ClearSkies Re-Defining SIEM with BigData Security Analytics

Irene Selia
iselia@odysseyc.com
Product Manager, ClearSkies

ODYSSEY Cyber Security
Impossible Challenges, Possible Solutions!

Agenda

1. Concerns/Challenges Faced by Organizations Today
2. We Live in the Internet of Everything Era
3. SIEM As A Service
4. What Will Help you Achieve
5. Available ServiceModules
6. BigData Security Analytics
7. Re-Defining SIEM with Big Data Security Analytics

On-Premise SIEM Implementations

Concerns Faced by Organizations Today:

- Simplify and Reduce the Implementation Time
- Ongoing Maintenance and Administration
- Scalability
- Streamline Event Log Collection
- Effectiveness of Log Analysis
- Minimize Operational Cost
- Enhanced Compliance

SIEM Security As A Service

50% *of new SIEM implementations will be delivered via SIEM-as-a-Service* ***by 2020***

60% *of all advanced Security Analytics will be delivered from the cloud as part of SIEM-as-a-Service offerings* ***by 2020***

Source: Gartner "Innovation Insight for SIEM as a Service" Report November 2015

We live in the Internet of Everything Era

Challenges Faced by Organizations Today:

1. Treat Landscape is changing
Cyber-Criminals are:

- Well Funded
- Better Organized
- Highly Skilled
- Using Sophisticated Tools
- Highly Motivated ← **Money**

We live in the Internet of Everything Era

Challenges Faced by Organizations Today:

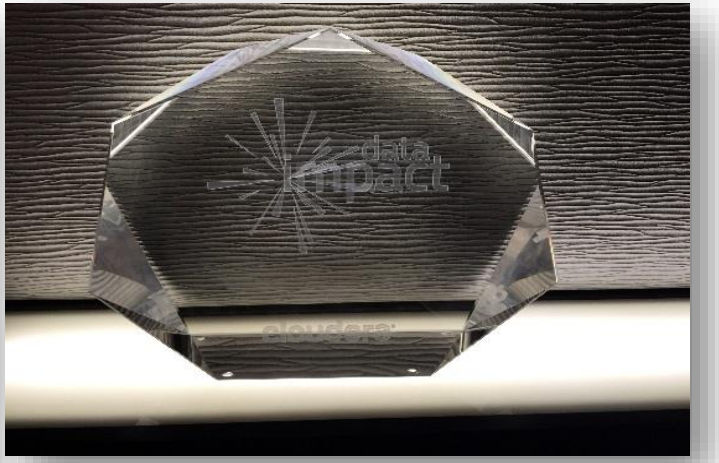
1. Organizational **Networks Expands** in Size and Complexity
2. More Difficult to Manage the **Exponentially Increasing Volume** of Log Data Generated By the Connected Devices.

50 BILLION *devices will be connected to internet,* by ***2020***

ClearSkies Architecture

2015 Data Impact Awards

Most Admirable Architecture



data impact

www.odysseyc.com

ODYSSEY Cyber Security
Impossible Challenges, Possible Solutions!

What will help you Achieve

- **Uncover** Suspicious **Attack Patterns** and **Security Anomalies** in-Real-Time
- **Achieve up to 95% Reduction** in the Number of **False - Positive** Alerts
- **Significantly Accelerate your Organization's Proactive** Cyber-Threat Detection Capability
- **Protect the Confidentiality** of Sensitive Information with Data Masking Functionality

What will help you Achieve

- **Safeguard the Integrity** of Log Information Ensuring that they can be Utilized for Forensic Investigation Purposes

- **Streamline your Compliance Process** as it Enables you to Drastically Simplify your Compliance Reporting

- **Clear, Real Time** View of Important Information Security Incidents, Metrics and Indicators Through Smart, Fully Customizable Intelligent Dashboards

ClearSkies ServiceModules

BigData Security Analytics

Processing and Analysis of Large Volumes of Log Data in Real-Time for Identifying **Patterns** and **Behavior** that represent **Real-Cyber-Threats** and/or misuse, which would go unnoticed by traditional analysis tools and techniques by utilizing:

- Behavioral,
- Predictive,
- Machine Learning

Re-Defining SIEM with Big Data Security Analytics

Put Right Away at Your Fingertips **Unique Functionality**, **Tools** and **Intelligence**, which will Enable you to Successfully Address the Cyber-Security Challenges of the Internet of **Everything Era**

www.odysseyc.com

ODYSSEY Cyber Security
Impossible Challenges, Possible Solutions!