

# A financial services firm teams with IBM to build its first SOC

## Optimize Your Security Investments

Identified and blocked

# 650+

suspicious incidents  
in the first 6 months  
of SOC operations



### ***Business Challenge***

- The bank did not have the security skills and resources to build its first SOC within the aggressive milestones set by their Board
- Wanted global protection for 16,000,000 accounts across 44 countries

### ***IBM Security Solution benefits***

- Automated real-time advanced analytics
- 24x7 SOC management and incident response support
- 13M+ events evaluated per day from 400K+ assets and 28K+ active log sources
- ~\$2M lower cost than in-house management

# An international energy company identifies critical events to investigate

## *Stop Advanced Threats with Security Intelligence*

An international energy firm analyzes

**2 billion**

events per day to find

**20 – 25**

potential offenses to investigate



### *Business Challenge*

- Reducing huge number of events to find the ones that need to be investigated
- Automating the process of analyzing security data

### *IBM Security Solution Benefits*

- Combined analysis of historical data with real-time alerts to gain a 'big picture' view and uncover patterns of unusual activity humans miss
- Immediately block suspected traffic

# A leading provider of information technology, consulting, and business process outsourcing services safeguards privileged IDs

## *Protect Against Unauthorized Access*

IBM Security  
Privileged Identity Manager for  
**500**  
privileged administrator users



### *Business Challenge*

- Increased security risks resulting from limited privileged activity monitoring
- Exposure to insider threat due to enterprise-wide sharing of privileged IDs
- Compliance issues due to poor privileged user management and lack of audit trail for privileged user access

### *IBM Security Solution Benefits*

- Streamlined and automated privileged user management
- Audit trail and monitoring of privileged access to all critical systems
- Safe management of shared privileged IDs and their passwords
- Full support of periodic privileged access recertification for audit and compliance