Zero – Hero: A 202-Year-Old Firm's Journey to End-End Security Visibility

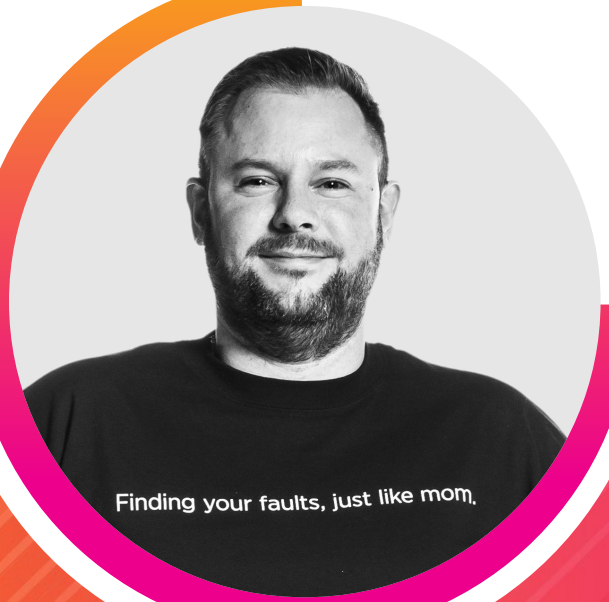
Craig Gilliver
Head of SecOps | Johnson Matthey

splunk> .conf19

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.



Craig Gilliver
Head Of SecOps, Johnson Matthey

Edward Asiedu
Senior Professional Services Consultant, Splunk

splunk> .conf19

Johnson Matthey

splunk> .conf19

"Our **vision** is for a **world** that's **cleaner and healthier**; today and for future generations."

"To **execute** our vision, we have to **protect** our **intellectual property** from physical and **cyber threats**."

SOC Overview

1. Cyber Threats and the JM Landscape
2. What is the Security Operations Centre (SOC) and how does it protect JM?
3. Work completed so far and our phased approach
4. Data Analytics
5. Building it for the future
   - What's next: Phantom & UBA

Cyber Threats and the JM Landscape

and how we align our executives on Cyber and justify what we do in our SOC

Situation	Target	Proposal
Cybercrime is a growing threat to businesses. JM is a prime target for cybercriminals and other threat actors, whose approaches are becoming more sophisticated. **Phishing attacks (malicious emails) which act as the starting point for most attacks are more common than ever.**	**Johnson Matthey becomes a cyber-resilient organization.** JM effectively manages our cyber risk, while enabling and supporting the business strategy while meeting the demands of our customers.	When it comes to protecting JM information and knowledge, we're only as good as our weakest link. **So it's important that we respond with a targeted uplift in our security technologies, business processes and ways of working.**

The likelihood of loss or theft of JM information is growing with an escalation of increasingly sophisticated threats, as well as increasing use of personal **mobile devices and other internet connected devices (IoT).**

The Landscape

Cyber Threats and the JM landscape

Threat Actors:

Organized Crime	Professional criminal gangs seeking financial gain
Nation States	Nation states undertaking cyber-(espionage or warfare) capabilities.
Terrorists	Use of cyber techniques to conduct or promote terrorism.
Activist Groups	Activists using cyber techniques to further a political cause or protest.
Recreational Hackers	Individuals using cyber techniques for fun or intellectual challenge.
Insiders	Can be malicious or unintentional/accidental.
Corporate Rival	Competitor seeking to gain commercial advantage.
Collateral Damage	Untargeted attack that unintentionally impacts the company.

- 11% Increase in security breaches since last year (Accenture)
- Public organisations receive 1 malicious email per 302 emails (Symantec)
- Worldwide cybercrime costs an estimated $600 billion USD a year (McAfee/Centre for Strategic and International Studies)

JM are a target for all Threat Actor groups, however the motivation and determination of some will be greater than others

Cyber Threats and the JM Landscape

4.1m
Gross Inbound Email

990,000
Inbound Blocked Emails

17,500
Inbound Blocked Malware

8,250
Blocked Phishing emails

27+
Identity Systems

8+
Anti-Virus solutions

14,800
Attempts to access Blocked Content

22,500
Attempts to access known compromised websites

202 Year Old
From a single office in London in 1817

30 +
Countries JM operates in

15 k
Global Employees

60 Sites +
Global Offices

72 Sites +
Global Manufacturing Which 42 being 24/7

FTSE 100
$ 20 billion 2018 turnover

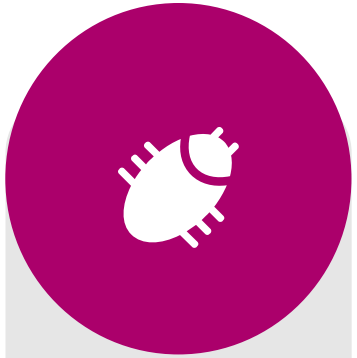
What is the Security Operations Centre (SOC) and How Does it Protect JM?

Log sources from multiple platforms are Ingested into the SIEM (Splunk) and correlates events

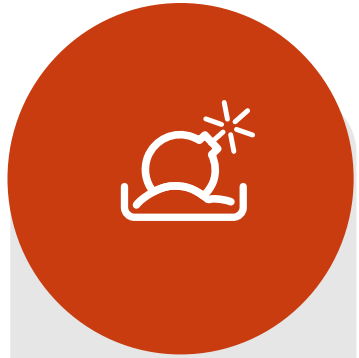
JM platforms are scanned for known technical weaknesses.

External Threat Intelligence data provides additional intel

Data analysis undertaken to look for activity which could be indicative of an incident or potential compromise



Potential incidents are identified, analysed, defended, investigated and reported



Tools are then improved to proactively prevent future attacks – e.g. email security, web filtering, AV

What is the Security Operations Centre (SOC) and How Does it Protect JM?

All data is ingested, correlated and combined to give a single pane of glass view of activity on the JM estate significantly increasing the SOC team's visibility and understanding which in turn matures/develops our cyber defences.

SOC Development Completed in Phase 1

1. March 2019
   - Core Platform built
   - Log feeds setup
2. April 2019
   - Commenced configuration of initial 35 + use cases
3. May 2019
   - Use case configuration tuning completed
4. June/July 2019
   - Dashboard building and testing

Assembling a Team For Success

Splunk Inc

Enterprise Account Manager (Al Kelly)

- Not just selling – ensures access to resources needed for success

Staff Solution Architect (Richard Mason)

- Ensures we do not create a unicorn – we want a robust architecture rather the best for cheapest which then runs on limits

Pre-sales Engineers (Johan Bjerke, Marc Thomas, Endre Peterfi)

- Engaged to aid discovery of what other customers are doing successfully

Delivery Manager (Gemma Jardim)

- Facilitated smooth delivery by managing and monitoring work being delivered, risks and issues

Professional Services (Edward Asiedu, Georgios Glymidakis)

- Advising and applying best practices and experience for best implementation outcomes

Assembling a Team For Success

Chief Information Officer (Paul Coby)

- Facilitating management buy-in, his team needs to provide the right data from the right systems

Chief Information Security Officer (Simon Strickland)

- Advises on:
  - what is most important
  - what is the biggest risk
  - what needs prevention
  - what just needs detection
- What are the escalation routes
- What are our policies and risk appetite

Assembling a Team For Success

Head of SecOps (Craig Gilliver)

- Technical and Executive Architect driving success of the deployment
- Responsible for building of the team
- Facilitating cooperation from security vendors

Project Manager (Aidan Loughran)

- Maintains project cadence and liaises for intra-company resources and with Splunk PM

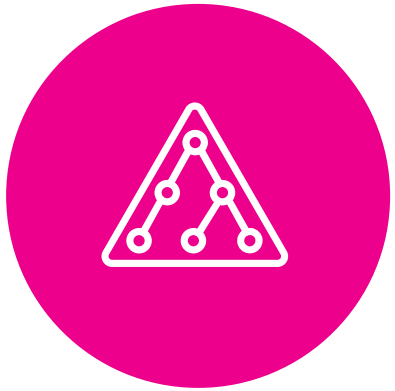
SOC Analysts (Rory Duncan, Roy Jenkins)

- SMEs on security infrastructure/apps and project technical contact to security vendors

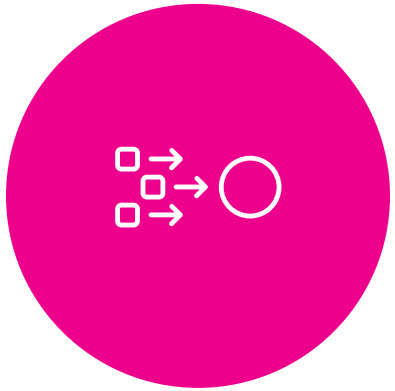
SOC Development in Phase 1

What did we do and why?

Prepared in Advance



Populated Internal Identities & Assets

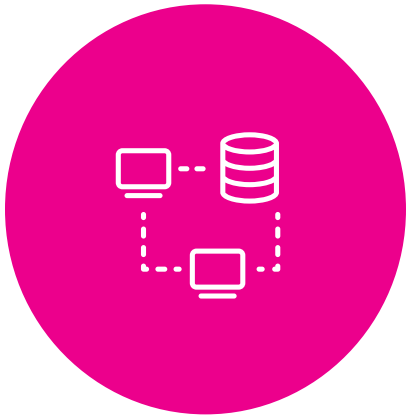


Pursued Data Success Strategy

Applied Strategy to Get Data In

Built Up the Data into Use Cases

ROI Increases with Advance Preparation



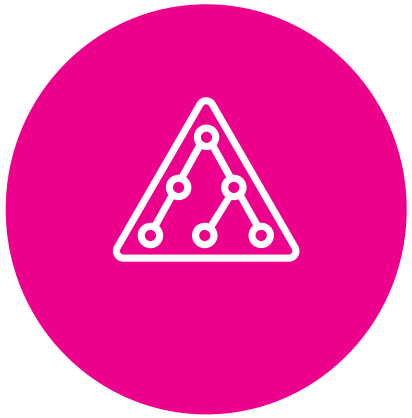
Completed these planning activities:

- Deep-dive solution architecture design
- Use case workshops
- Dashboard/Report content needs and data dependencies
- Built outputs into an agreed design

Completed these pre-implementation activities

- Prepared hardware
- Tested log data generation capability
- Ensured data could be accessed via networks and filesystems
- Obtained data samples

Populating Internal Identities and Assets



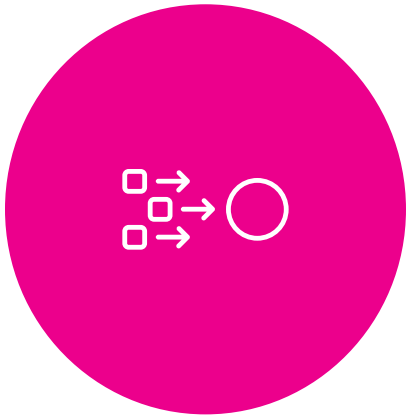
Assets and Identities onboarded as early as possible

Collected data about people, utility accounts, machines and devices wherever they resided

Identified normal locations of work for users (long/lat)

Identified any non-private IP addresses (RFC 1918) used on internal networks

Pursuing a Strategy for Data Success



Compliance with the Common Information Model

Consistency of source fields by host

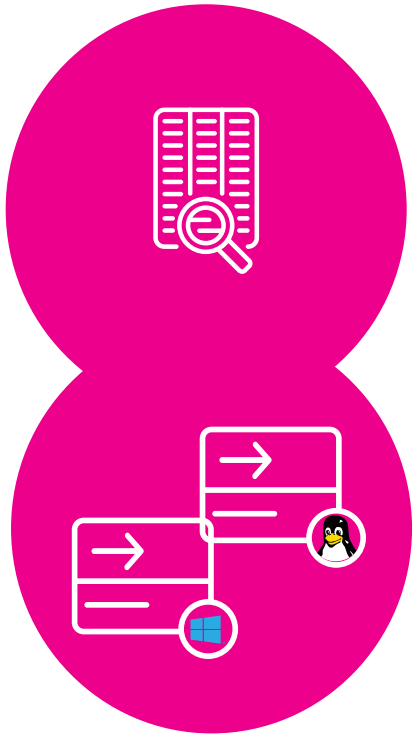
Leveraged technical add-ons (TAs) where possible

Monitored for delays and extended delays

Prioritised sources with high use case yield to accelerate

Separated data to indexes by audience and retention period

March GDI Strategy: Windows and Linux OS



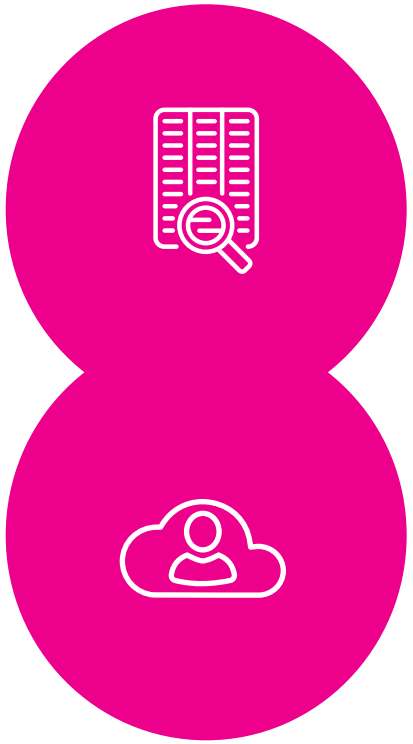
Universal forwarders deployed to thousands of endpoints via SCCM or script

Splunk Deployment Server (DS) managed forwarders for consistent configuration

DS rolled out Splunk TAs for acquisition of security and process event data.

OS logs gave visibility into endpoint processes, user, change and authentication activity.

March GDI Strategy: Cloud Directory Service Data



Used Splunk TA on a Heavy Forwarder to collect user and admin audit logs from the Office 365 API/Azure AD

Quickly gave us CIM-compliant data

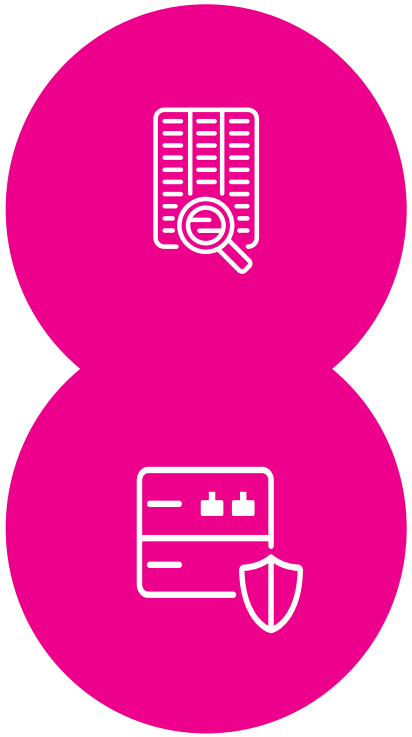
Gave us visibility of cloud-based app authentications

Any challenges?

- Overcame data delay by fixing network bottleneck

In combination with Windows and Linux OS security data, supported authentication and suspicious change use cases

March GDI Strategy: Proxy Data



Logs only accessible via obscure script interacting with a gateway to select names of available log files and write them to a list for download

Duplicate avoidance needed on each run of script

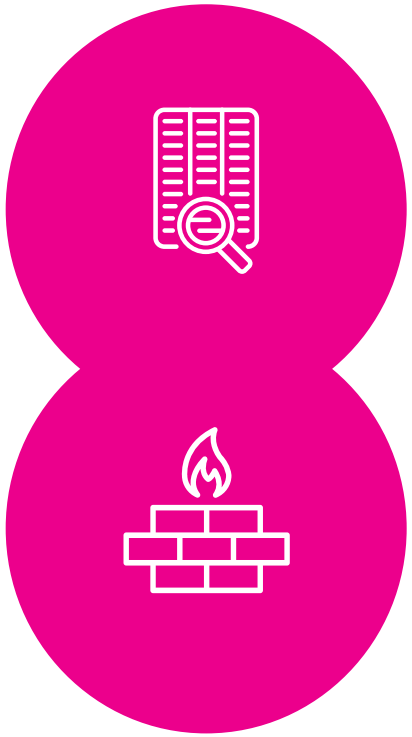
Files streamed to Splunk Cloud via UF on syslog

Any challenges?

- Logs did not match any Splunk Base TA, required new TA build
- Interesting log features like representing the IP address 85.115.32.5 as 1433608197

Provided visibility for C2 use cases and risky site visits

March GDI Strategy: Firewall Data



Received syslog data from MSP over encrypted link

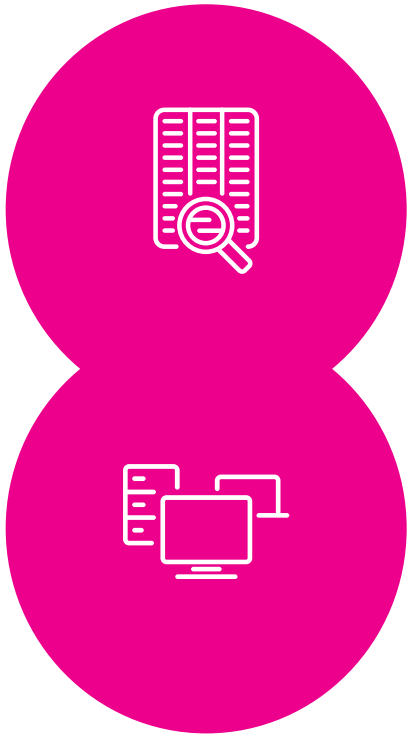
Any challenges?

- Needed clarification for multiple timestamps per event
- Worked with MSP to output logs written closer to format expected by vendor's TAs

Closer alignment to TA allowed faster time to value and update compatibility

Firewall data provided insights into network such as activity by host, protocol and ports and used

March GDI Strategy: Endpoint Data



Service with endpoint agents sending data to cloud

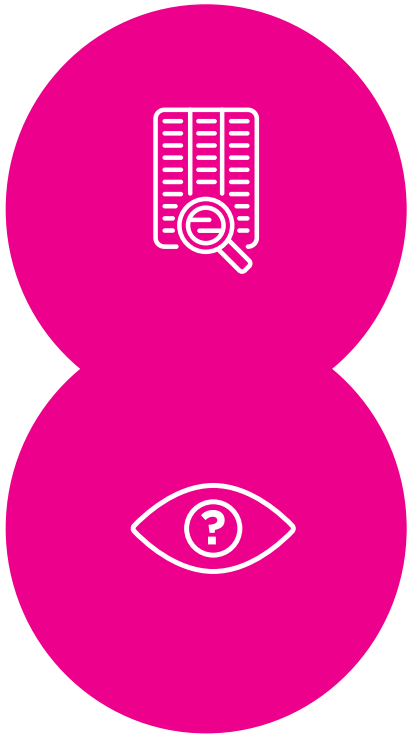
Received data via an AWS syslog server

Any challenges?

- Swapping certificates for secure receipt of syslog data
- Worked with vendor to provide data in format close to one of their published Splunkbase TAs
- TA expected JSON data, but data received was JSON prefixed with syslog headers – tweaked TA to clean

Data supported detection of suspicious command line and process activity

March GDI Strategy: Threat & Vulnerability Intel



Selected Recorded Future (RF) intelligence feed subscription over OOB intelligence feeds

RF apps integrated tightly between Splunk ES and RF online portal

Selected vulnerability scanning/intel vendor which provided both TA's and dashboard apps for Splunk

Vulnerability scans provided additional inventory of assets

April: Building Data into Use Cases

- Stated the use case as simply as possible
- Created a suitable ordinary search of indexes
- Checked for expected results
- Verified the fields in ordinary search were present in the CIM and extended datamodels as needed
- Accelerated ordinary searches by converting to tstats correlation search of datamodels
- Previewed sample security incidents with SOC and tuned by amending query instead of suppressions
- Finalised correlation search options, including custom fields and throttling

April: Highlights of 35 + Use Cases

Malware outbreaks/reoccurring malware infections
Attacks on user accounts
Attempts to force logins into servers/computers
Activity from leavers
Deletion of audit logs
Communication to known bad external networks
Discovery of known bad executables
Malicious processes
Single letter process
Powershell execution policy bypass
etc.

May: Use Case Tuning

Testing and evidence collection completed

All data ingestion correlated against the use-cases that have been setup

Dashboard design and configuration commenced

Custom searches and alerts

Splunk Cloud Gateway enabled for index monitoring

June/July: Dashboard Building and Testing

Dashboards completed and ready

Testing finalized

SOC analysts training

Service transition activities concluded

Go live

Scoping to commence Phase 2

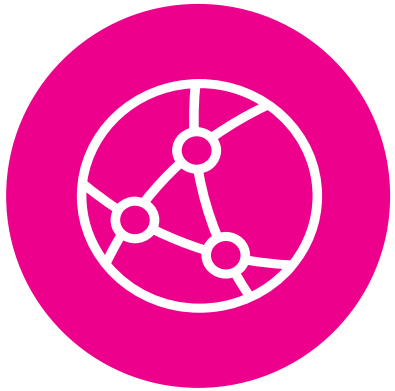
Phase 2

Data sources identified

- Critical Tier 1 Apps (PaaS & SaaS)
- Network Layer (OSI layer 2 & 3)
- Linux Servers (log collecting capability)
- On-premise Cisco ASA/Wireless LAN Controller data
- Internal DNS data
- On-premise SharePoint platforms
- PAM (Privileged Access Management)
- Phantom and UBA BC creation

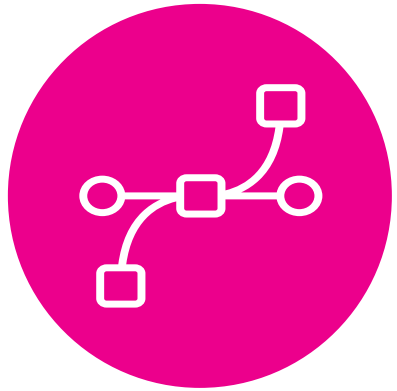
Milestones for Phase 2

Extended Syslog Deployment

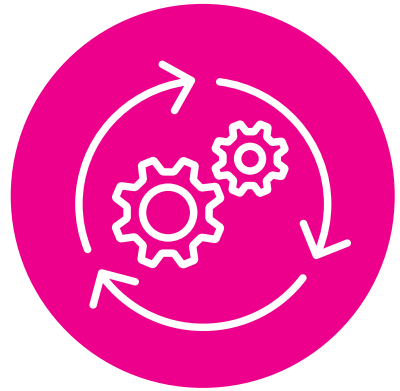


VPN, DNS and DHCP Session Tracking

REST API Source Expansion

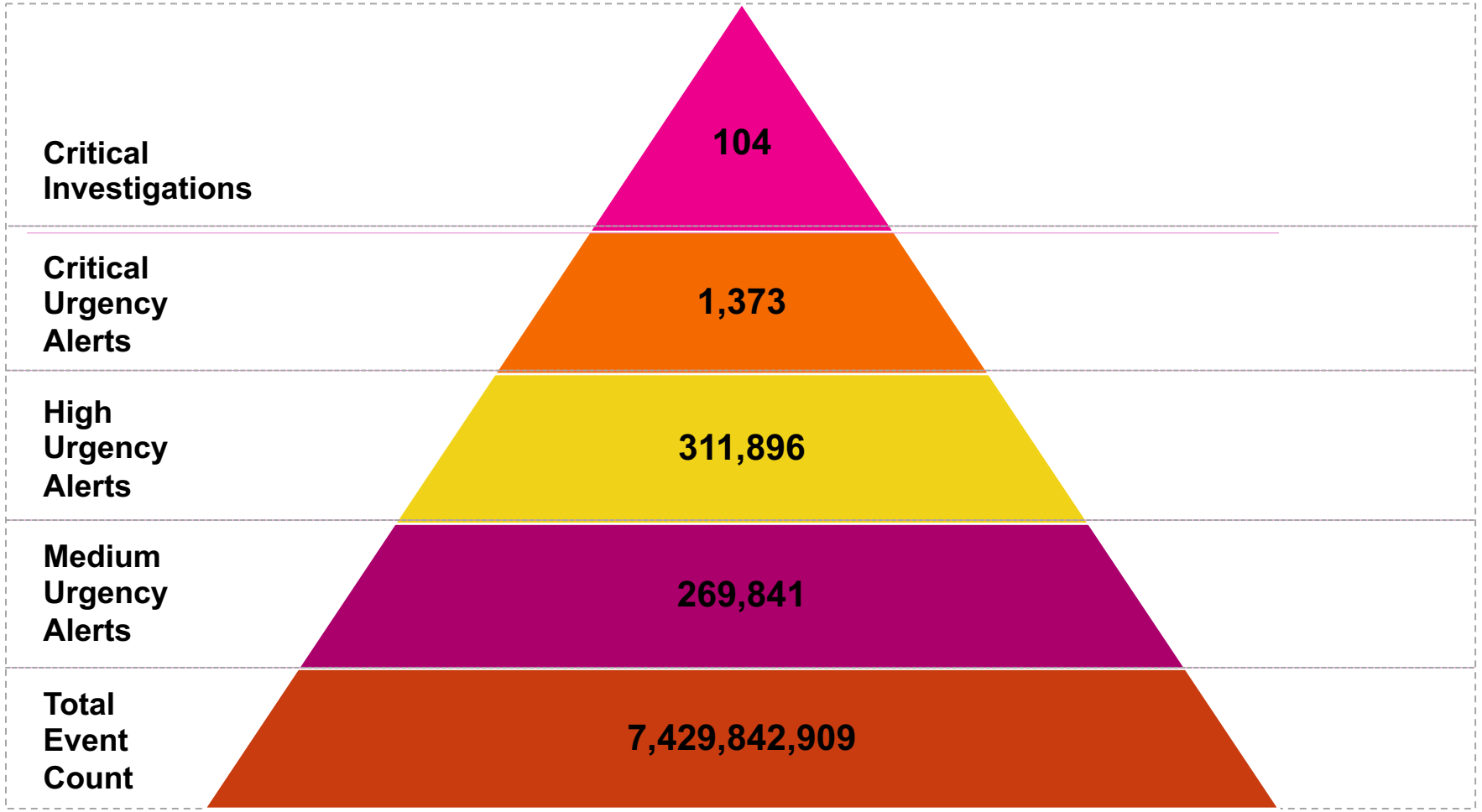


Network Infrastructure Flow Collection



Orchestration Automation (SOAR) Planning

Data Analytics – June Splunk Data



Key Takeaways

Building a global award winning soc

1. SIEM implementation is a journey – not a product that you implement
2. There is no magic button where it works by just installing
3. For cloud or managed security products, vendor cooperation on logs is essential
4. Key to success was planning, one-vision collaboration and adaptability of Splunk software to varying data constraints

"Guys, we caught him **red-handed**.
Well done!
He was **installing Ubuntu on his machine.** He became **very worried…**"

Craig Gilliver, April 30th, 2019

.conf19

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION