MAKING SECURITY SIMPLE

DATA SECURITY

APPLICATION SECURITY

THREAT INTELLIGENCE

INFRASTRUCTURE SECURITY

CONTRAST SECURITY

Blueliv.

randtronics

sonatype

TeejLab
DATA | RESEARCH | SOFTWARE | INNOVATIONS

SENSORFLEET

Arctic Security

RUGGED TOOLING

MAKING SECURITY SIMPLE

Hot and Trending

- Digital Transactions
- Open Source
- API Usage
- IoT
- Security Assessments
- Intelligence Driven Cyber security
- NGN Application & Network Security testing
- DevSecOps

Image by Gerd Altmann from Pixabay

RamoGnee Technologies Pvt. Ltd
Making Security Simple

Benefits

- Emphasis on technologies for early and automated detection, and into small actionable steps developers can take quickly

- Improved ROI in existing security infrastructure

- Improved operational efficiencies across security and the rest of IT

- CI/CD integration & Continuous application monitoring

- Threat hunting internally would enable proactive approach

- Security ownership across organization

- Greater speed, collaboration and agility for security teams to respond to change and needs rapidly
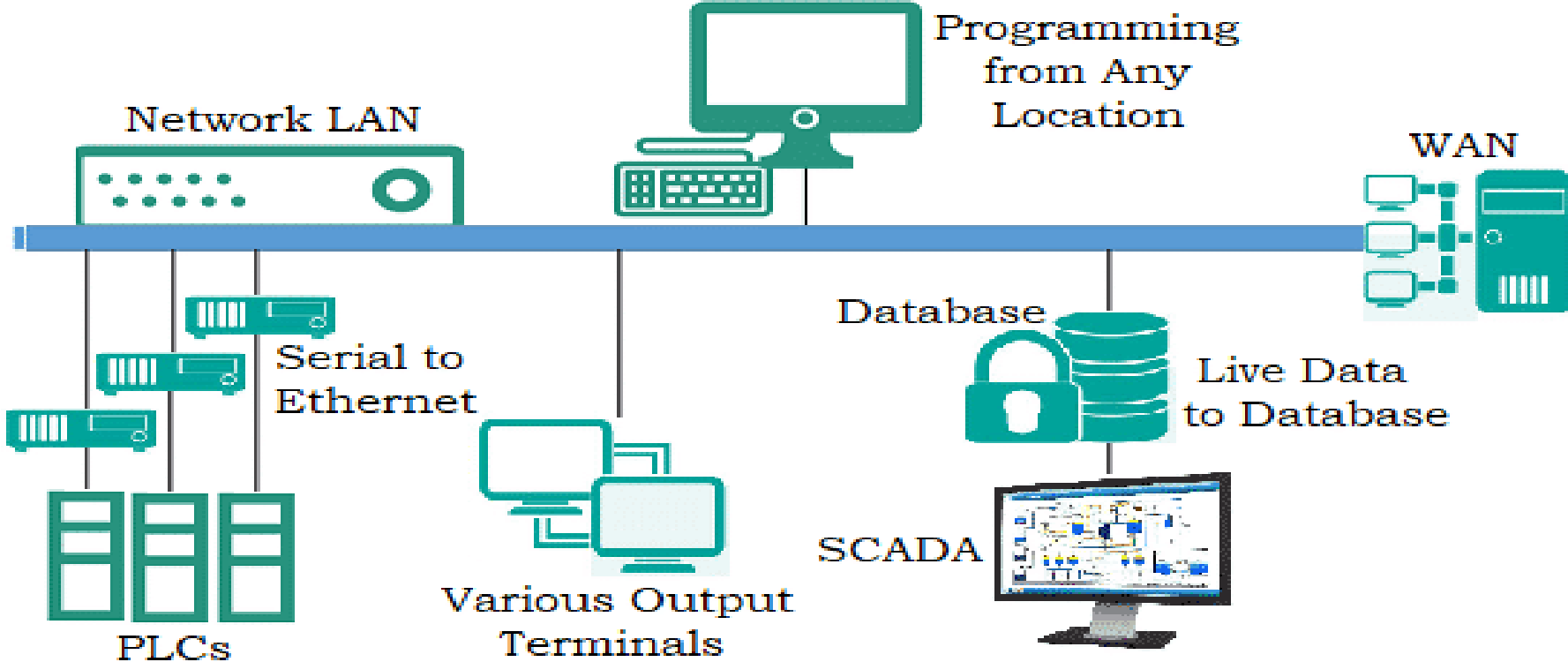
Myths

➢ Myth #1- ZERO Open Source Consumption

➢ Myth #2- Network security testing takes care of my application security

➢ Myth #3 – Best tools they are automated and find " Application Vulnerabilities "

➢ Myth #4 – Audits mandate and many random

➢ Myth #5 – A strong manual testing team and they have never found a single vulnerability

➢ Myth #6– Our OEM has given a declaration

Cloud, SCADA and IoT security – Y Secure?

❑Cyber threats: sophisticated and professional

❑Deployment and adoption: Quick with dependencies on 3rd party components, usage of components with little/zero security testing, NO BOM

❑Cyber Attacks: focused, motivated and dedicated politically or financially

❑Specialists: Hackers who know these domains and their exploits

❑Zero-day Vulnerabilities- or Unknown: 2014 onwards they are growing

SCADA Architecture

Network LAN

Programming from Any Location

WAN

PLCs

Serial to Ethernet

Various Output Terminals

Database

Live Data to Database

SCADA

IoT Architecture

IoT Architecture

Challenges

- ❑ Cloud Security
  - ❑ Perimeter Security meeting my requirement?
  - ❑ Choosing the right Cloud infrastructure and components
  - ❑ Are Applications Security tested & cloud ready
  - ❑ Is my data secured?
- ❑ SCADA & IoT
  - ❑ Are the devices security tested for vulnerabilities
  - ❑ Is there a mechanism to manage these devices
  - ❑ Are they truly isolated
  - ❑ How is information fed back to teams to be proactive

Best Practices

- Cloud
  - Focus on applications which are CI/CD Ready
  - Applications hosted should have exposed API
  - Ensure Data privacy to ensure data is encrypted always and right to information
  - Security testing all applications
- SCADA & IoT
  - Application security- testing of SCADA and IoT Protocols
  - Ensuring you have a detailed BOM of all components consumed and managing of OSS
  - Conducting of Application security testing
  - Deployment of Pure Network Isolation solutions and monitoring the network
  - Feeding back of security vulnerability data back to the team

About Us

- A young team who look at IT Security a little differently

- Solutions are focused around Automation, DevSecOps, Securing your supply chain and ensuring a continuous monitoring of your network and environment.

- Our strength lies in helping Software and Hardware factories and users adopt DevSecOps and Security best practices early, thus enabling them to be secured.

- Not just provide the tools, but match it with our strong domain expertise and knowledge of these tools

- Cover application security, data privacy and management, network security and isolation and incident monitoring.

- Customers - Welcome to be one

IF YOU WANT TO MAKE SECURITY SIMPLE

EMAIL- MRAMPAL@RAMOGNEE.COM OR SALES@RAMOGNEE.COM
OR CALL US AT MSS +91-9871583777