Leading Industry Security Concerns

Facilitator: Jim Henry, CHS Inc.

Speakers:

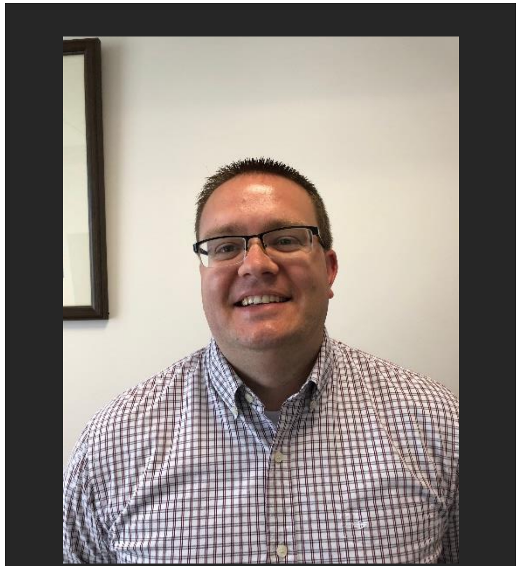
John Timian, Stewart's Shops
Ashwin Swamy, Omega ATC

Introductions

Pinnacle Summit

Jim Henry, CHS
Facilitator

Pinnacle Summit



Jo [illegible] mian,
Stewart's Shops

Pinnacle Summit

Ashwin Swamy,
Omega ATC

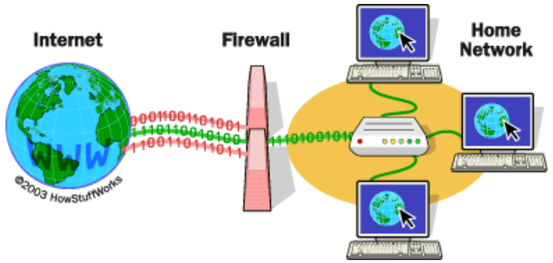
Agenda for Panel Discussion

Three Categories for Panel Discussion:

1. Physical/Hardware
2. Logical/Software
3. People/Training

Category – Physical/Hardware

1. Firewall protection



2. POS and Network Equipment locked up and stored

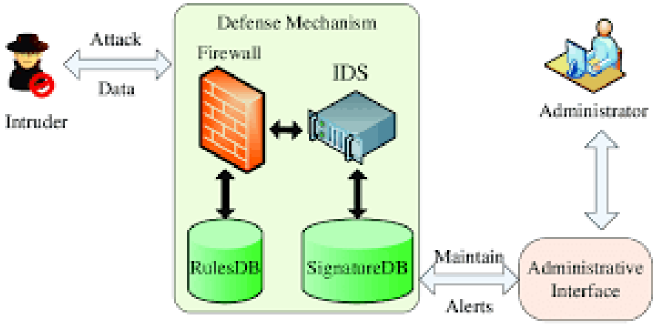
3. Dispensers have proper locks and security tape

4. Secure Card Readers and Encrypted Pin Pads

© Convenience Store Technologies, LLC

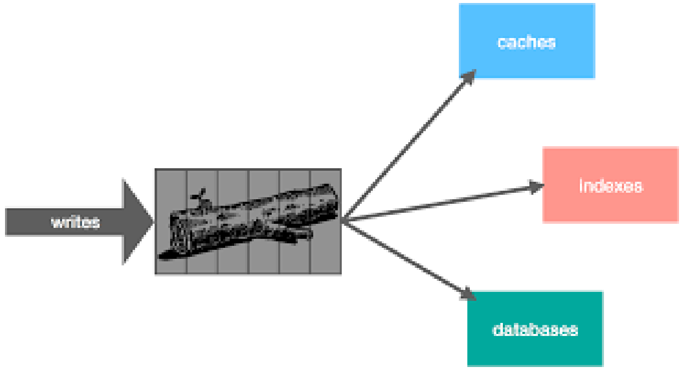
Category – Logical and Software

1. **Intrusion Detection System (IDS) and Intrusion Preventive System (IPS)**



2. **Antivirus and Anti-malware**

3. **Centralized Logging**

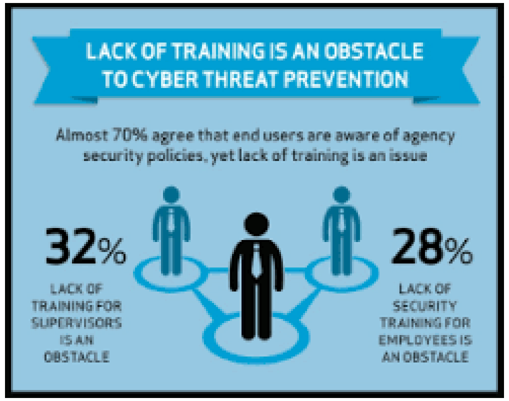


4. **Current/Up-to-Date Software and O/S**

5. **Equipment Configurations**

Category – People and Training

1. Insuring personnel are trained on what to look for


LACK OF TRAINING IS AN OBSTACLE TO CYBER THREAT PREVENTION

Almost 70% agree that end users are aware of agency security policies, yet lack of training is an issue

32% LACK OF TRAINING FOR SUPERVISORS IS AN OBSTACLE

28% LACK OF SECURITY TRAINING FOR EMPLOYEES IS AN OBSTACLE

2. Complete Equipment Inventory

3. PCI Training and Audits

shutterstock.com • 603785879

4. Proper Policies and Procedures

5. Incidence response and management

Managing Network Security

Stewart's Shops

John Timian

Bio + Company Info

Stewart's Shops

- 3rd generation, family and employee owned
- 334 stores throughout upstate NY and Western Vermont
- Known in the area for ice cream, MYO sundaes, coffee, and award winning milk
- Started at Stewart's Shops in 2004
- Spent first few years on the road installing Pinnacle Palm throughout our chain
- Project lead for Lottery Inside project with Gtech, epay integration, EMV conversion with Worldpay, and most recently the Sunoco integration

Pinnacle Summit 2019

Pinnacle CORPORATION

Store Networking

1. Every shop has a Juniper router and managed switch with a VPN connection back to corporate office
2. Shop specific IP ranges
3. Registers joined to Stewart's retail domain
4. Router has port specific functions – 1 port to the managed switch, 1 port dedicated to Gtech for lottery router, 1 port for cell connection, 1 port for cable connection
5. Firewall configurated with implicit deny all
6. Switch is configured to only have certain ports active to reduce number of potential rogue devices
7. Separated into different VLANs – 1 for PCI side equipment, 1 for IP Phone, 1 for non-PCI scope equipment
   - Configuring a new VLAN to support EMV outside

Store Physical Security

1. All network equipment is now in a locked network cage
2. Developing an ID app for our shop handheld device that would allow partners to confirm identity of someone looking to gain access to back room
3. Shop Inspections – periodic checks of all payment devices for skimmers by our gas service company and Tech Center personnel

Store Software Security

1. CarbonBlack (Bit9) – whitelist software forces any executable to be approved from corporate before it will run on registers
2. Windows Updates – within 30 days of release by Microsoft for all Critical and Security patches (SolarWinds Patch Manager)
3. Dual-factor authentication for any user trying to access store network (RSA)

Corporate Security

1. Data Center is accessed only with prox card
2. Video monitoring
3. Roles defined in Active Directory for store level access
   1. Tech Support
   2. Gas Marketing
   3. Video Retrieval
4. Monthly PCI meetings to review policies and procedures
5. Internal and External penetration testing
6. PCI on-site audits
7. Developing Security Training app for shop level partner awareness

Takeaways

Much easier now to plan projects with Security as a main component as opposed to an afterthought and having to layer it in

We are in the Convenience industry…
Security is not Convenient!

SECURING THE SMART STORE

Ashwin Swamy
Director - Resilience
Omega ATC

About Omega ATC

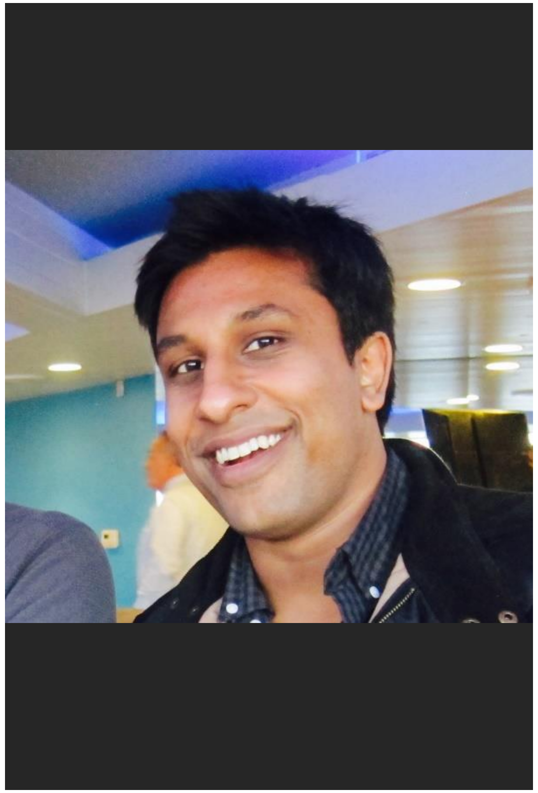
1. Offering solutions for retail systems since 1991.
2. Based in St. Louis, Missouri
3. Pinnacle partner since 2009
4. Offer solutions for endpoint management and security, network management and security, and operational intelligence.
5. Level 1 PCI DSS 3.2 Service Provider

Pinnacle Summit 2019

About Ashwin Swamy

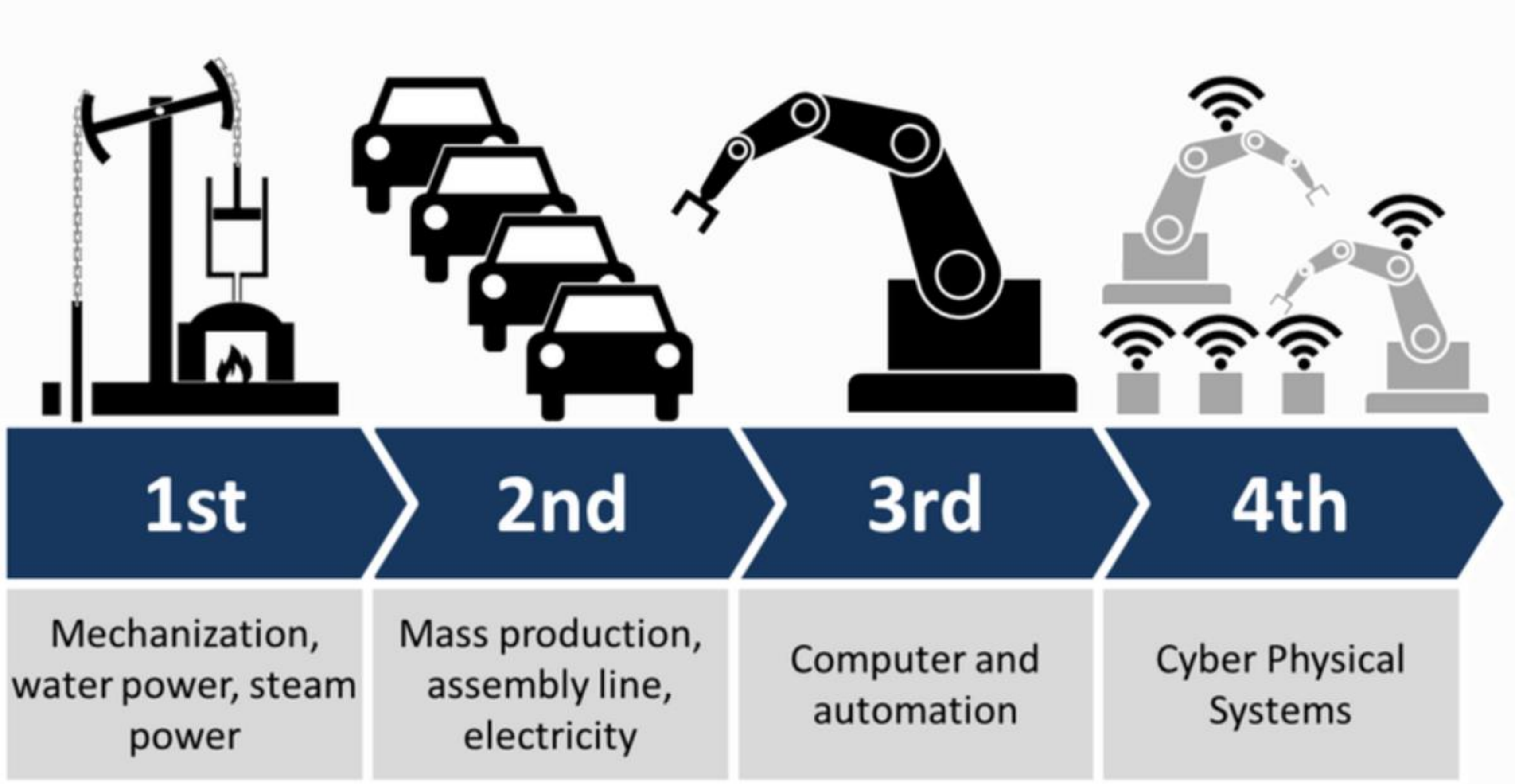
1. Previously consultant with IBM; focused on developing smart grids for public utilities (outage management and geographical information systems)
2. Data Scientist with background in supervised and unsupervised machine learning.

Pinnacle Summit 2019



Pinnacle CORPORATION

The Fourth Industrial Revolution is driving the next wave of “big data” and making stores “smarter.”



1st
Mechanization, water power, steam power

2nd
Mass production, assembly line, electricity

3rd
Computer and automation

4th
Cyber Physical Systems

The 4 Industrial Revolutions (by Christoph Roser at AllAboutLean.com)

The Fourth Industrial Revolution is driving the next wave of "big data" and making stores "smarter."

POS System

The Fourth Industrial Revolution is driving the next wave of “big data” and making stores “smarter.”

POS System

SMART SHELVES

BUILDING MANAGEMENT SYSTEMS

SIGNAGE

SECURITY CAMERAS

DRINK COOLERS

TRAFFIC COUNTERS

CAR WASHES

REFRIGERATORS

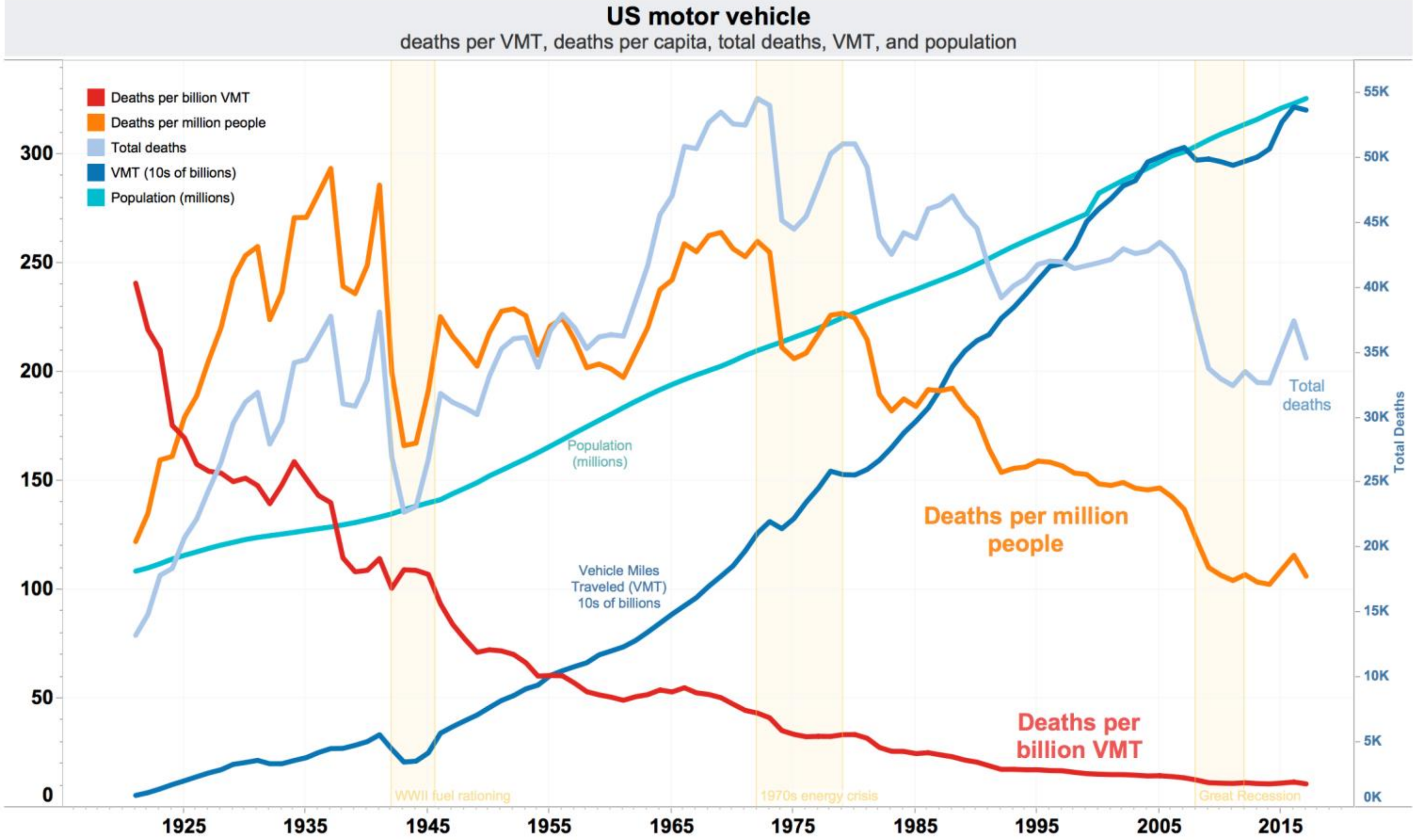
FRYERS

THERMOSTATS

PUMPS

Overview -- security and IT operations should not be managed separately.

Overview -- security and IT operations should not be managed separately.



Source: National Highway Traffic Safety Administration

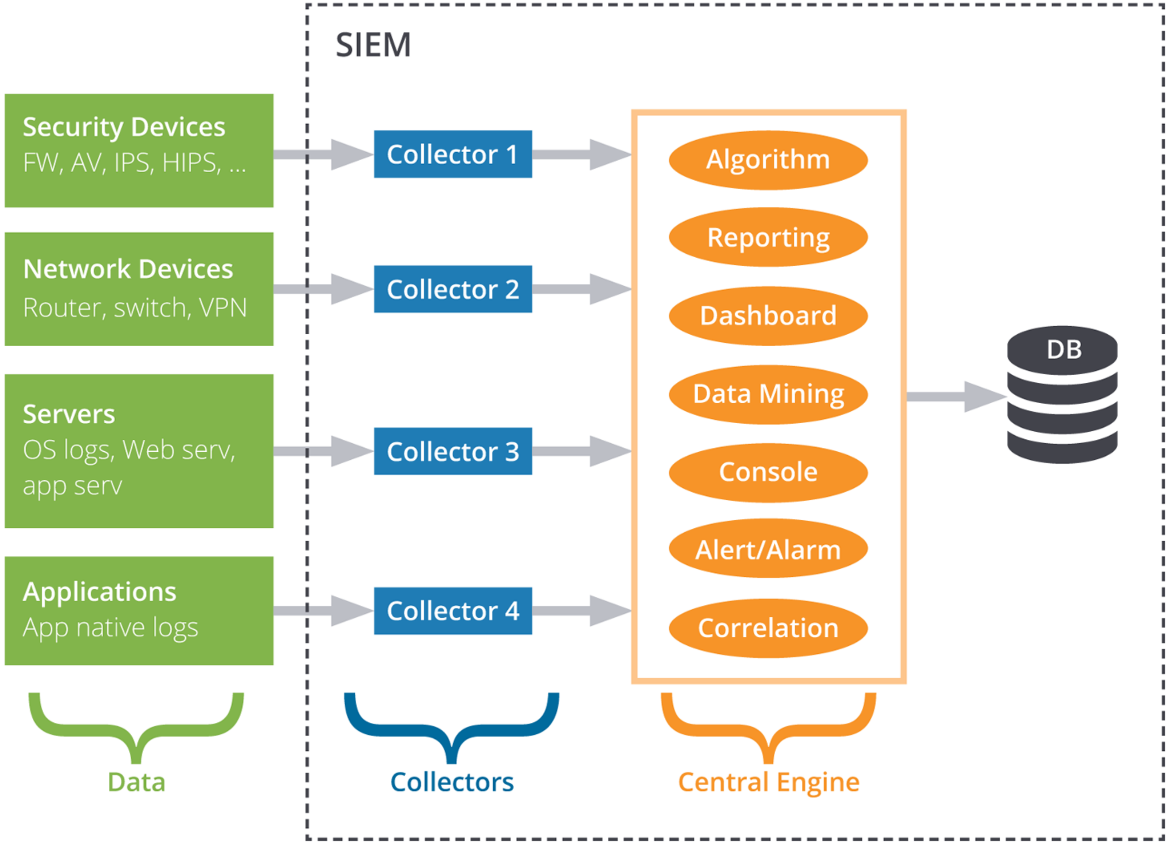
Overview -- security and IT operations should not be managed separately.

1. Take a resilient approach to managing systems – visibility, prediction, rapid recovery, flexibility, automation.
2. Collect data on all devices in the environment to ensure overall operational health.
3. Automate whatever you can so you can focus on convenience!

Take a resilient approach to managing systems – visibility, prediction, rapid recovery, flexibility, automation.

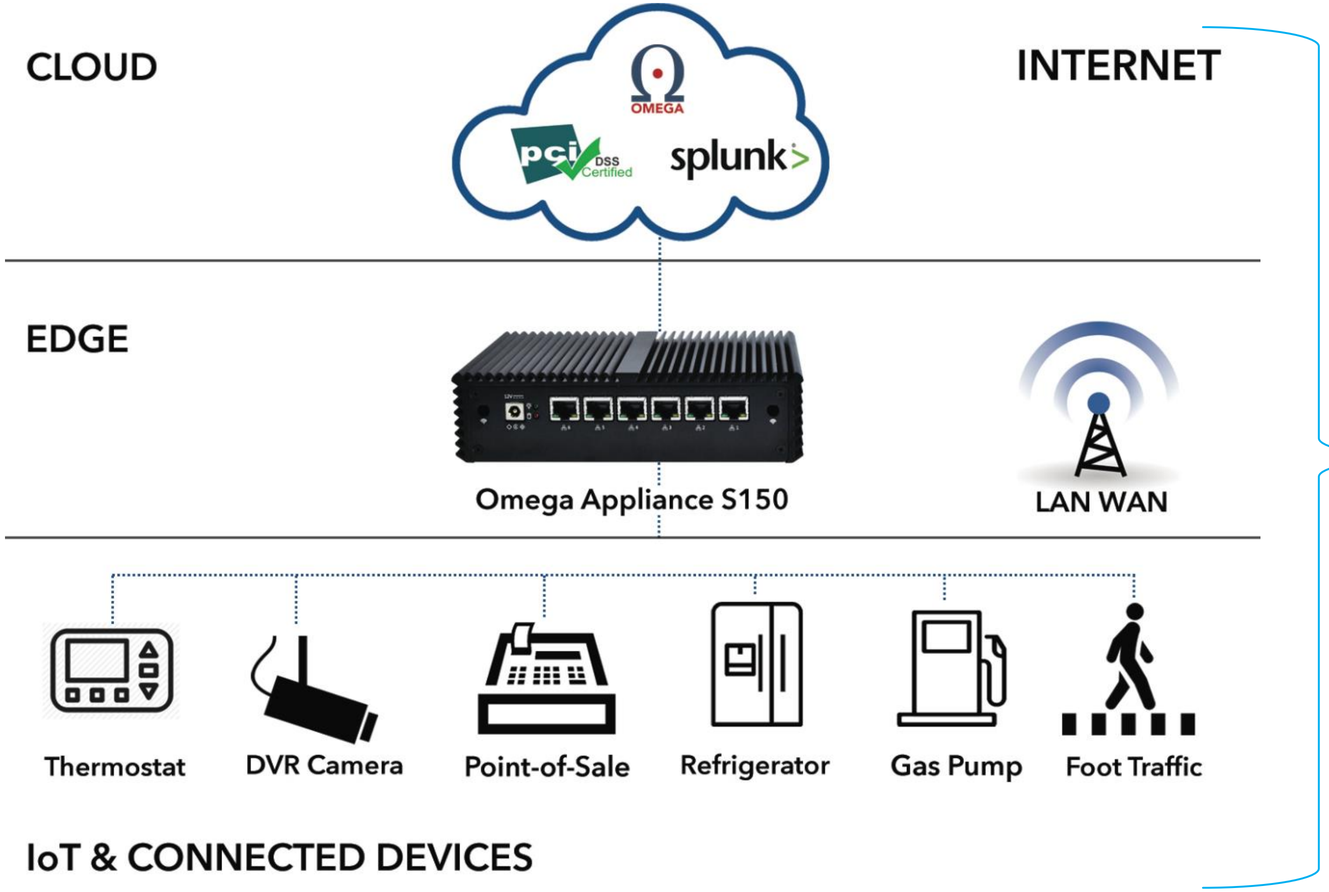
1. Collect data on any machine you can, via logging, SNMP, API integration, or any other method available.
2. Find ways to transform and parse data locally, at the "edge," before bringing it into the cloud.

Take a resilient approach to managing systems – visibility, prediction, rapid recovery, flexibility, automation.



Traditional Security Information and Event Management (SIEM) Data Flow

Take a resilient approach to managing systems – visibility, prediction, rapid recovery, flexibility, automation.



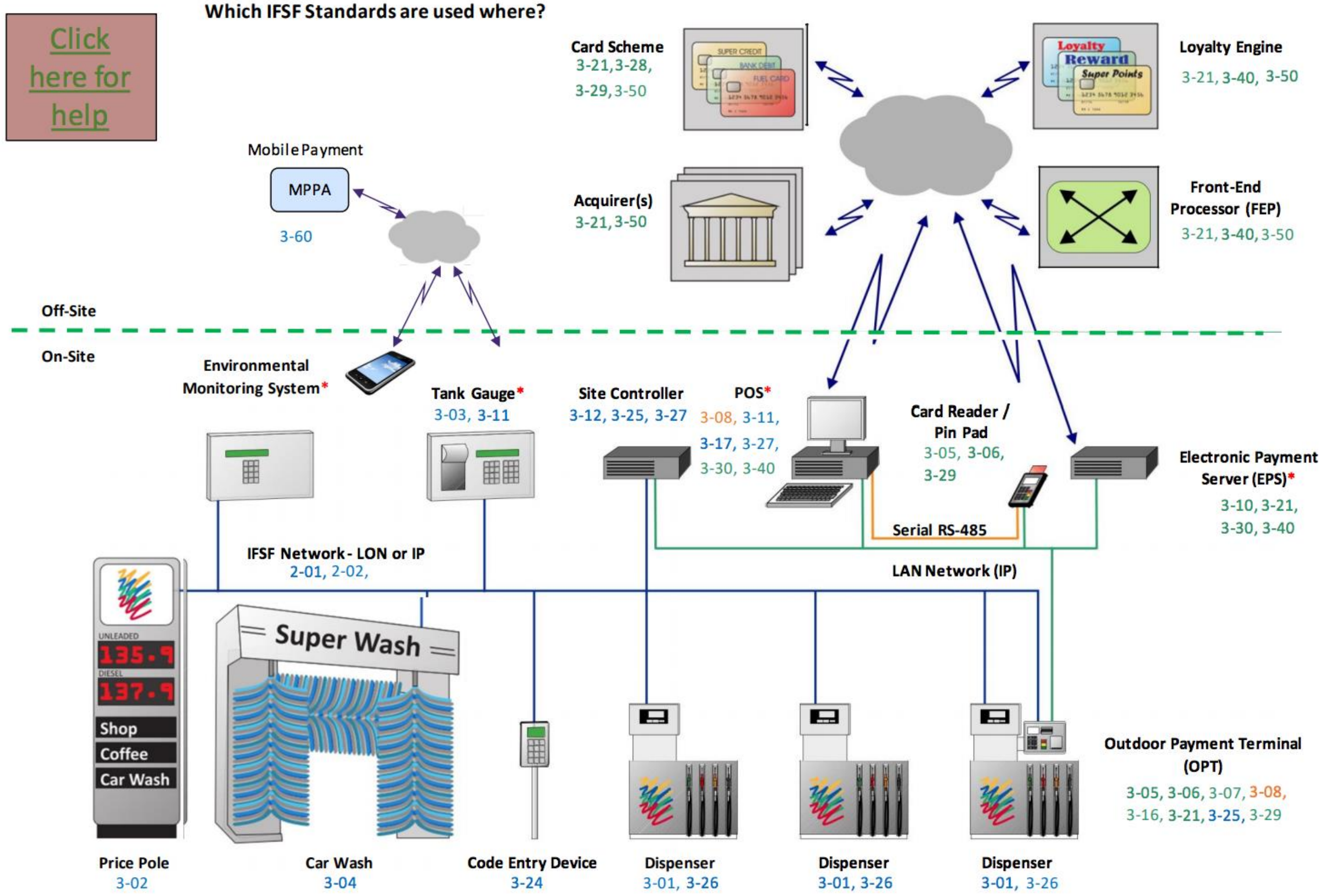
Security
+
Operational Data

Take a resilient approach to managing systems – visibility, prediction, rapid recovery, flexibility, automation.

Click here for help

INTERNATIONAL FORECOURT IFSF STANDARDS FORUM

CONEXXUS solve forward



Which IFSF Standards are used where?

Mobile Payment
MPPA
3-60

Card Scheme
3-21, 3-28,
3-29, 3-50

Acquirer(s)
3-21, 3-50

Loyalty Engine
3-21, 3-40, 3-50

Front-End Processor (FEP)
3-21, 3-40, 3-50

Off-Site

On-Site

Environmental Monitoring System*

Tank Gauge*
3-03, 3-11

Site Controller
3-12, 3-25, 3-27

POS*
3-08, 3-11,
3-17, 3-27,
3-30, 3-40

Card Reader / Pin Pad
3-05, 3-06,
3-29

Serial RS-485

Electronic Payment Server (EPS)*
3-10, 3-21,
3-30, 3-40

IFSF Network - LON or IP
2-01, 2-02,

LAN Network (IP)

Outdoor Payment Terminal (OPT)
3-05, 3-06, 3-07, 3-08,
3-16, 3-21, 3-25, 3-29

Price Pole
3-02

Car Wash
3-04

Code Entry Device
3-24

Dispenser
3-01, 3-26

Dispenser
3-01, 3-26

Dispenser
3-01, 3-26

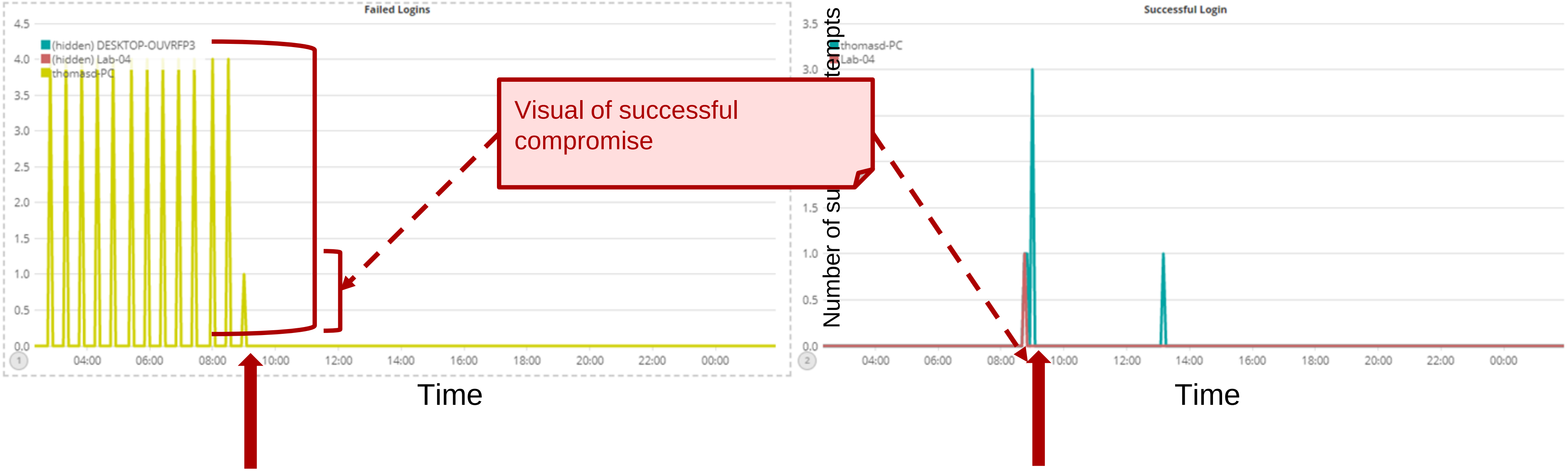
Take a resilient approach to managing systems – visibility, prediction, rapid recovery, flexibility, automation.

1. Outdoor EMV will make pumps IP connected.
2. Though increasing scope, it may also provide the ability to collect logs for improving operations and security.
    1. Door opens and closes
    2. System malfunctions
    3. Running out of receipt paper
    4. Filter replacement?
3. Use exploratory data analysis -- visual and otherwise -- to see what insights can be found from existing data feeds.

Take a resilient approach to managing systems – visibility, prediction, rapid recovery, flexibility, automation.

Time	Firewall	POS	Back Office	EPC
01:00:00	FW Event A	POS Event A	BO Event A	EPC Event A
01:01:00	FW Event B	POS Event B	BO Event A	EPC Event B
01:02:00	FW Event C	POS Event A	BO Event B	EPC Event C
01:03:00	FW Event D	POS Event C	BO Event C	EPC Event D

Take a resilient approach to managing systems – visibility, prediction, rapid recovery, flexibility, automation.



Visual of successful compromise

Take a resilient approach to managing systems – visibility, prediction, rapid recovery, flexibility, automation.

X = multiple login attempts over regular time intervals in 2 or more machines with a sudden stoppage in login attempts after 1 successful login

Y = specific pattern of file change activity

- A pair of X and Y, (X1,Y1), should be assigned a higher probability and fall into the queue as a higher priority alert. This ensures that more likely signs of malicious behavior are being addressed first.
- Whereas the specific pattern of file change activity may represent only a 5% chance of being a sign of malicious behavior, the conditions of X AND Y being met could represent a 33% chance of malicious activity.

Take a resilient approach to managing systems – visibility, prediction, rapid recovery, flexibility, automation.

Time	Firewall	POS	Back Office	Conversion Rate
01:00:00	FW Event A	POS Event A	BO Event A	49%
02:00:00	FW Event B	POS Event B	BO Event A	63%
03:00:00	FW Event C	POS Event A	BO Event B	20%
04:00:00	FW Event D	POS Event C	BO Event C	18%

Outage, maintenance, security incident, etc.

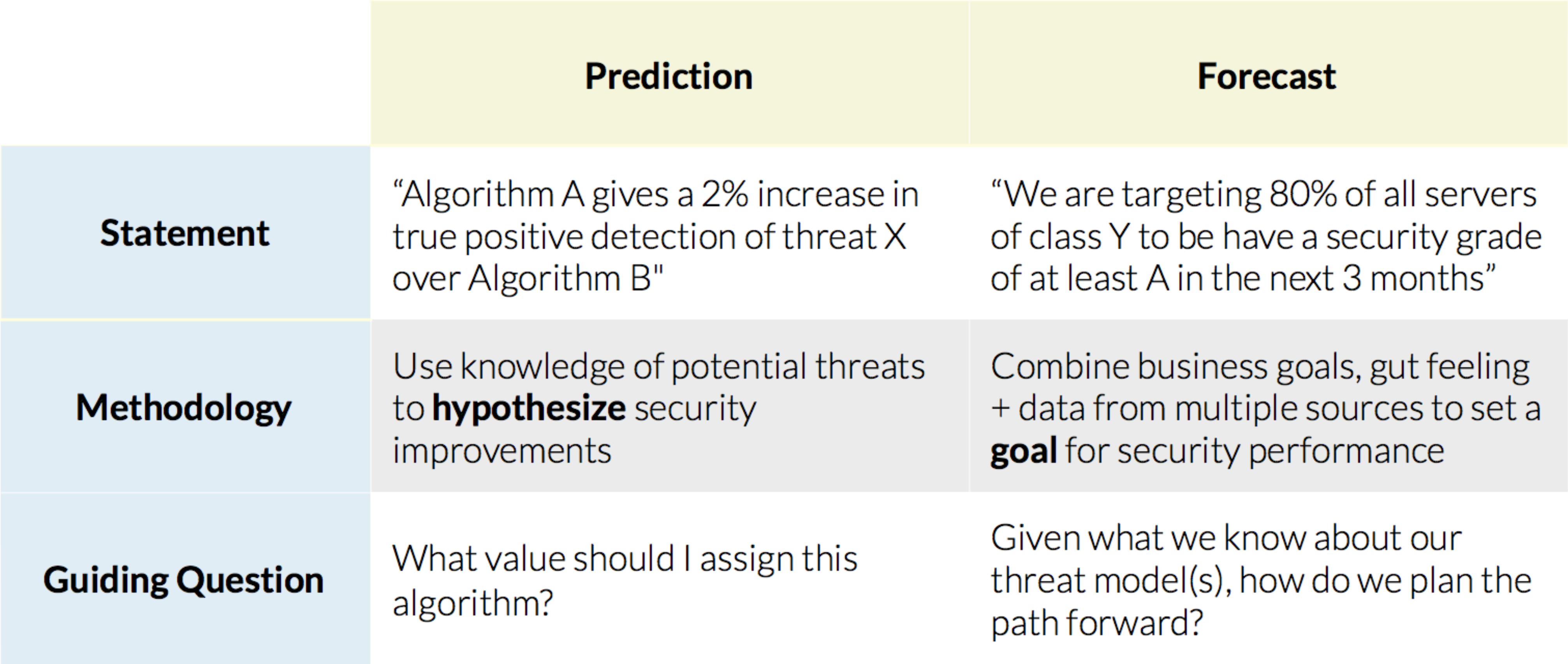
Business impact.

Take a resilient approach to managing systems – visibility, prediction, rapid recovery, flexibility, automation.

- A prediction is a definitive and specific statement about when and where an earthquake will strike: a major earthquake will hit Kyoto, Japan, on June 28.
- Whereas a forecast is a probabilistic statement, usually over a longer time scale: there is a 60 percent chance of an earthquake in Southern California over the next thirty years.

Nate Silver, *The Signal and the Noise*

Take a resilient approach to managing systems – visibility, prediction, rapid recovery, flexibility, automation.



	Prediction	Forecast
Statement	"Algorithm A gives a 2% increase in true positive detection of threat X over Algorithm B"	"We are targeting 80% of all servers of class Y to be have a security grade of at least A in the next 3 months"
Methodology	Use knowledge of potential threats to **hypothesize** security improvements	Combine business goals, gut feeling + data from multiple sources to set a **goal** for security performance
Guiding Question	What value should I assign this algorithm?	Given what we know about our threat model(s), how do we plan the path forward?

Source: Conor Nash, NBS Consulting

Take a resilient approach to managing systems – visibility, prediction, rapid recovery, flexibility, automation.

1. Consider methods for implementing “self-healing” through active monitoring of Pinnacle endpoints.
   1. POS application failures – if services stop, employ methods to “auto restart.”
   2. Monitor Windows firewall auto-starting and causing issues.

Take a resilient approach to managing systems – visibility, prediction, rapid recovery, flexibility, automation.

1. Example: monitoring of Palm.exe and Pharoh.exe.
    1. Omega has a monitor for each of these services; if one fails, the services auto-start. If the service continues to fail, an alert is generated.
2. Example: Windows Firewall.
    1. If one machine has incorrect settings, it will automatically reset back to company standard.
3. Visual exploratory data analysis
    1. Create dashboards that allow you to easily eyeball abnormal behavior.

Take a resilient approach to managing systems – visibility, prediction, rapid recovery, flexibility, automation.

1. Take advantage of any existing platform that can help reduce PCI scope.
2. Example: schedule file transfers.
    1. Price book changes, Employee Files (names, ID, etc..), PJR (POS Journal) Files (Information on transaction data) can be sent between PO and Back Office securely via a “middle man” on a scheduled basis.

Take a resilient approach to managing systems – visibility, prediction, rapid recovery, flexibility, automation.

1. For widespread ransomware attacks, deploy "vaccines" or "kill switches" whenever they are available.

Take a resilient approach to managing systems – visibility, prediction, rapid recovery, flexibility, automation.

1. Example: NotPetya ransomware would search for a local file and exit encryption routine if file already existed on disk.
    1. NotPetya “vaccine” consisted of creating a file on PCs, setting it to “read-only.”
    2. Upon learning of NotPetya vaccine process, Omega deployed file across all endpoints (“perfc in the C:\Windows folder) for each Pinnacle POS in the card data environment.

Overview -- security and IT operations should not be managed separately.

1. Take a resilient approach to managing systems – visibility, prediction, rapid recovery, flexibility, automation.
2. Collect data on all devices in the environment to ensure overall operational health, locally or in the cloud.
3. Automate whatever you can so you can focus on convenience!

Tools are widely available to help you get started working with data.

data
iku

alteryx

LogRhythm™

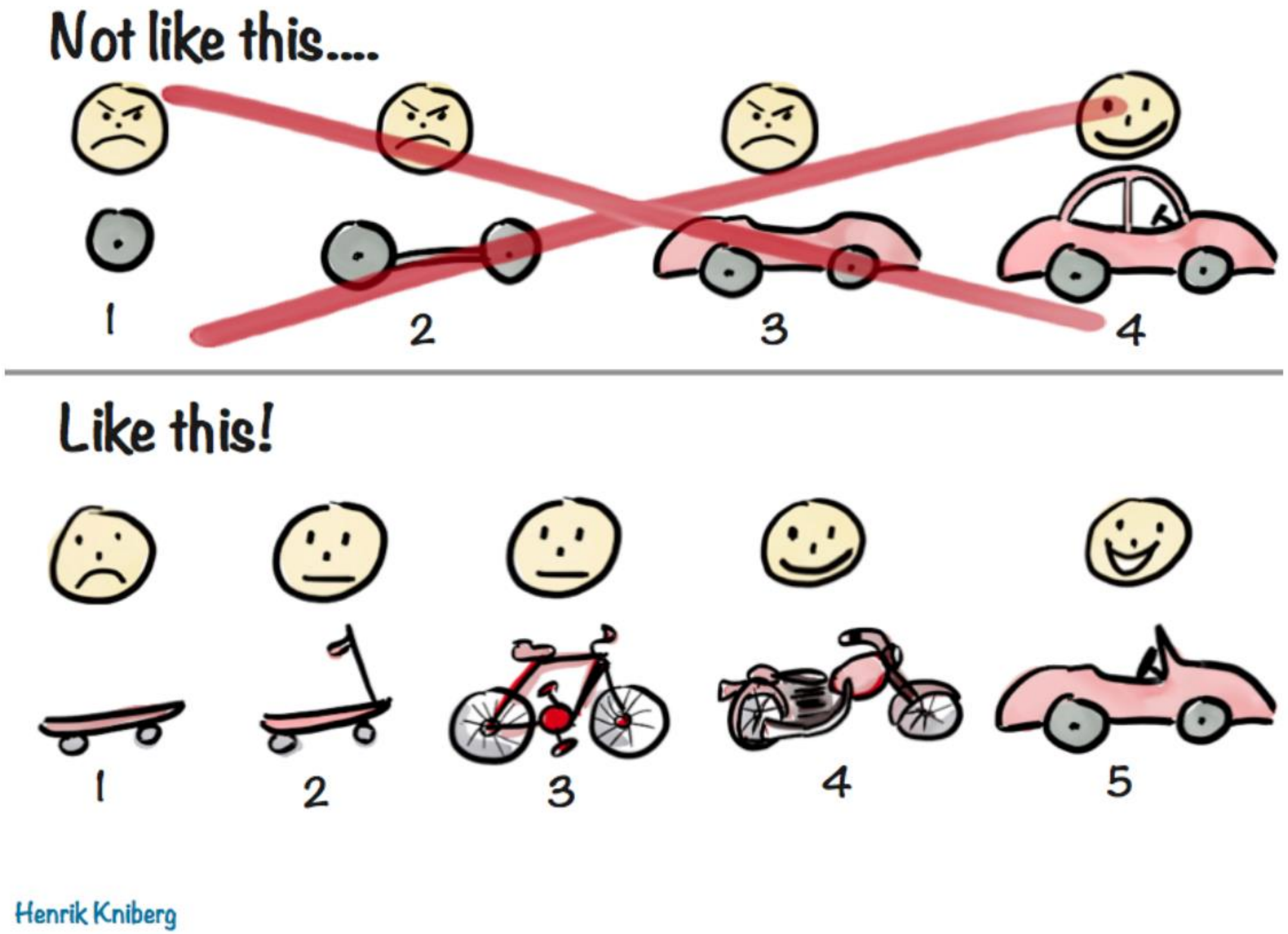
elastic

ALIEN VAULT

splunk>

graylog

What does progress look like?



Thank You!

Any Questions?