CenturyLink®
Top Cyber Security Trends – 2018

Robert Anderson
Principal Cyber Security Architect

May 1, 2018

CenturyLink®

Some Background Information

CenturyLink Cyber Security

OWASP The Open Web Application Security Project

CYBER THREAT ALLIANCE

cloud security alliance® CSA

NATIONAL CYBERSECURITY ALLIANCE

Joined CenturyLink Cyber Security in FEB 2015

- Principal Cyber Security Architect
- Developed Solutions for our MSS Platform & Portal
- Developed Broad Array of Solutions for All Primary Cyber Security Functions and Domains
- Developed the Cyber Security Consulting Practice

25 Years in IT and Cyber Security

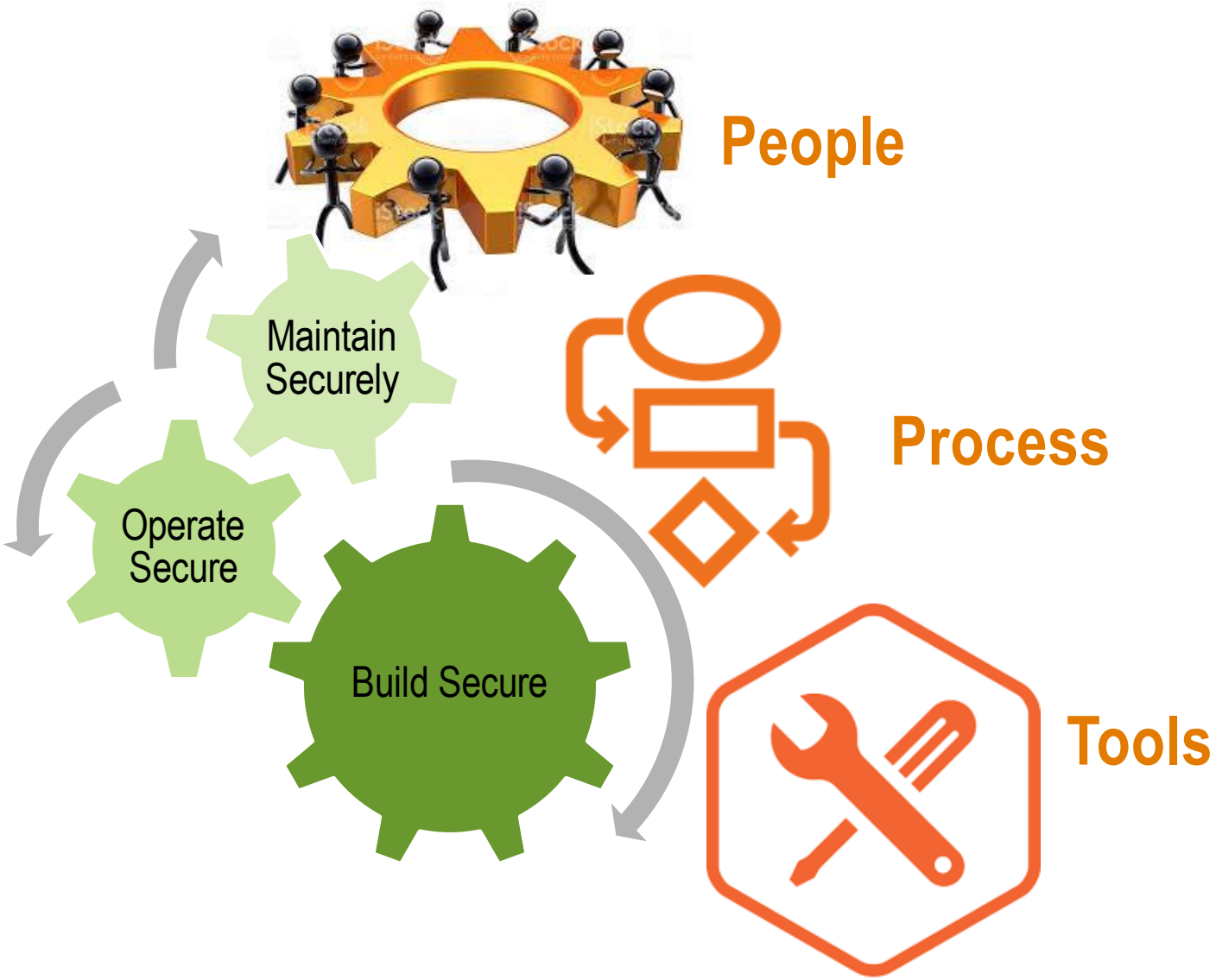
- Highly Trained – Multiple IT/Cyber Certifications
- Developed 500+ Cyber Solutions or Programs
- Cyber Security Experience in multiple of Industries
- Acting CISO/Director of Cyber Security

12 Years in Intelligence and PSYOPS

- Supported Multiple Information Warfare Missions
- US Army/Israeli Interrogation Training/Instructor
- Arabic Linguist and Translator

Observations of other Cyber Security Professionals – 2018

Enterprise Life-Cycle Cyber Security



Overall Peer Opinions in Cyber Security for 2018

- Cyber Security Budgets Increasing from 5% - 10%
- Organizations exploited by a Cyber Attack over 75%
  - Quantity of Successful Cyber Attacks has decreased
  - Frequency of Successful Cyber Attacks has decreased
- Most feared Cyber Threat
  - Phishing/SpearPhishing
  - Advanced Malware
- Cyber Security Most Susceptible Areas
  - Cloud Infrastructure Systems
  - Application Containerization
  - Mobile Devices and Applications
- Largest Challenge in Cyber Security Programs
  - Cyber Security Staffing and Skills is still the largest Challenge
  - DevSecOps is the new Challenge to Cyber Security
- Cloud Deployments and Systems are expanding
  - Cyber Security Challenges are increasing
  - CASB deployments are increasing

Overall Peer Investments for Cyber Security for 2018

Highest Tech Planned for Acquisition

- Cyber Security Budgets Increasing from 5% - 10%
- Advanced Malware Analysis Solution – Sandboxing
- Next Generation Firewall – NGFW
- Deception Security Solution – Honeypots
- User/Entity Behavior Analytics – UBS/UEBA
- Cyber Threat Intelligence Solutions

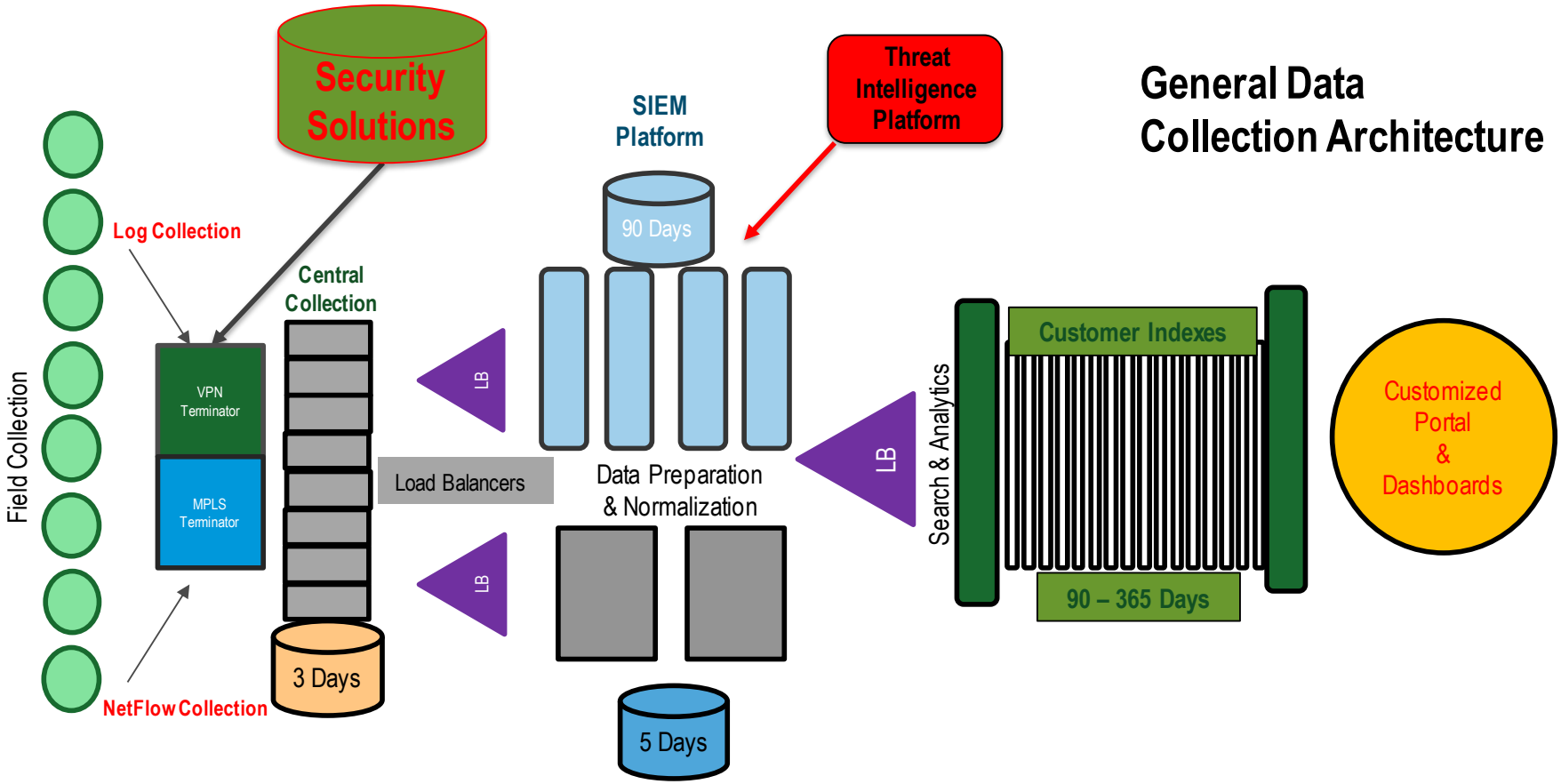
Lowest Tech Planned for Acquisition

- Standard EndPoint Security or Anti-Virus (AV)
- Security Email & Web Gateways
- Privileged Access Management (PAM)
- Deep/Full Packet Capture Analysis
- SSL/TLS Decryption Solutions or Platforms
- Data Loss Prevention (DLP)

Cyber Security Strategies for 2018

- **Implement a Threat Intelligence Solution**
  - Faster MTTD
  - Faster MTTR
  - Major Impact on EPAH
- **Contract with a Managed Security Service (MSSP)**
  - Provides Security Expertise
  - Proven Cyber Security Platform
  - Augment FTE Staff as needed
- **Deploy a Cloud Access Security Solution**
  - Consider a CASB – Budget Issue
  - Monitor All Access to the Cloud
  - Detect and Block Access
- **Deploy more Cyber Security in the Cloud**
  - More Scalable & Agile
  - Broader Global Defense
  - Outsourced Management
- **Deploy Intelligent Automated Asset Management**
  - CMDB vs Patching/Upgrades
  - Orchestration of IT Activities
- **Implement DevSecOps policy and process**
  - Increases Application Security
  - Avenue - Attack Surface Analysis
  - Adapt to a Threat Model for Risk

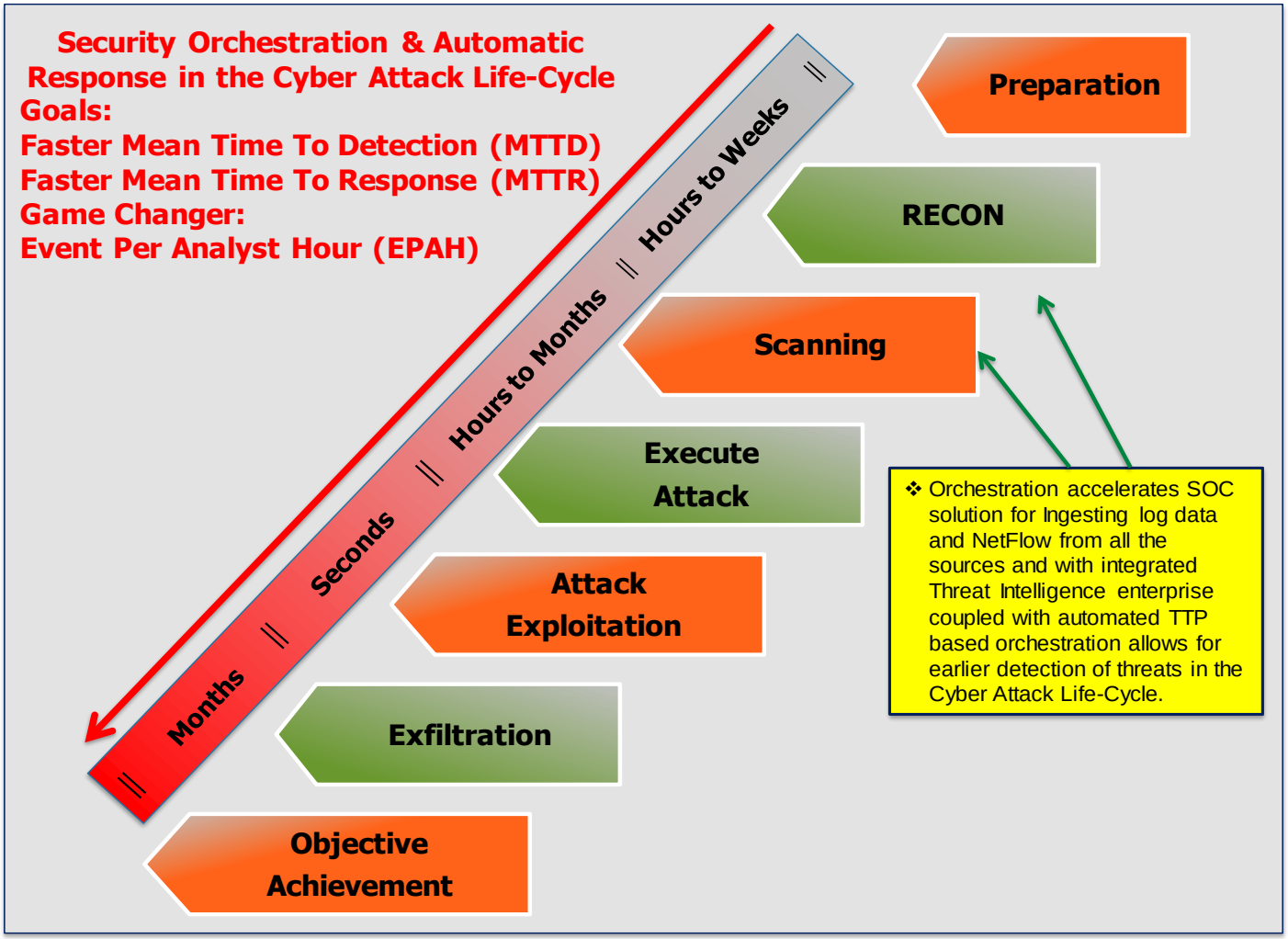
Next Generation SIEM Platforms



Cyber Security Use Cases for NextGen SIEM

- Standard MSS SIEM Security Use Cases
- EndPoint Detection & Response – EDR Use Cases
- User/Entity Behavior Analytics – UBA/UEBA Use Cases
- Deception Security Use Cases

Security Orchestration Automated Response – SOAR



Questions & Answers