

# Cyber Security Analytics Services

Applying Use Cases Beyond Just Compliance for Added ROI

## WHAT WE'VE DONE FOR OTHERS

### CRITICAL INFRASTRUCTURE

Proactive posture protected against logistic failures that could cost \$2Million per minute

### MAJOR AIRLINE

Achieved 45% drop in reactive tasks over a period of 6 months, allowing more time for proactive steps

### ENERGY UTILITY

Cut through the noise to correlate, analyze, and respond to 400 Million attack scans and probes per month

## WHAT WE CAN DO FOR YOU

BUSINESS USE CASE ADOPTION

ARCHITECTURE & DESIGN

PLATFORM INTEGRATION & ENHANCEMENT

OPERATIONAL MANAGEMENT

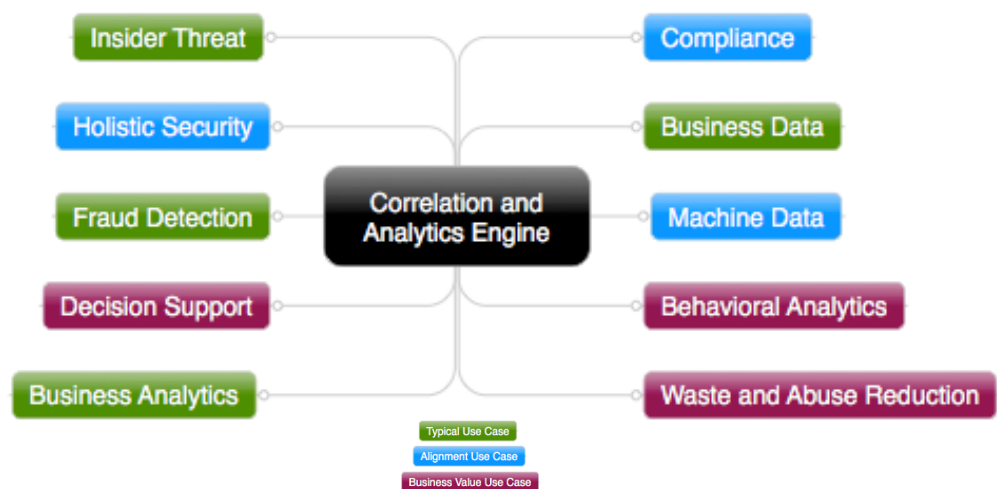
Performing correlation of log files is just the beginning of the cyber security analytics journey. Quantification of threats ideally requires correlating your business transactional data with machine data, so it becomes intelligence that can be leveraged by the business for decision support and process improvement.

However, even good input can sometimes yield garbage out when not properly managed. A lot has to do with how the input is selected, rules that are at the heart of the analytics platform, and what actions are taken from such alerts. From all of this, meaningful metrics should emerge, that prompt continual business improvement.

Case in point, having deployed a platform such as Splunk, a tremendous amount of noise is expected at first. The key is to filter that noise so business-focused intelligence can emerge. Until then, its a challenge to extract meaningful KPI's and SLA's. At times, its not known if its really working, or if heading in the right direction.

Most organizations start out with regulatory compliance as the first use case, however, ones that consider additional set of use cases such as below, transition to a higher maturity level:

### BUSINESS USE CASE SAMPLES



Taking on additional business use cases accelerates yield of value when existing use case maturity levels continually rise!

# Cyber Security Analytics Services

## Increasing Capability Maturity to Deliver Stakeholder Value

### CAPABILITY MATURITY MODEL

#### Behavioral Analytics

Predictive and Behavioral Model Development  
Integration with Business Strategic Direction  
Waste and Abuse Reduction  
High-Risk Profile Generation & Fraud Detection

#### Managed Metrics

Risk-Prioritized and Statistical Reporting  
Continual Analytics Improvement  
Measurement of Analytics Efficiency

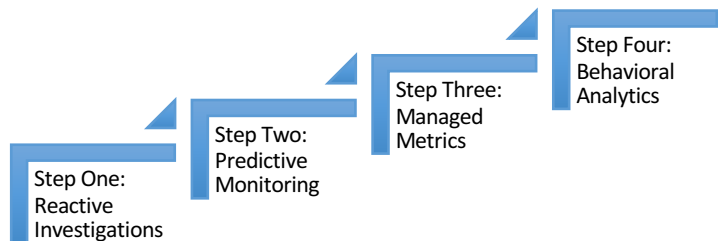
#### Predictive Monitoring

Benchmarking and Gap Analytics  
Dashboard Views with Drill Down Analytics  
Multi-Dimensional Linkages of Data Elements

#### Reactive Investigations

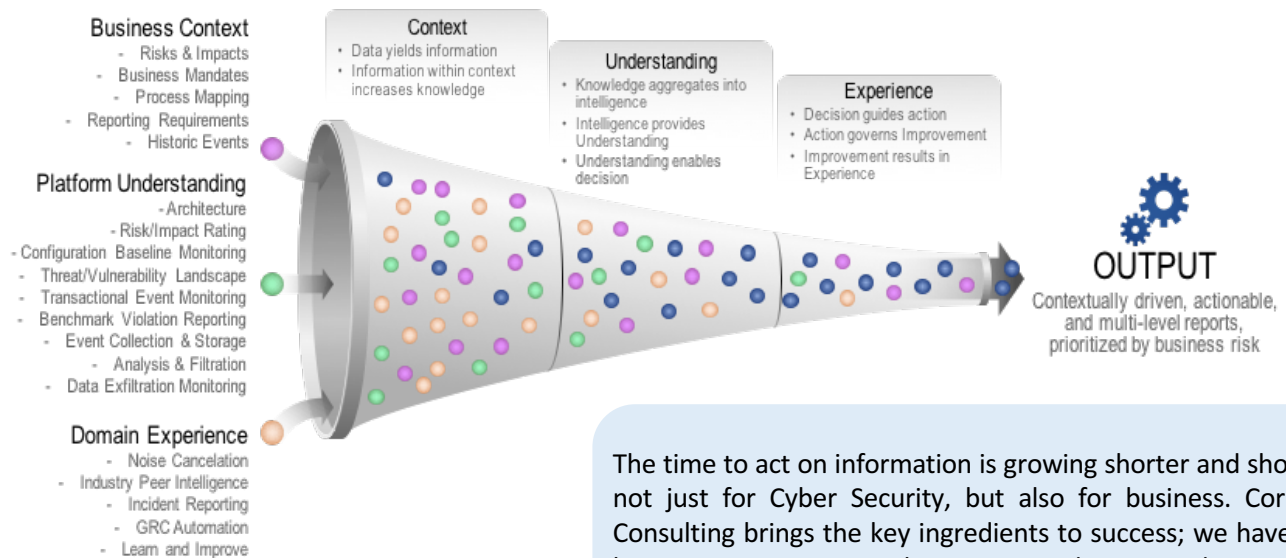
Measure of Effectiveness & Baselining  
Adherence to Compliance  
Setting the Stage for Proactive Measurements

There's a disconnect between noisy Alerts and meaningful KPI's/SLA's. The compliance investment you made can create real Business ROI by taking steps to increase maturity.



However, such an approach requires proper business context, including not just requirements, but also success measures. Managing business risks and partnering with stakeholders provides the understanding to succeed, coupled with our team's experience to ensure that you are delivering the value that stakeholders have yearned to realize.

By fulfilling additional business use cases, you will be relieved of the burden of justifying your investment on an annual basis. How is that for a win?



The time to act on information is growing shorter and shorter, not just for Cyber Security, but also for business. Corpnets Consulting brings the key ingredients to success; we have the business context, carry the necessary domain understanding, and apply our deep experiences to ensure your success.

You've already invested; now lets enable the business. Take the next step towards realization of business KPI's and SLA's. We are here to help!