Veeva

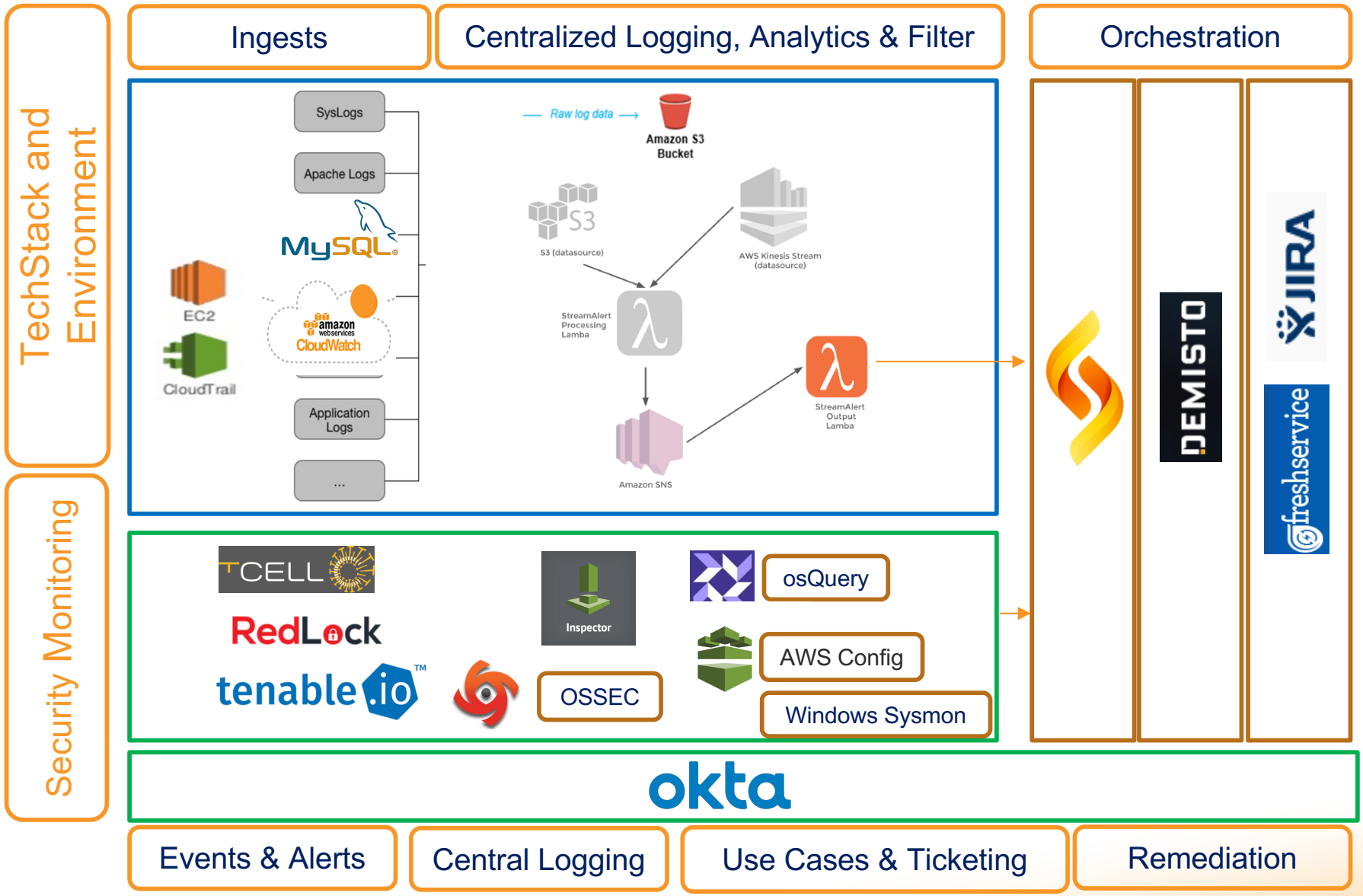
Security Orchestration (& Monitoring)

ISC2 11 May 2017

Security Orchestration (& Monitoring)

- **Need to design monitoring and orchestration at once**
  - Prevent stale data sitting in logging solution
- **Low headcount**
  - Rely heavily on automation
- **Requirements:**
  - Scalable
  - Automated
  - Support AWS

Security Monitoring & Orchestration



Orchestration & Monitoring

- **Ingest from multiple sources**
  - AWS security tool, WAF, vulnerability scanner, etc.
- **Trigger alerts**
  - StreamAlert serverless SIEM
- **Initiate orchestration**
  - Enrich data
  - Allow incident handler to automate common responses

Orchestration Use Cases

#	Use Case	Logs analyzed / correlated	Priority
1	Unauthorized user account / Privilege Escalation	Okta	
2	Malicious behavior of compromised account	FTPS, Okta, Cb Defense	
3	Connection attempt from compromised host (Unauthorized IP)	Redlock, tCell	
4	Compromised customer account leads to DDoS attack	Rendition server logs, Check MK	
5	Performance Degradation in short duration	Rendition server logs, Check MK	
6	Variations on compromised endpoint	Cb Defense, Cisco Umbrella	
7	Redlock Alerts on AWS infra	Redlock, AWS Cloudwatch	
8	CSS Alerts from tCell	tCell	
9	Gitlab code monitoring	Gitlab / Truffle Hog	
10	Monitoring for suspicious outbound connectivity	Redlock	
11	Compromised & Infected system tracking	Cb Defense, syslog, Redlock	
12	Tracking web application attacks	tCell, IPS/IDS	
13	Evil Insider		
14	Anomalous Geo Location / Unauthorized Tethering	In-built rules from SIEM	

Orchestration Functionality

- **Data Enrichment**
  - IP reputation
  - Correlate with threat intel feeds
  - Correlate with other logs
- **Simply remediation**
  - ChatOps to block/disable/escalate
  - Privileged use – attestation at time access is granted
- **Long term plan:**
  - Pattern incident response behavior (feedback loop)

Questions