

## About Us

Positka is a management consulting and technology solutions firm with head office in Singapore and presence across Asia, US and Europe.

Customers engage us to access the capability of business practitioners with deep domain knowledge and proven capabilities in leading edge technologies.

Our domain focus is on Security, Analytics, Lean IT operations, Digital transformation and Management Consulting.

We partner with leading technology companies such as Splunk, Palo Alto, IBM, Cisco, to address customers' requirements and challenges.

At Positka, we cater to customers across industry verticals with services and operational insights supporting a wide span of use cases.

## Our Global Footprints



SG: +65-3163-3225  
IN: +91-8939625405

US: +1-646-5689-760  
UK: +44 20 8089 2050

## Turning Machine Data Into Business Value



## Solution Areas

Cybersecurity

IT Operations

Environment coverage

Public Cloud (AWS, Azure, GCP)  
On-premises

Tools coverage



## CONTACT US

## Cybersecurity solutions

## IT Operations solutions

### Domain Expertise



- Understand the business context
- Assess threat exposure Design how to detect / prevent
- Select best-fit tools & processes

### Platform



- Data consolidation & analytics
- Provides single pane of glass view
- Set up advanced rules & alerting
- Flexible and easy to customize

### Automation



- Manage escalating alerts volume
- Speed of detection, triage, response
- Orchestrate point products for security
- Scale with limited professionals available

### Domain Expertise



- Understand the business context
- Identify problem statements, objectives
- Leverage the right People, Processes and Tools to achieve outcomes

### Platform



- Consolidate logs and events from virtually any data source
- Advance rules to fine-tune performance and capacity
- Full stack observability across infra, apps and services
- Flexible and easy to customize, massively scalable

### Observability



- Designed for modern, cloud-native apps
- Full-stack visibility
- Contextual insights into the behavior of critical business and operational systems

## Offerings Overview

### Platforms



#### Our Offerings

- SIEM: Splunk, Splunk ES, QRadar
- SOAR: Phantom, Cortex XOAR
- ITOA: Splunk ITSI, SignalFx

#### Customer Benefits

Future ready technology to scale with business needs

*Platforms capable of supporting multi-year maturity journey and use case evolution*

### Services



#### Our Offerings

- Consulting
- Implementation
- Managed Services

#### Customer Benefits

Partnership with trusted and certified experts

*Years of domain experience combined with technology expertise; end-to-end services by people you can trust*

### Products



#### Our Offerings

- Cloud Security Monitoring
- Smart Security Monitoring
- Threat Intelligence

#### Customer Benefits

Fast speed to value from your investment

*Products built on enterprise class technology; readily customised for your needs; fully supported by domain and technology experts*

## CONTACT US



Major Fast-Food  
Retailer

### Solution Elements

Integrate Cloud infrastructure logs (AWS) into Splunk and created a Cloud Monitoring dashboard serving as a central visibility model to provide insights of the user activities and resource utilization.

Automated report and alert generation to notify any suspicious/ important activity in the infrastructure

Provide real time operational intelligence across applications and services



Financial Services  
Major

### Solution Elements

Reorganize the existing infrastructure organization and prioritized processes that maximum savings opportunity and designed target end-state

Train client managers and implemented new data centre operations processes in 3 countries

Introduce solutions for process automation and developed and delivered analytics for productivity tracking and faster decision making



Top Global Bank

### Solution Elements

Measuring and correlating application performance to service performance by providing real-time insights into issues, errors, KPIs, SLOs, service visualization, notable events affecting SLAs.

Lowered MTTR through faster troubleshooting

Integrated with APM tools and improved full- stack observability



Leading Ride-Hailing  
service

### Solution Elements

Designed and defined security use cases working with payment experts

Architected highly automated solution for replication and scalability

Implemented world-class security analytics platform

Delivered SOC monitoring capability across multiple countries

Provide VAPT services to periodically test for security weaknesses

CONTACT US



[susan@positka.com](mailto:susan@positka.com)



[www.positka.com](http://www.positka.com)