datacentrix showcase 2017
the reality of singularity

datacentrix

SECURITY

How Secure is your Organization?

WHAT
is going on?

Do you have the **visibility to prevent** becoming another global breach news headline?

Can your organization **detect and defend** in real time?

HOW
important is it?

Can you quickly and easily get the **security intelligence** needed to investigate and resolve incidents before they do damage?

How well does your organization **prioritize** incidents to avoid scrambling around false positives?

WHERE
should I focus resources?

Do you have the **right monitoring solution** to effectively deal with threats?

Is your organization **smart, fast, and able to automate** threat response actions across your security infrastructure?

Fidelity Security Group Case Study

Fidelity Security Group

- Est. 1958
- Acquired Springbok Security in 1998
- ADT Acquisition 2017
- 120 Branches in 6 countries
- 58 000 Employees
- 3rd largest Security Force in the country

Fidelity Security Group Requirements

Provide us with the same level of visibility and insight into our virtual world as we currently have in our physical environment


PASSWORD
PASSWORD

SA POLICE SERVICE
SA POLICE SERVICE
SA POLICE SERVICE
SA POLICE SERVICE

Fidelity Security Group SOC Requirements

- Real time visibility into Security Breaches
- Full incident management
- Advanced Threat Detection Capabilities
- Threat Identification
- Advanced correlation across all IP based devices
- Policy breach and enforcement
- Daily Security Posture reporting
- Forensic Case Study

SITE VISIT

CIT BRANCH

- Interviewed CIT Staff
- Walked through all processes
- Understand the blend between physical and virtual worlds
- Understand the temptation

Fidelity Security Group

PILOT

- Deployed collector
  - Integrated a number of IP Assets into SIEM and SOC
- Defined Business Use Cases
  - Enabled security policy enforcement
  - Configured scenario based detection metrics
- Created incident management work flow
  - Roles and responsibilities and metrics
  - SLA Defined activities
- Base Line reporting

Fidelity Security Group

Fidelity Take On

Achieved full compliance across all requirements

Fidelity Security Group

Pilot to Production

- Switched POC to full production SOC Service
- Further refinement of reporting, daily, weekly, monthly
- Established Security Operations Committee
- Develop Custom Dashboard for onsite visibility
- Deployed several security controls across the entire organization
  - 90 sites
- Live within 30 days

Fidelity Security Group

ADT

- ADT Acquisition
  - 30 sites

Datacentrix SOC Solutions

INTELLIGENT

Real-time advanced analytics

Automated rule, risk/behavior and statistical correlation

Threat prioritisation

Turns billions of “so what” events into actionable information

ACTIONABLE

Active and customisable dashboards

Makes threat investigation and response easy

High performance data management engine

Fast response to data ingest, analytics and threat investigations

Ease of operation

Hundreds of out-of-the-box rules and reports plus a unified compliance framework

INTEGRATED

Comprehensive security

Broad data collection of devices, including cloud and VM support, plus McAfee Security Connected active integrations enable efficient and effective response