Corporate Overview

- Established in 2003; Based in Ottawa, Canada
- Products: Network and Security monitoring solutions
- Services: Network and Security software analytics
- Expertise: AI/ML for Traffic Analysis, cyber security; Large scale network asset discovery
Solana Products

**SmartFlow**
Security Monitoring based on Network Anomaly Detection & Machine Learning

**SparrowIQ**
Advanced Network Traffic Analytics

**SmartHawk**
Network Asset and Topology Discovery for Large Enterprises and Service Providers

www.solananetworks.com
Solana Services

Cyber Security
Specialist in network security -- machine learning based POC development for cyber threat detection in automobile, SCADA and IT networks

Software & Applications
Networking Software development for network and data centre asset discovery, traffic analysis and ML based analytics development
Example Cyber Security Projects

1. SmartFlow – Netflow based anomaly detection solution for IT networks
2. Cyber Defence Decision Support Tool
3. Intrusion Detection System - SCADA
4. CYTHREIDS - Cyber alert false positive reduction
5. Cyber threat detection for automotive application
SmartFlow – Netflow Anomaly Detection

- Identify attacks based on traffic flow anomaly
  - Baseline network behavior & apply analytics on flow features to detect anomalies
  - Pinpoint offending flows
  - Analyze flow characteristics to identify attack type
  - Drilldown capabilities to detect offending Ips
  - Integrate with discovered network topology & network map
Cyber Network Defence

**Problem:**
- Cannot block all security threats
- IT security resources/budgets are finite.

**Solution:** Tools to understand network cyber posture & vulnerabilities:
- Analytics to evaluate cyber security risk
- Identify potential risk mitigation actions
- Proactive suggestion of remediation / actions

Retrieve data from multiple cyber security sensors & combine with analytics
Intrusion Detection System (IDS) for SCADA Industrial Control Network

- Implemented module for Suricata IDS
- Added support for signature-based threat detection for the EtherNet/IP Protocol (ENIP)
- Available in Suricata 3.2 Release
- Designed to work with Snort Rule-sets
- Work involved
  - Rule parsing & Packet parsing
  - Signature-based match functions
  - Alert definitions
**Problem:**
- Security tools generate a large number of false positives that overwhelms analysts
- Use analyst’s feedback combined with machine learning to reduce false positives

**Solution:** Develop a system with Human-in-the-Loop (HIL):
- Analyst flags cyber alerts as valid and invalid during learning phase and used to build a supervised ML model
- For prototype, alerts from 3 security sensors are used: IDS, Anomaly detector and Web logger with SSH attack prevention
Cyber threat detection for Automobile

**Problem:**
- Detect cyber threat in automobile CAN bus
- Solution must be with a low computation cost

**Solution:** Cyber threat detection by analyzing traffic behavior:
- The approach uses machine distributed computation to reduce computation cost
- Advanced machine learning techniques on CAN bus data is applied to ensure low false positive
- The solution works as complementary approach with other threat detection mechanism

Source: McAfee Labs