

What we have need to do

- Prepare:
  - Validate methods of collection
  - Scope for available resources to collect into Splunk
  - Identify any "gotchas"
- Cook:
  - Develop implementation plan

Verify audit data availability



Verify audit data availability

LastPass

Hi! We are here to help you.

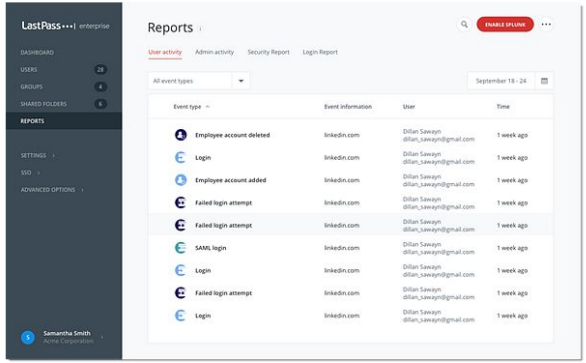
Type your question here, or browse topics below to view answers or reach a support agent.

Generate LastPass Enterprise Reports

Generate LastPass Enterprise Reports

LastPass Enterprise offers extensive reporting to help you safeguard your organization's data and build compliance. Available in the Admin Console, the Reports feature offers admins an audit trail that can also be exported to be shared with key stakeholders as needed.

Note: Are you seeing something different? See instructions for the New Admin Console.



User Activity report

While logged in to the Admin Console, select **Reports** from the left menu, where the User Activity tab provides a comprehensive log (up to 2 years of history) of every login event, passwords or username update, attempted or completed Form Fills, and deleted Sites by your LastPass Enterprise users. The logs include attempted (e.g., failed login attempts) and successful actions. The reports can be filtered by date range or user, and can be exported to Excel for

Need password support? I ca

BSIDES splunk>

Verify audit data availability

Admin Activity report

The Admin Activity report provides a detailed breakdown of all administrative actions taken via the Admin Console, including the following:

- Create, delete, disable, or reactivate an employee account
- Reset a user's Master Password
- Add admin permissions to a user
- Remove a user from the company
- Add, delete, or edit policies
- Add, edit or delete User Groups
- Update policy users

A complete list of all actions and their designations can be found here. Please note that you must be actively logged in with a LastPass Enterprise or LastPass Identity account in order to view the full list of actions available.

Security report

Select **Reports** from the left menu, then click **Security report** for a summary of various critical user statuses, around which additional education or training may be warranted (e.g., Reused Master Passwords, Weak Security Challenge Scores, More than three duplicate passwords, etc.). The goal of this view-only report is to help optimize the use of LastPass among your end users to help improve the security of your company's digital assets.

Additionally, you can set up to receive email notifications for these security statuses by navigating to **Settings** > **Email Notifications** > **Add Notification** > **Configure**.

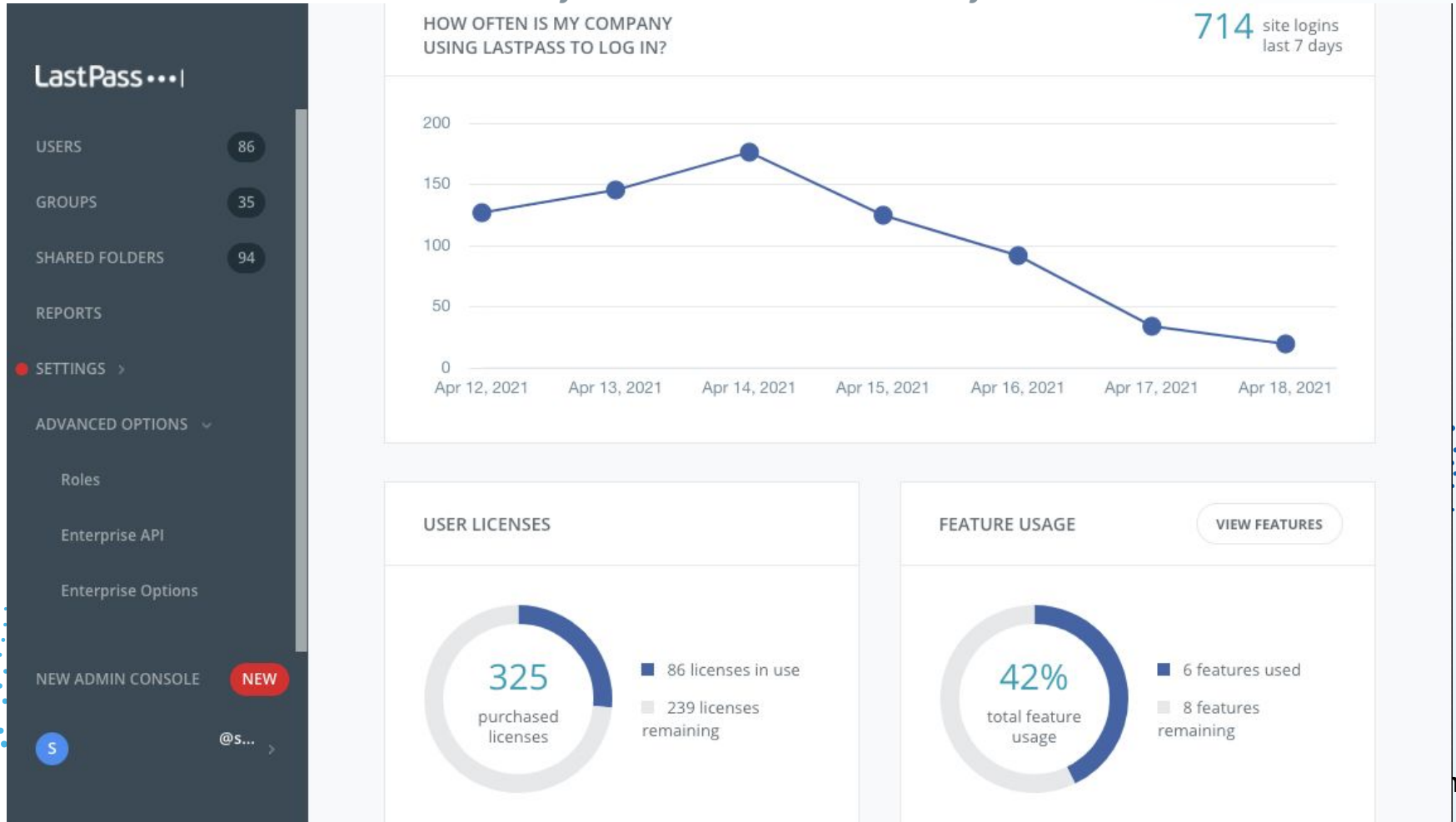
Splunk Integration report

Take advantage of your existing Splunk account with the LastPass integration. With the Splunk integration in LastPass Enterprise it's even easier for your IT team to collect data and manage reports in one central location — your Splunk Cloud account. To take advantage of this integration, you need a running Splunk Cloud instance with a configured Data Input as HTTP Event Collector.

You can set up the integration between LastPass and Splunk by configuring your Advanced Enterprise Options. Once your Splunk settings are configured, all available reporting events (e.g., login events, password changes, Form Fill attempts, etc.) will be passed to the Splunk Cloud, where you can then create custom User Activity reports using that data. This allows you to use the advanced functionality of Splunk to access and report on your LastPass Enterprise activity.

BSIDES splunk>

Verify audit data availability



Verify audit data availability

LastPass •••|

USERS 86
GROUPS 35
SHARED FOLDERS 94
REPORTS
SETTINGS
ADVANCED OPTIONS
Roles
Enterprise API
Enterprise Options
NEW ADMIN CONSOLE NEW
S @s...

JSON - Reinvite User (cmd = reinviteuser)

Reinvite individual users.

Example Request:

⊕ Request Sample

⊕ Response Sample

JSON - Disable Multifactor (cmd = disablemultifactor)

Use the disablemultifactor command to disable a user's multifactor authentication.

Example Request:

⊕ Request Sample

⊕ Response Sample

JSON - Event Reporting (cmd = reporting)

Use the reporting command to gather information on events that have taken place within your Enterpr
000 users at a time. Use the 'next' parameter to paginate over a larger dataset. Events are sorted by tir
times should be represented in this time zone: US/Pacific.

from
Pull reporting data starting from this date.

to
Pull reporting data until this date.

search
A search string to filter the reporting data.

nk>

Verify audit data availability

LastPass

- USERS 86
- GROUPS 35
- SHARED FOLDERS 94
- REPORTS
- SETTINGS
- ADVANCED OPTIONS
  - Roles
  - Enterprise API
  - Enterprise Options
- NEW ADMIN CONSOLE NEW

S @s...

⊕ Request Sample

⊕ Response Sample

JSON - Get User Data (cmd = getuserdata)

The getuserdata command returns information about users in the enterprise. The optional data element is used to filter or limit the returned data set. Tip: To prevent details from being omitted from the response, avoid retrieving more than 2000 users at a time.

pagesize
Limits the maximum number of items listed per page.

pageindex
The page number. Default: 0.

username
<username> - Return only the specified user.

disabled
0 - Return only active accounts.
1 - Return only disabled accounts.

admin
0 - Return only non-admin accounts.
1 - Return only admin accounts.

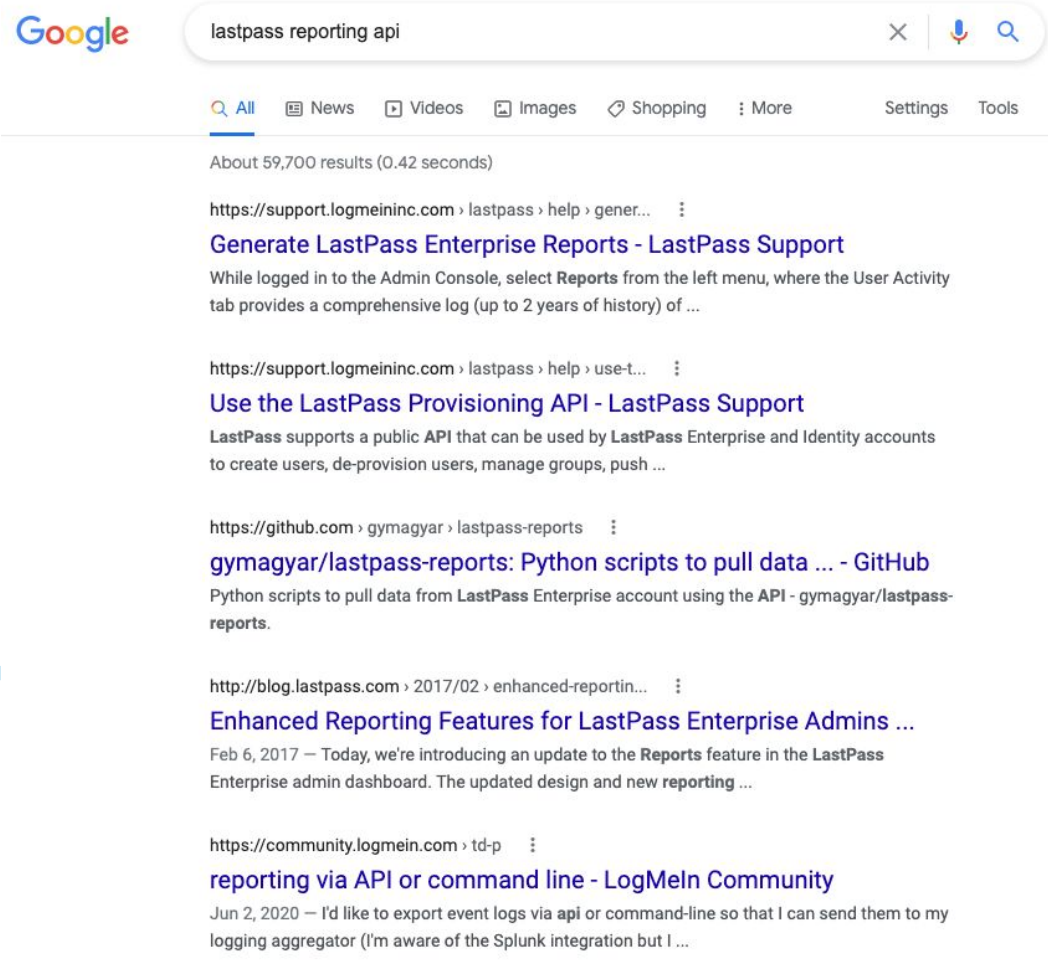
Example Request:

⊕ Request Sample

⊕ Response Sample

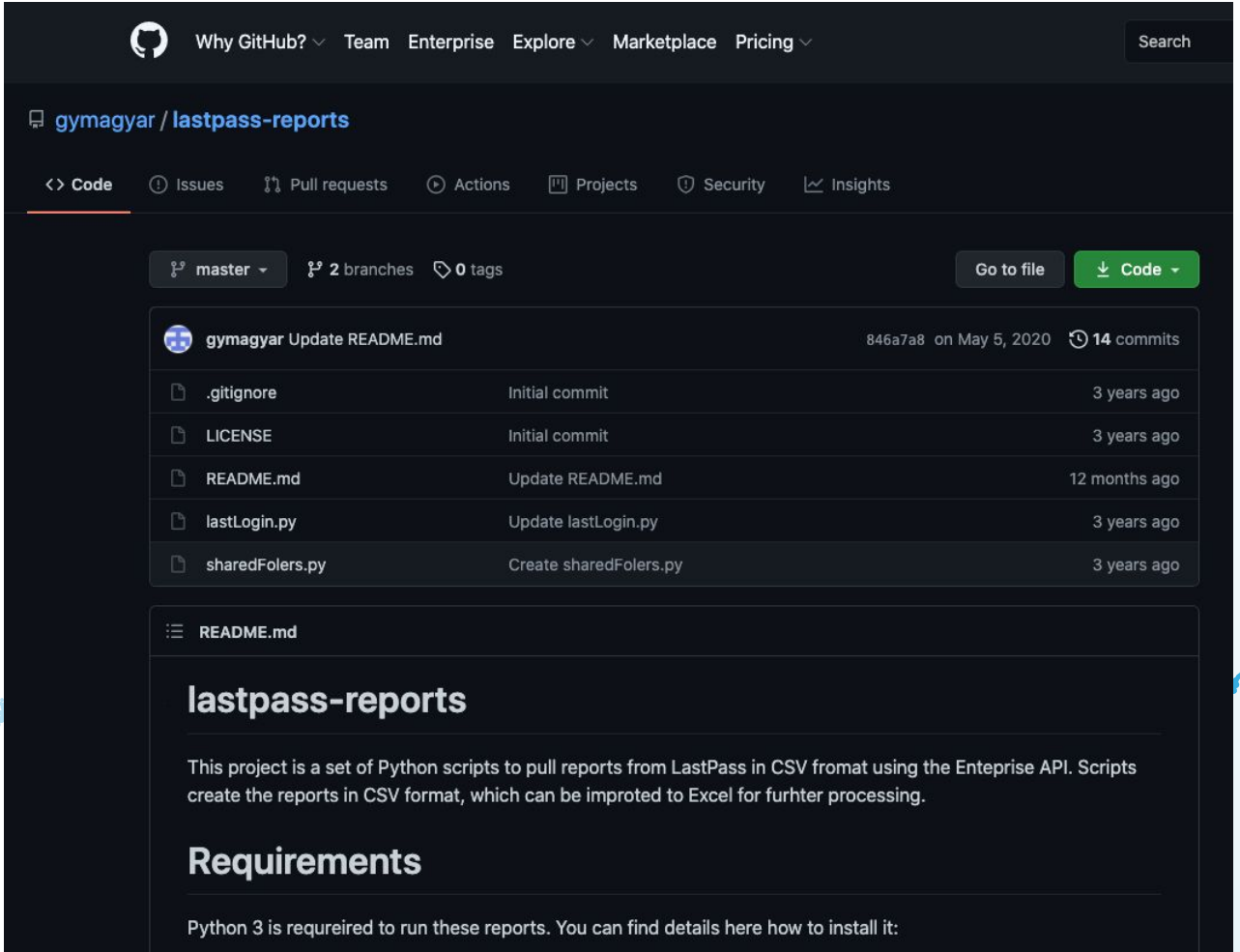
JSON - Delete User (cmd = deluser)

Collection methods

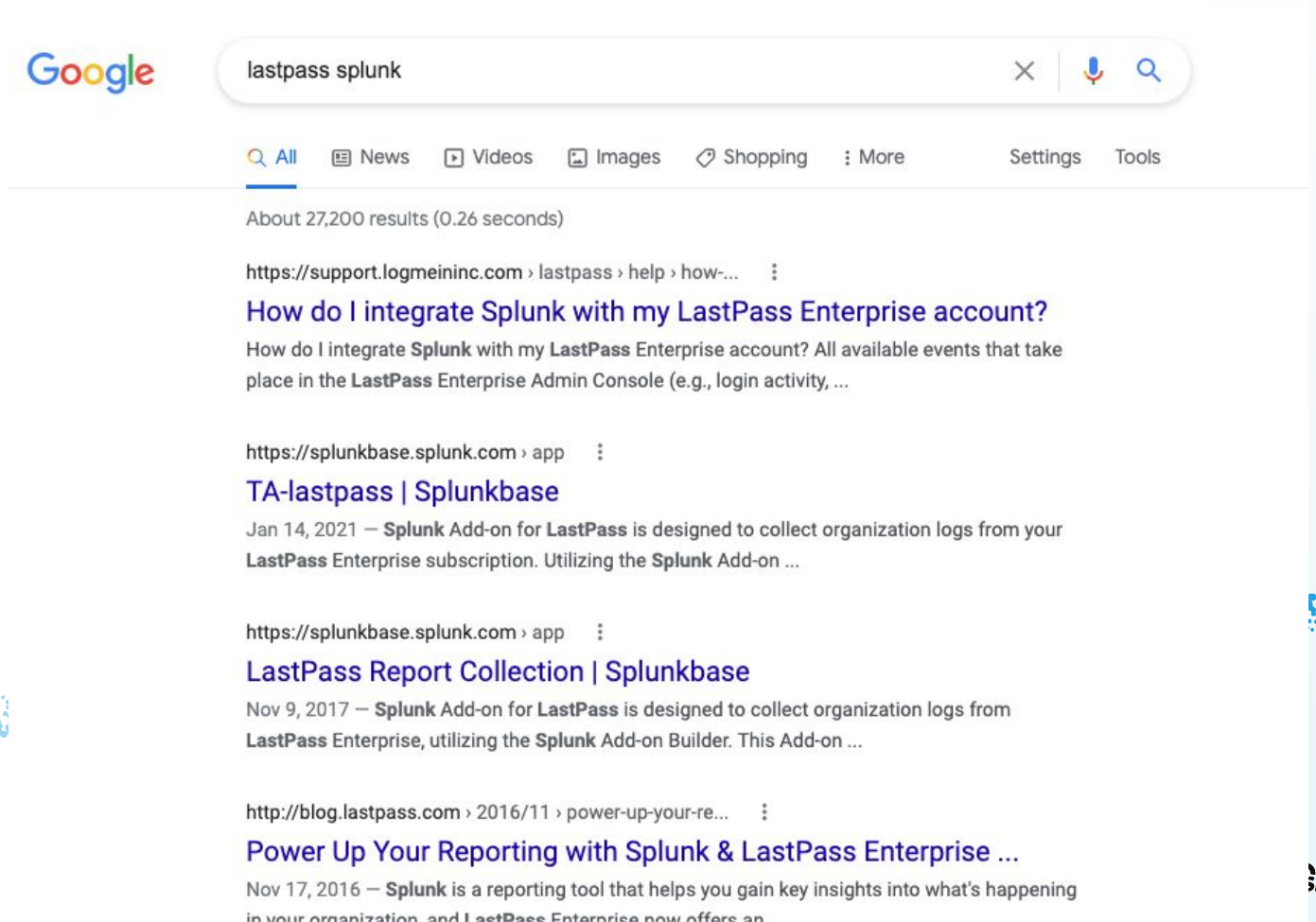


BSIDES splunk>

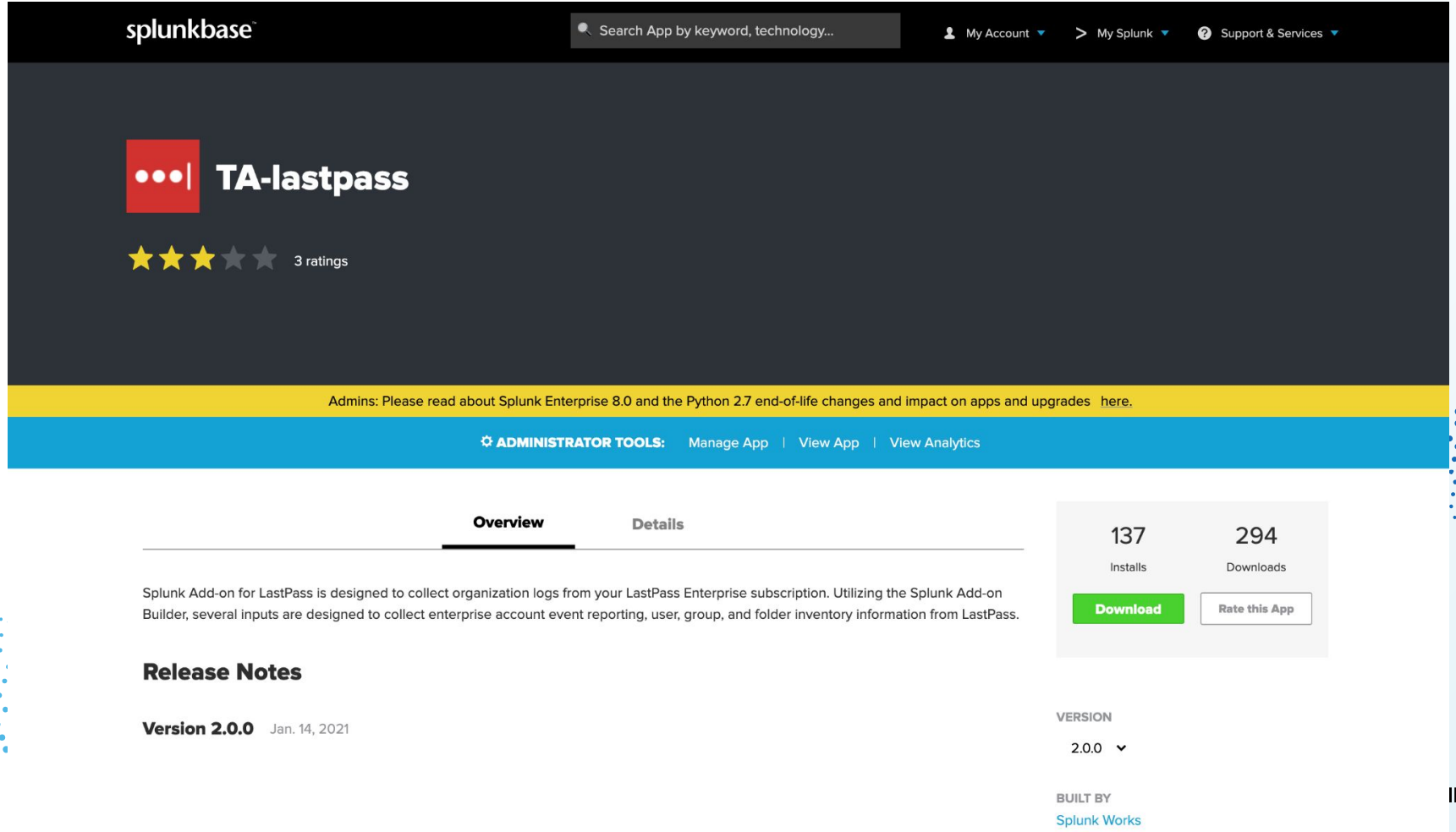
Collection methods



Verify existing integrations



Collection methods



LastPass

What did we end up with?

- Target delivery:
  - Activity and configs to track sharing activities and credential exposure
    - Vendor has an “Event Reporting” API endpoint
  - Determine user attribution
    - Configurable user reference exposure for audit log
- Validate methods of collection
  - Supports SplunkCloud HEC delivery
  - Enterprise API
- Scope for available resources to collect into Splunk
  - Github
  - Splunkbase
- Identify any “gotchas”
  - Requires enterprise subscription + admin role to review, configure settings
  - Need to customize audit logs for enhanced information
- Develop implementation plan
  - Work with service owner to configure access, data quality of audit logging
  - Leverage API
  - Validate TAs

Recipe for data discovery: GCP

GCP

What are our objectives?

- Target delivery:
  - Collect as much data possible for IaaS access and service administration
- Validate methods of collection
- Scope for available resources to collect into Splunk
- Identify any “gotchas”
- Develop implementation plan

Recipe: data on-boarding GCP

Let's use our framework and start with what we know

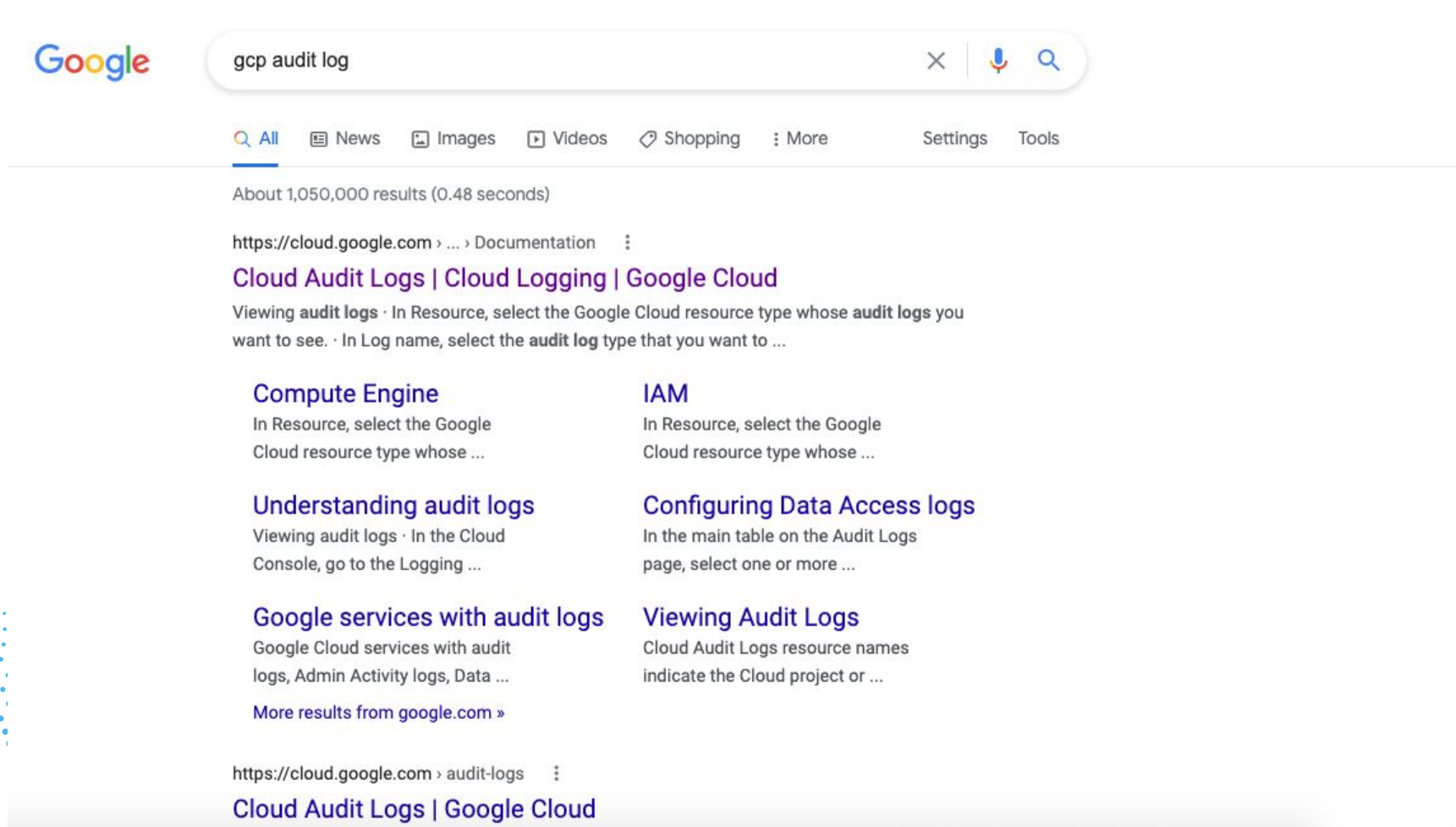
What we have

- Ingredients:
  - Requirements for access events
  - Requirements for service administration events
  - Requirements for provisioning events

What we have need to do

- Prepare:
  - Validate methods of collection
  - Scope for available resources to collect into Splunk
  - Identify any "gotchas"
- Cook:
  - Develop implementation plan

Verify audit data availability



Verify audit data availability

Google Cloud | Why Google | Solutions | Products | Pricing | Getting Started | Docs | Support | English | Console

Operations Suite | Overview | Guides | Reference | Samples | Support | Resources | Contact Us

- All concepts
- Basic concepts
- Access control
- Available logs
- Platform logs
- Data regionality
- Structured logging

Security logging

- Access Transparency logs
- Cloud Audit logs
  - Overview
  - Configuring Data Access audit logs
  - Understanding audit logs
  - Services with audit logs
  - Best practices
- Google Workspace audit logs
- Audit logs datatypes

Solutions

- Storing your organization's logs in a log bucket
- Multi-tenant logging on GKE

Operations Suite > Logging > Documentation > Guides

Rate and review

Cloud Audit Logs

Send feedback

Table of contents

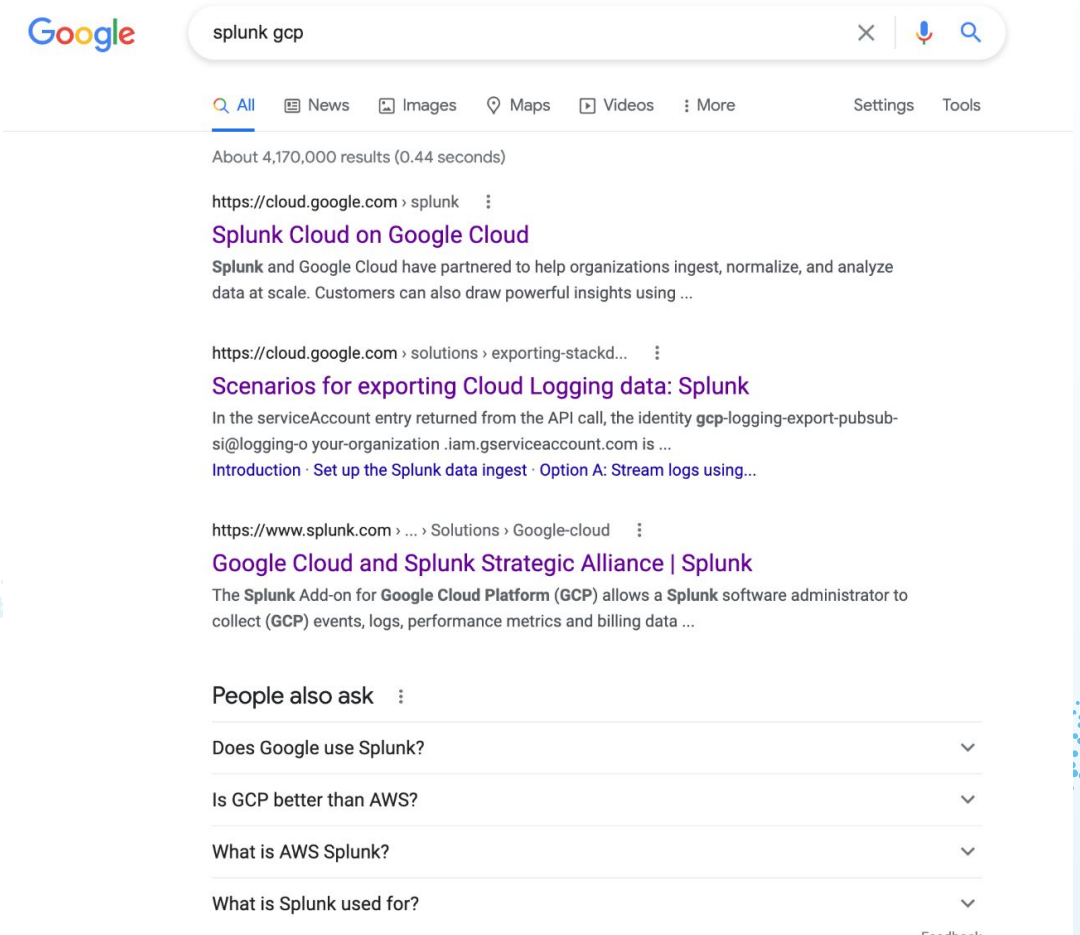
Cloud Audit Logs provides the following audit logs for each Cloud project, folder, an

- Admin Activity audit logs
- Data Access audit logs
- System Event audit logs
- Policy Denied audit logs

Google Cloud services write audit log entries to these logs to help you answer the questions of "who did what, where, and when?" within your Google Cloud resources.

nk>

Verify existing integrations



Collection methods

Cloud Architecture Center
« Return to Cloud Architecture Center

Scenarios for exporting Cloud Logging data: Splunk

Send feedback

This scenario shows you how to export selected logs from Cloud Logging into Splunk Enterprise or Splunk Cloud in real time. Splunk enables you to search, analyze, and visualize logs, events, and metrics gathered from your on-premises and cloud deployments for IT and security monitoring. By integrating logs from Cloud Logging, you can continue to use existing partner services like Splunk as unified log analytics solution — with options to deploy Splunk on-premises, in Google Cloud as SaaS, or through a hybrid approach.

This document gives you an overview of two different supported methods for log export to Splunk: either by pushing or pulling logs from Google Cloud. As explained in the following section, the cloud-native push-based approach is recommended in most cases. For more in-depth information on how to deploy the push-based log export solution, see Deploying production-ready log exports to Splunk using Dataflow.

This scenario is part of the series Design patterns for exporting Cloud Logging.

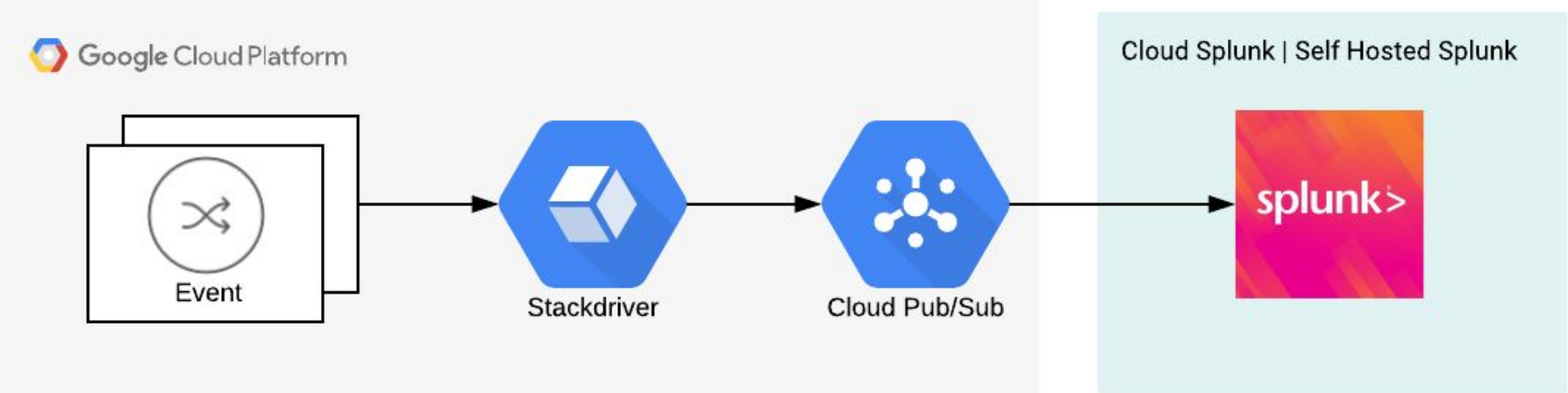
Introduction

There are two methods for ingesting Google Cloud data supported by Splunk:

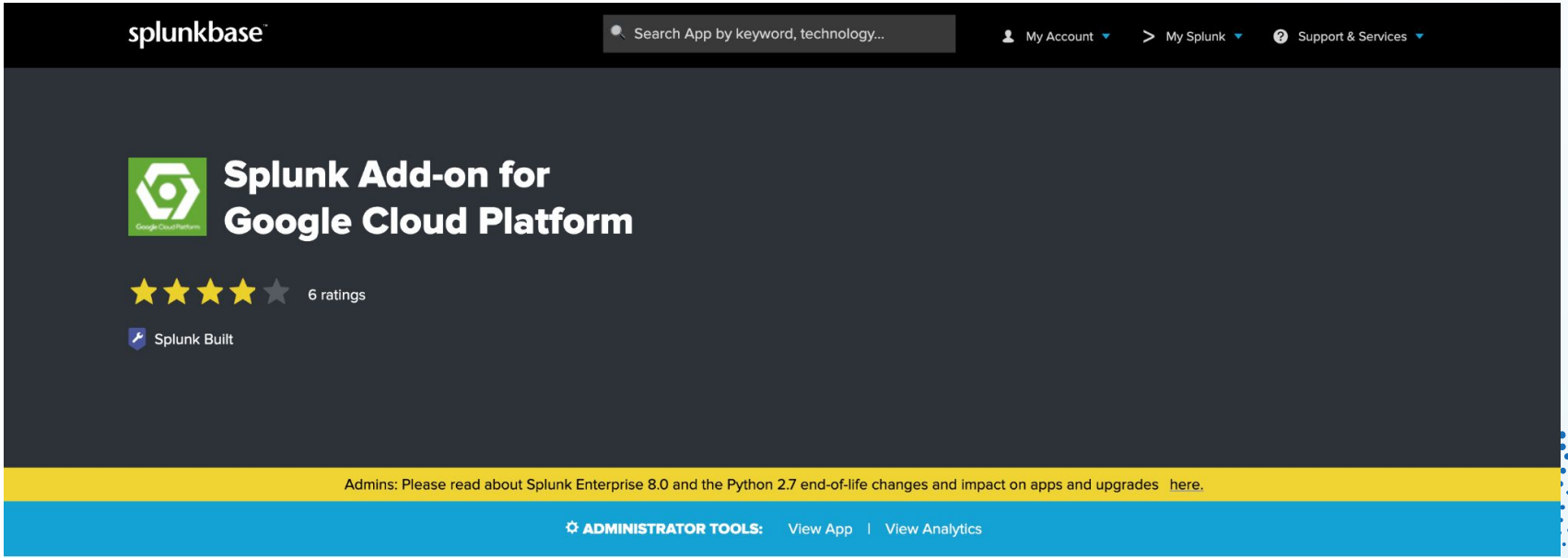
- **Push-based method**: data is sent to Splunk HTTP Event Collector (HEC) through a Pub/Sub to Splunk Dataflow job.
- **Pull-based method**: data is fetched from Google Cloud APIs through the Splunk Add-on for Google Cloud Platform.

We recommend that you use the push-based method to ingest Google Cloud data in Splunk. This method has the following advantages:

Collection methods



Collection methods



GCP

What did we end up with?

- Target delivery:
  - Collect as much data possible for IaaS access and service administration
    - Vendor has a number of audit logs available for collection
- Validate methods of collection
  - Recommended solution: Google pub/sub
  - Multiple methods are supported
    - Push: Splunk HEC (webhook)
    - Pull: Splunk TA (API)
- Scope for available resources to collect into Splunk
  - Both Splunk and Google have (jointly) published content and solutions
  - GCP: pub/sub
  - Splunk: TA
- Identify any “gotchas”
  - Pub/sub model is dynamic but will require budget, operational cost
- Develop implementation plan
  - Work with service owner to configure access, data quality of audit logging
  - Leverage API
  - Validate TAs

Summary time

What were we able to accomplish?

- Given security use case and desired data quality, how to target information from the technology
- Prioritize data artifacts (data quality) for MVP
- Leverage pre-existing happy paths for collection processes
- Discover and validate collection methods
- Review resources
  - From product
  - From 3rd party source
- Identify any gotchas up front for implementation
- Establish a checklist to measure success

Thanks!

Any questions?

You can find me at

- @henry
  - in Splunk User Community Slack
- hcbomb@yahoo.com
- #BSides21

Appendix

References

- https://attack.mitre.org/
- https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- https://medium.com/cycraft/cycraft-classroom-mitre-att-ck-vs-cyber-kill-chain-vs-diamond-model-1cc8fa49a20f
- https://owasp.org/www-project-cyber-defense-matrix/
- https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html
- https://owasp.org/www-project-top-ten/2017/A10_2017-Insufficient_Logging%2526Monitoring
- https://owasp.org/www-project-application-security-verification-standard/
- https://github.com/OWASP/ASVS/raw/v4.0.2/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0.2-en.pdf
- https://cloud.google.com/solutions/exporting-stackdriver-logging-for-splunk
- GCP TA: https://splunkbase.splunk.com/app/3088/
- LastPass TA: https://splunkbase.splunk.com/app/2633/
- https://github.com/gymagyar/lastpass-reports
- https://github.com/splunk/TA-lastpass
- https://chiefmartec.com/2014/02/1000-marketing-technology-vendors-new-normal/
- https://venturebeat.com/2020/10/21/the-2020-data-and-ai-landscape/
- https://www.splunk.com/pdfs/technical-briefs/using-splunk-adaptive-response.pdf
- https://digital-forensics.sans.org/media/Targeted-SOC-Use-Cases-for-effective-Incident-Detection-and-Response-Angelo-Perniola-David-Gray.pdf
- https://lastpass.com/logmsgdoc.php
- https://splunkbase.splunk.com/app/3435/
- https://docs.splunksecurityessentials.com/

Security data onboarding checklist

- Planning
  - Verify motivation
  - Validate and quantify visibility gaps
  - Resource allocation
  - Timing and alignment of partnering teams
- Analysis
  - Scope requirements, limitations
  - Discover options for collection methods
  - Identify LOE for logging data quality
  - Identify service owners and other partners
- Design
  - Prioritize deliverables for MVP (minimal viable product)
  - Requirements validation
  - Data collection solution
- Implementation
  - Data Sourcing
  - Technology Integration
- Content Engineering
- Testing & Integration
  - Stage collection setup
  - Stage data indexing, Splunk apps
- Maintenance
  - Deployment
  - Production Rollout
  - Operational Process Refinement
  - Content Delivery
    - Measureable
  - SLA Enforcement
  - Feedback Loop Enablement
  - Gap Collection