POSITKA

Why SIEM?

Features of SIEM

Combat Threats with Advanced Analytics

Powered by Security Information Event Management (SIEM)

- NETWORK TRAFFIC
- INTRUSION DATA
- ENDPOINT
- MALWARE AUTHENTICATION
- WIRE DATA
- ASETS & IDENTITIES

→

SIEM

SECURITY ANALYTICS

→

- Monitor Security Activity
- Correlate and Sequence Events
- Validate Alerts
- Prioritize, Review and Investigate
- Decide Best Path to Resolution

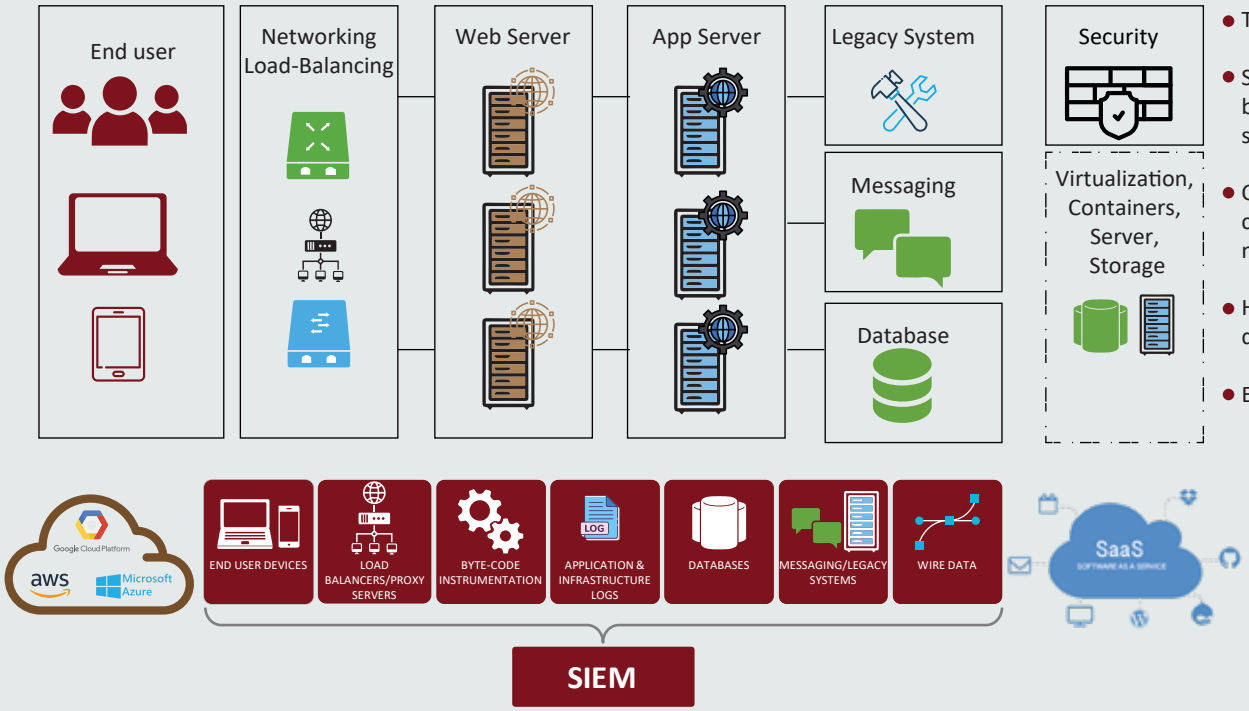
SIEM Use Cases

Security Monitoring | Compliance | Fraud Detection | Incident Response | Advanced Threat Detection | Insider Threat | Incident Investigation & Forensics | SOC Automation

Why do I need a SIEM when there are so many other security solutions?

SIEM vs. point solutions

I have Firewall / EDR / IPS / IDS and a million other things ... Why do I need a SIEM?



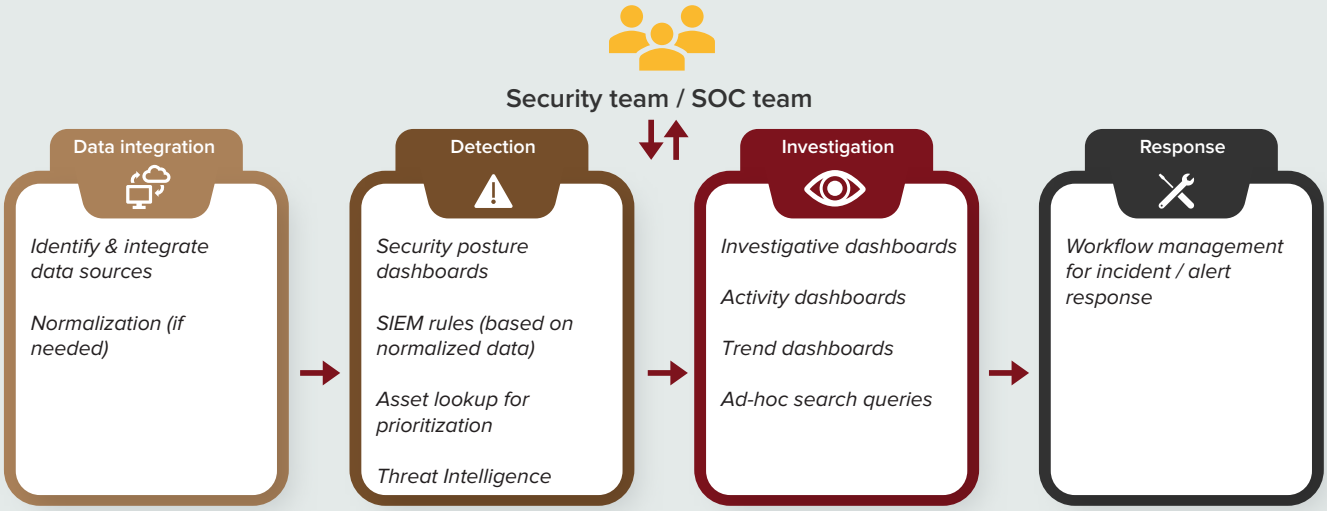
- Total visibility
- Simple to correlate between disparate data sources
- Context, enrichment capabilities, searching and more
- Handle vast amounts of data
- Excellent at detection

www.positka.com | susan@positka.com

POSITKA

Extracting true value from a SIEM

Key features of an effective security monitoring solution

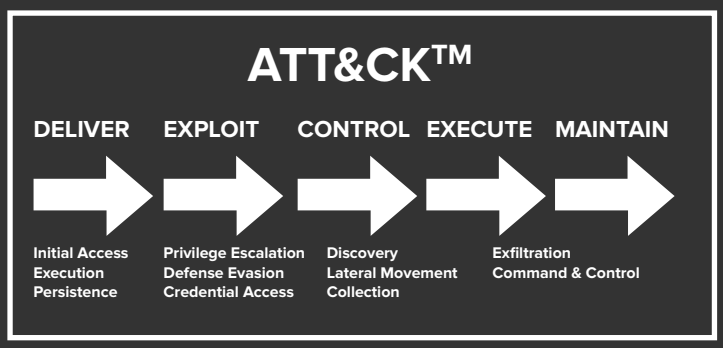


Looking for malicious activity

Some frameworks that can be utilized for effective threat hunting and detection

SIEM alerts mapped to ATT&CK show an attacker possibly moving through the cyber kill chain, over time

MITRE ATT&CK



Investig-ation

Risk aggreg-ation

Build up risk score of assets / identities, and alert on breach of risk threshold – Good for reducing noise & higher possibility of catching APTs

Threat Intel

IOC matching: Domain name, Email ID, IP address, URL, file hash, file name, etc.

www.positka.com | susan@positka.com

POSITKA

Key data sources for effective monitoring

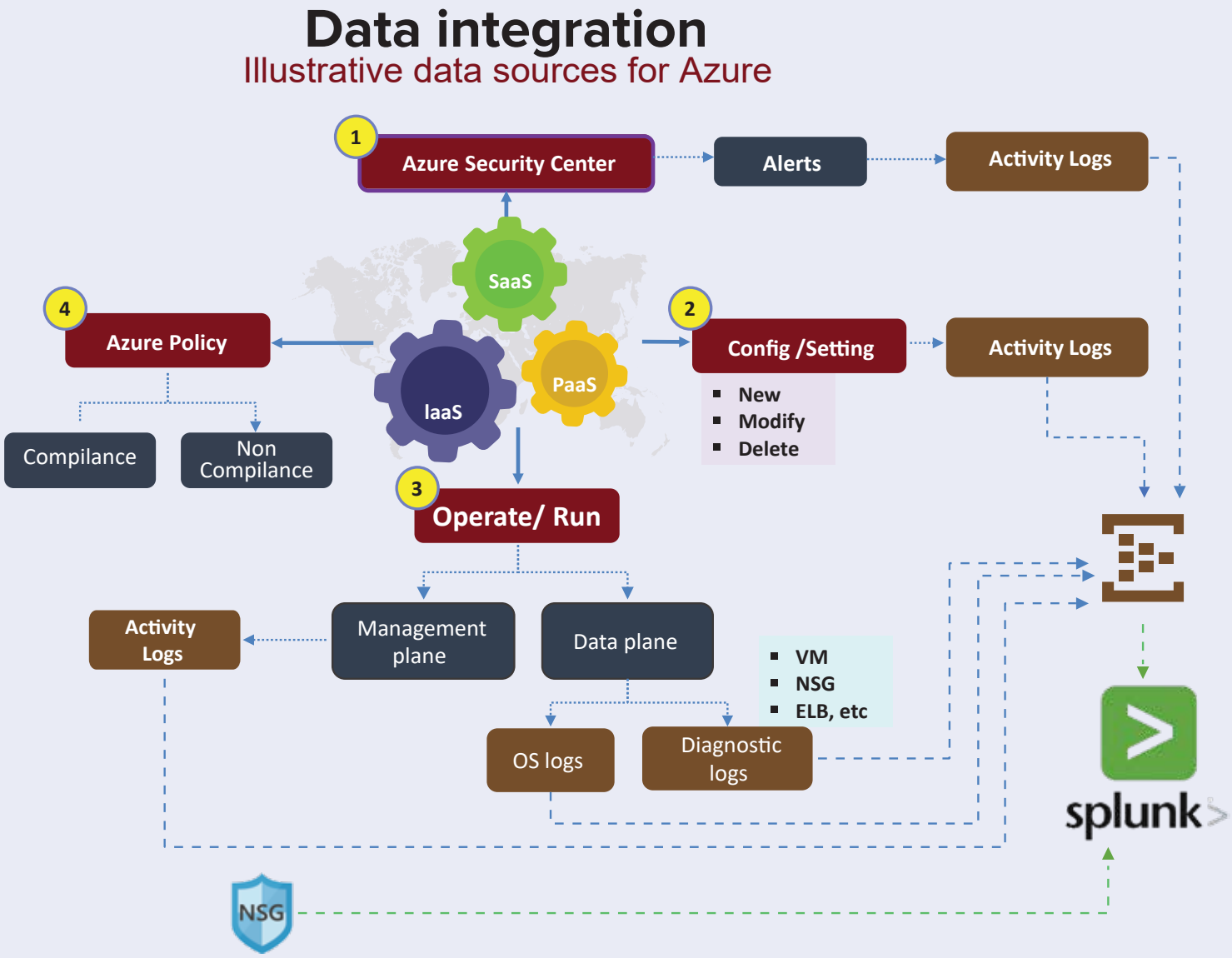
Typical data sources to Integrate (On-prem)

Integration – Key data sources

Typical On-premise data sources for security monitoring

Security infrastructure	Server Infrastructure	Network Infrastructure
Endpoint protection / Anti-Malware	Windows server	Routers syslog (via syslog server)
Firewalls	Linux server	Switches syslog (via syslog server)
Active Directory	Web server	
Web Proxy	DNS server	
Network IDS / IPS		
Authentication		

Typical data sources to Integrate (Cloud eg: Azure)

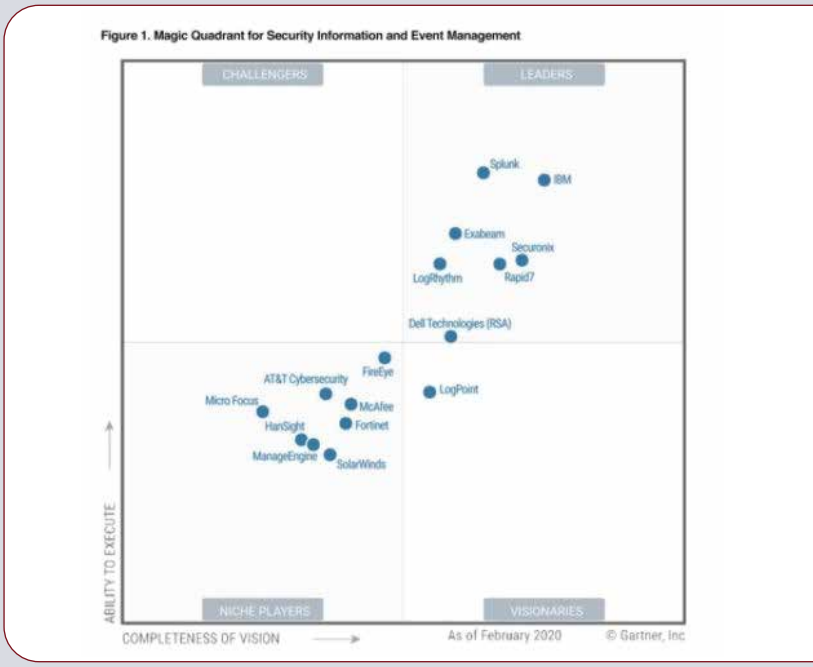


POSITKA

Why is Splunk the Best Solution?

Splunk a Leader in Gartner Magic Quadrant for SIEM

- Splunk has been recognized as a market leader by Gartner Research in the SIEM Magic Quadrant (MQ) for seven straight years in a row
- Each year Gartner evaluates vendors to determine the placement in the MQ.
- Splunk has helped customers to accelerate incident investigations and response



Positka's offering – RAPID ADOPTION PACKAGE

Bundle Overview

- **SIEM based on class leading platform (Splunk – Gartner Magic Quadrant leader)**
- **Fixed discounted pricing for up to 25 GB/day data ingestion Splunk license**
  - **Capable of onboarding ~ 100 – 150 devices**
- **Implementation:**
  - **Splunk deployment**
  - **Data integration**
  - **SSM installation and configuration**
  - **Rules installation and refinement**
- **Complimentary subscription to 30+ threat feeds matched to Splunk data**
- **Splunk installation technical support for 1 year [L1/L2]**

What next?

- **For more information on our security monitoring solutions or to request a demo, please visit our website**
  - **https://positka.com/cloud-security-monitoring-solution/**
  - **https://positka.com/smart-security-monitoring-solution/**
- **For any queries or to schedule a consultation, please reach out to us:**
  - **susan@positka.com**