DRAGOS

WEBINAR

A Real-World Roadmap for Continuous Cybersecurity Improvement: Amgen's Story

October 27, 2022 @ 2 pm EST

AMGEN

PANELISTS

Darren Lensky
Principal OT Security Architect, Amgen

David Pessoa
Principal OT Security Engineer, Amgen

Jose Giboyeaux
Principal IS Architect, Amgen

AMGEN

Digital, Technology & Innovation

GOAL: INCREASE AMGEN’S RESILIENCE TO A *NOTPETYA*-STYLE CYBER ATTACK AND AN ISOLATION TYPE OF EVENT

OCT 2022

DAVID PESSOA → DARREN LENSKY → JOSE GIBOYEAUX

AGENDA

- Historical Perspective
- Themes for Security Projects
- IT/OT differences
- Why Dragos?
- Dragos Solutions
- Sustaining Resilience
- How to Scale Governance

HOW WE GOT HERE

NotPetya started spreading in the Ukraine on June 27, 2017. It spread worldwide soon after.

The ransomware used different vectors to spread: Server Message Block (SMB) Protocol; Collection of Password on Local Machine; MeDoc Update Server

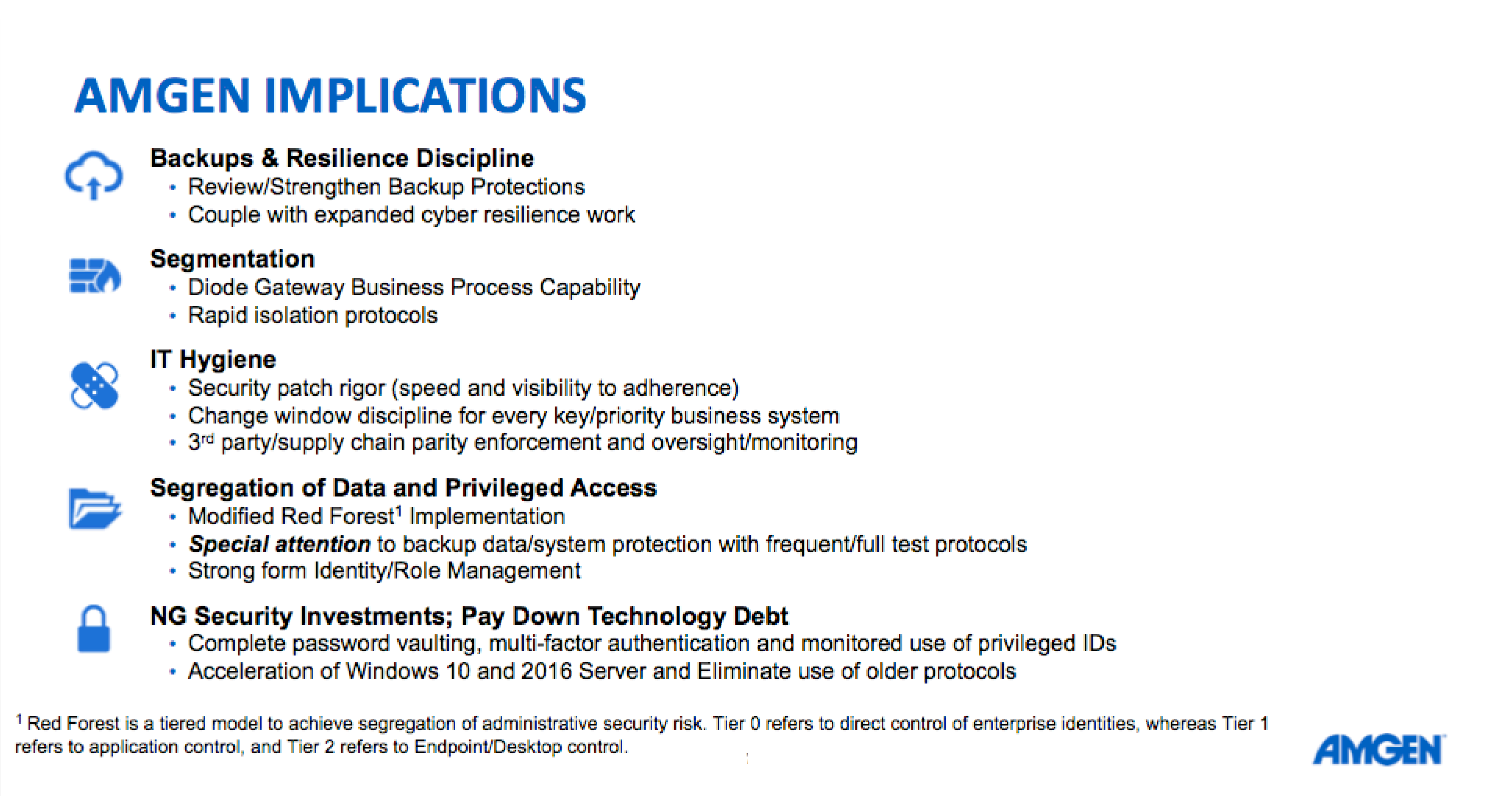
NotPetya was built to destroy not extort; it was meant to spread fast and cause damage

NotPetya has been tested in a controlled environment:

- The malware creates certain files in the Windows directory
- The files will be created there only if elevated\admin privileges are present
- The malware will also attempt to install itself on other computers in the network using common windows administration tools that are packaged with the malware.
- The security tools present in our environment are able to block and prevent the spread of this version of the threat.

Hurricane Maria led to a long isolation event and the need for self sufficiency

Solution space breaks down into five themes



AMGEN IMPLICATIONS

Backups & Resilience Discipline
- Review/Strengthen Backup Protections
- Couple with expanded cyber resilience work

Segmentation
- Diode Gateway Business Process Capability
- Rapid isolation protocols

IT Hygiene
- Security patch rigor (speed and visibility to adherence)
- Change window discipline for every key/priority business system
- 3rd party/supply chain parity enforcement and oversight/monitoring

Segregation of Data and Privileged Access
- Modified Red Forest[1] Implementation
- ***Special attention*** to backup data/system protection with frequent/full test protocols
- Strong form Identity/Role Management

NG Security Investments; Pay Down Technology Debt
- Complete password vaulting, multi-factor authentication and monitored use of privileged IDs
- Acceleration of Windows 10 and 2016 Server and Eliminate use of older protocols

[1] Red Forest is a tiered model to achieve segregation of administrative security risk. Tier 0 refers to direct control of enterprise identities, whereas Tier 1 refers to application control, and Tier 2 refers to Endpoint/Desktop control.

Our Approach

Conduct three workshops

- Workshop A: Backups & Resilience Discipline
- Workshop B: Segmentation / Segregation of Data and Privileged Access
- Workshop C: IT Hygiene / IT Debt

Workshops Agenda:

- Confirm the Problem Statement and High-Level Work Description
- Confirm and Rank the Questions to Ask
- Estimate Cost and Effort to implement Ideas / Answers
- Build a Roadmap
- Obtain Sponsorship / Funding for the Roadmap
- Execute and Report Back

Our Workshops

Aug 29

7:30

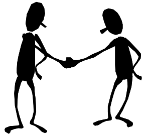
15’

How We Got Here

7:45

10’

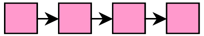
Ground Rules, Introductions, Roles, etc



7:55

25’

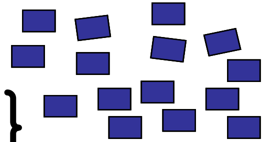
Understand Problem



8:20

10’

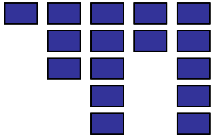
Brainstorm Questions



8:30

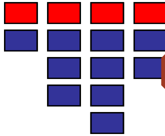
15’

Share with All



8:45

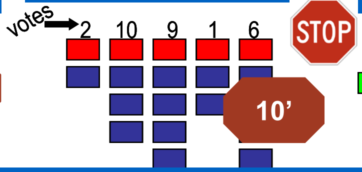
Define Sub-Categories



5’

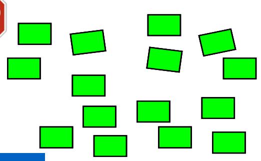
8:50

Prioritize within your group

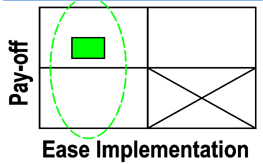


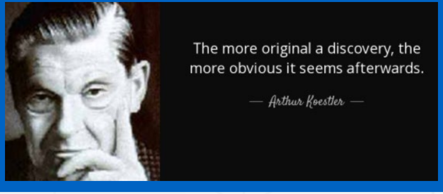
10’

Brainstorm Ideas / Answers



Assess Ideas and Develop Proposal(s) within your group





The more original a discovery, the more obvious it seems afterwards.

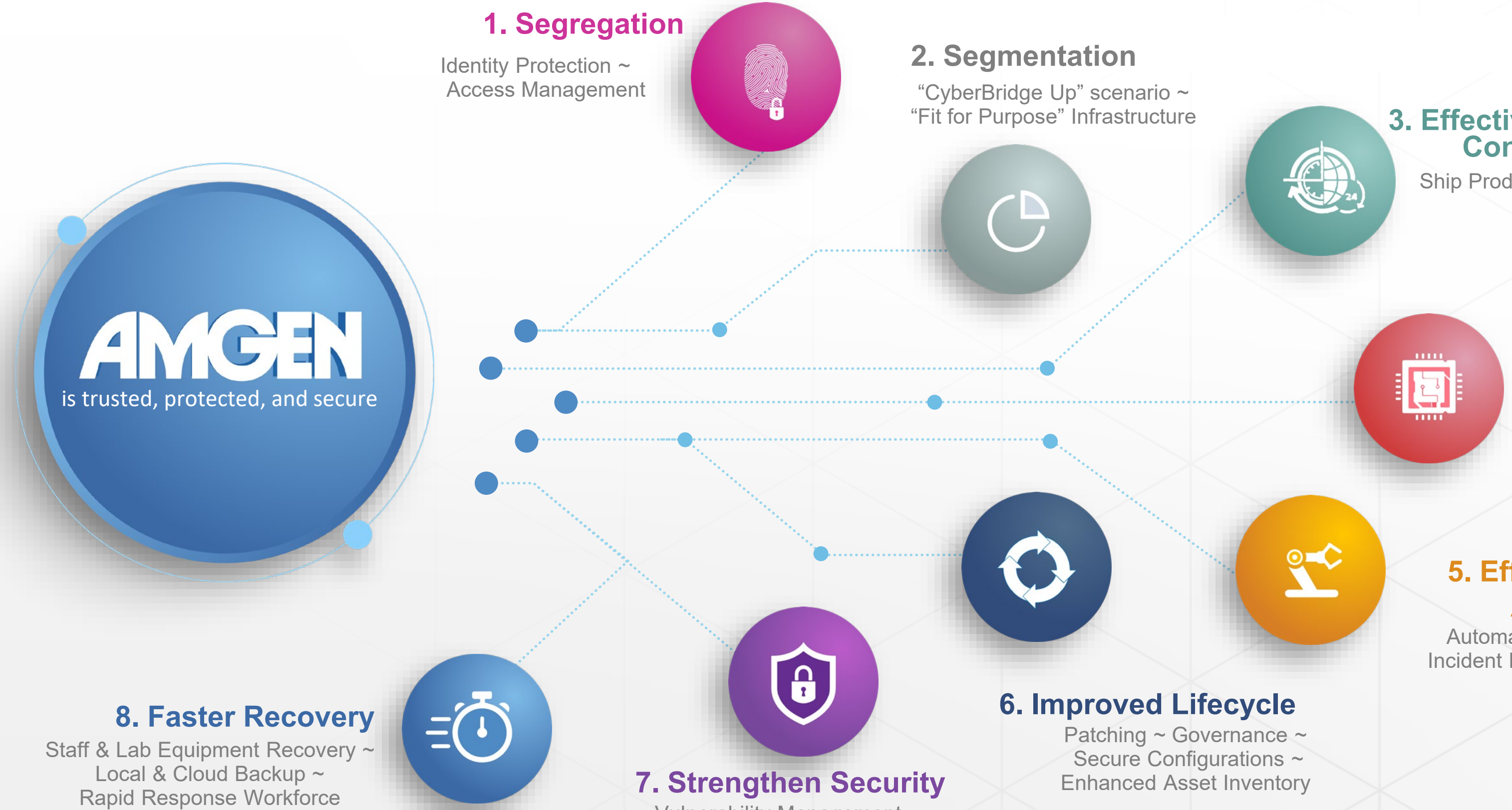
— Arthur Koestler —

Share with All

Sep 5

60’

Enterprise Cyber Resilience Program



AMGEN is trusted, protected, and secure

1. Segregation

Identity Protection ~
Access Management

2. Segmentation

“CyberBridge Up” scenario ~
“Fit for Purpose” Infrastructure

3. Effective Business Continuity

Ship Product Manually & Disposition

4. Resilient Technology

Data Protection ~ Site Resilience ~
Communication Availability ~
Infrastructure Modernization

5. Efficiency through Automation

Automated Rebuild ~ Patching ~
Incident Response ~ Access Review

6. Improved Lifecycle

Patching ~ Governance ~
Secure Configurations ~
Enhanced Asset Inventory

7. Strengthen Security

Vulnerability Management ~
Allowlisting ~ Penetration Testing ~
Threat Monitoring

8. Faster Recovery

Staff & Lab Equipment Recovery ~
Local & Cloud Backup ~
Rapid Response Workforce

AMGEN

Digital, Technology & Innovation

AN INSIDE LOOK FROM AN ARCHITECTURAL PERSPECTIVE

OCT 2022

DARREN LENSKY

PRINCIPAL IS ARCHITECT, AMGEN

AMGEN FACED WITH CHALLENGES

IT / OT Differences	CIA Model
	Different Technologies
	Different Processes
No Visibility	Network Telemetry
	Inconsistent deployment of Security Tooling
Shared Infrastructure	Limited Segmentation
	Weak Access Control
Timing Issues	Lack of downtime
	Planning for change management

KEY MILESTONES IN AMGEN'S JOURNEY

- Segmentation
- IR plan to focus on OT
- MFA
- OT Specific Visibility
- SafeListing Security Tooling
- Not just IT, Security, or Technology
- Lots of Powerpoint Slidedecks

AMGEN'S SUCCESS FACTORS | KEY TAKEAWAYS

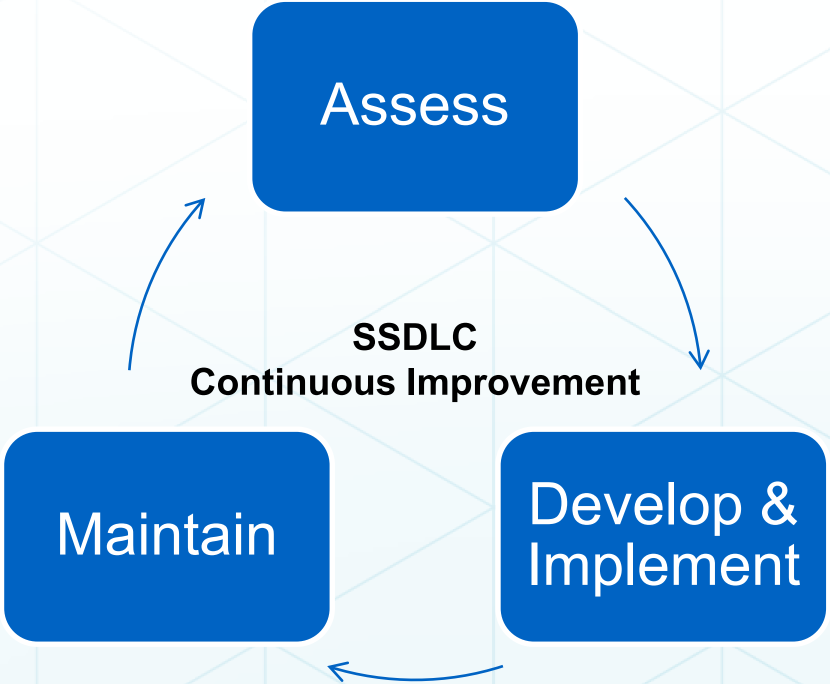
Top leadership support. Program and commitment to make this happen

Remember: THIS is the business

Goals: Security as a business enabler. We're there to protect Amgen's ability to manufacture, produce, and deliver product

WHY DRAGOS?

- Strategic Partner
- Leader in the space
- Professional Services
- Community Education
- Valuable insight to threats respective to OT



Digital, Technology & Innovation

ENTERPRISE CYBER RESILIENCY SUSTAINABILITY

OCT 2022

JOSE A GIBOYEAUX

PRINCIPAL IS ARCHITECT, AMGEN

LIFECYCLE MANAGEMENT FRAMEWORK

BACKGROUND

As part of the enterprise cyber resilience program, several security and resilience capabilities are being deployed to strengthen Amgen's manufacturing plants

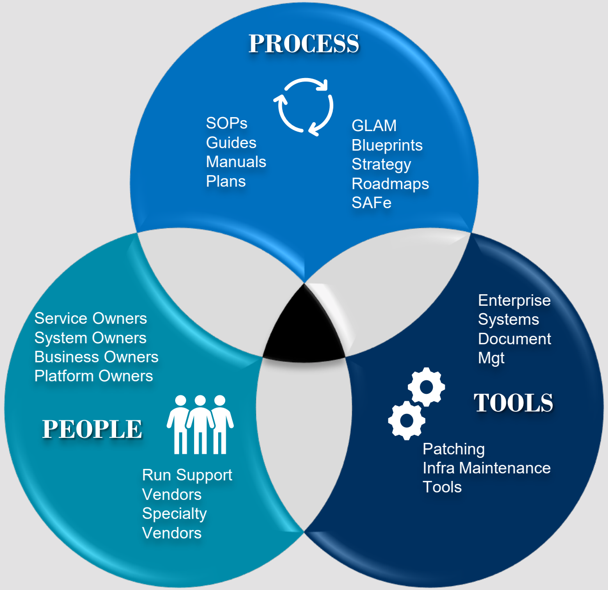
These capabilities need to be sustained in run state and follow lifecycle management activities

SOLUTION

To ensure sustainability for run state support, a comprehensive sustainability framework has to be developed that addresses all aspects for operational efficiencies

This framework is to be collectively managed by shared ownership between Site IS and other functions

ECR – Operations Sustainability Framework



PROCESS

SOPs
Guides
Manuals
Plans

GLAM
Blueprints
Strategy
Roadmaps
SAFe

PEOPLE

Service Owners
System Owners
Business Owners
Platform Owners

Run Support
Vendors
Specialty
Vendors

TOOLS

Enterprise
Systems
Document
Mgt

Patching
Infra Maintenance
Tools

SUSTAINABILITY PRINCIPLES

Governance

Corporate and site specific governance, resource & funding decisions

Strengthened Procedures

Lifecycle management, change control, configuration management

Audit & Accountability

Period access, security reviews, failover testing, RBAC reviews, & ownership

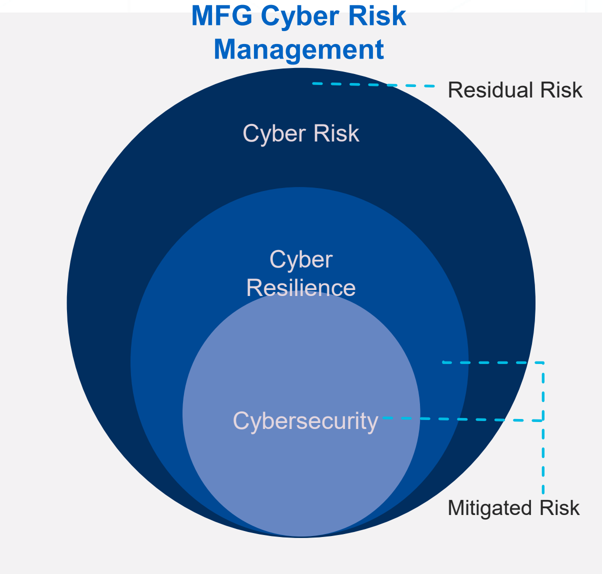
Integration

Manufacturing Framework, IS Blueprint, Digital Manufacturing & Platform Lifecycle

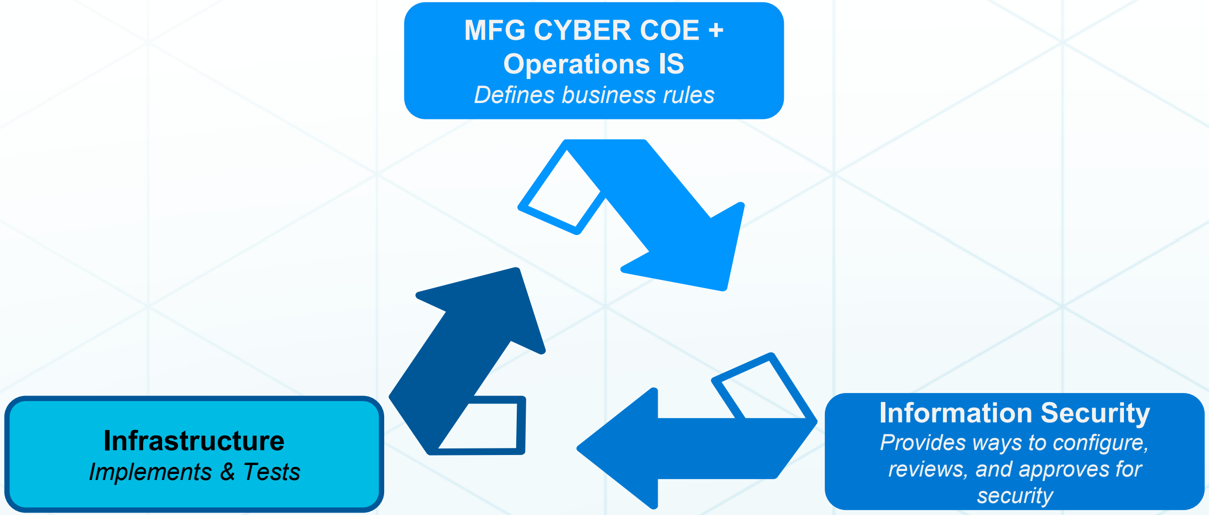
A robust sustainability framework for run state support results in operational efficiencies

MFG CYBER RESILIENCE SUSTAINMENT MODEL

Business Value

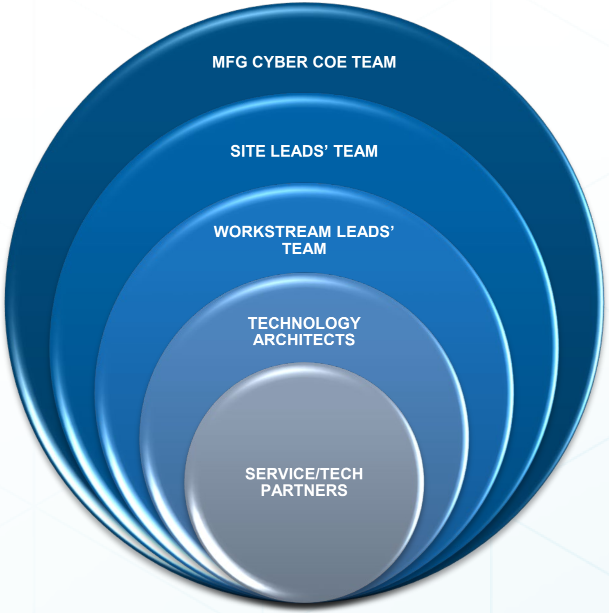


Operating Model


MFG CYBER COE + Operations IS
Defines business rules
Infrastructure
Implements & Tests
Information Security
Provides ways to configure, reviews, and approves for security

Operations IS, Information Security, Infrastructure collaborate closely to mitigate cyber risk to MFG

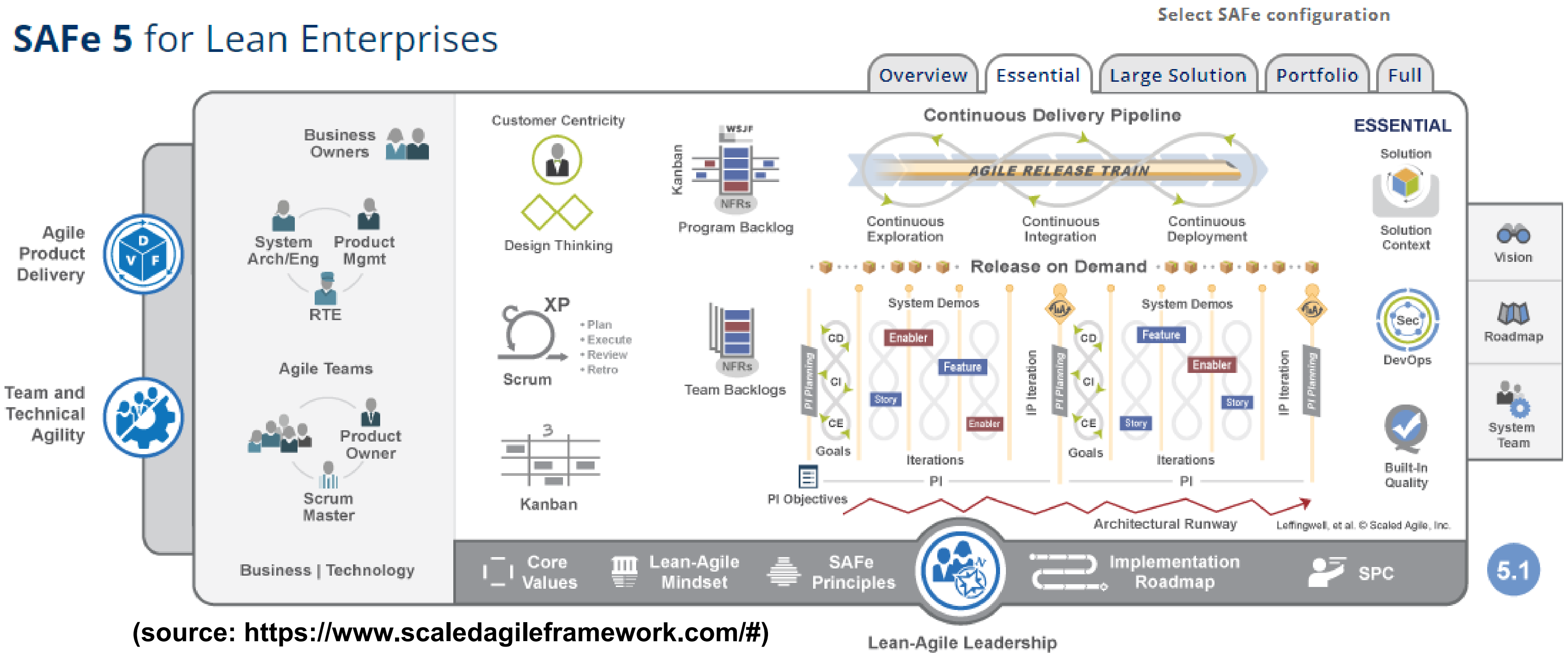
EXECUTION TEAMS



- MFG Cyber COE team is defined by workstreams to establish the security controls and sites for deployment.
- Functional leads & Service leads will provide guidance to workstream leads who will work with Site leads and MFG Cyber COE team for execution
- All activities are governed by MFG Cyber COE and Operations IS product team governance

If you want to go fast, go alone. If you want to go far, go together

MFG CYBER RESILIENCE BUSINESS VALUE DELIVERY FRAMEWORK

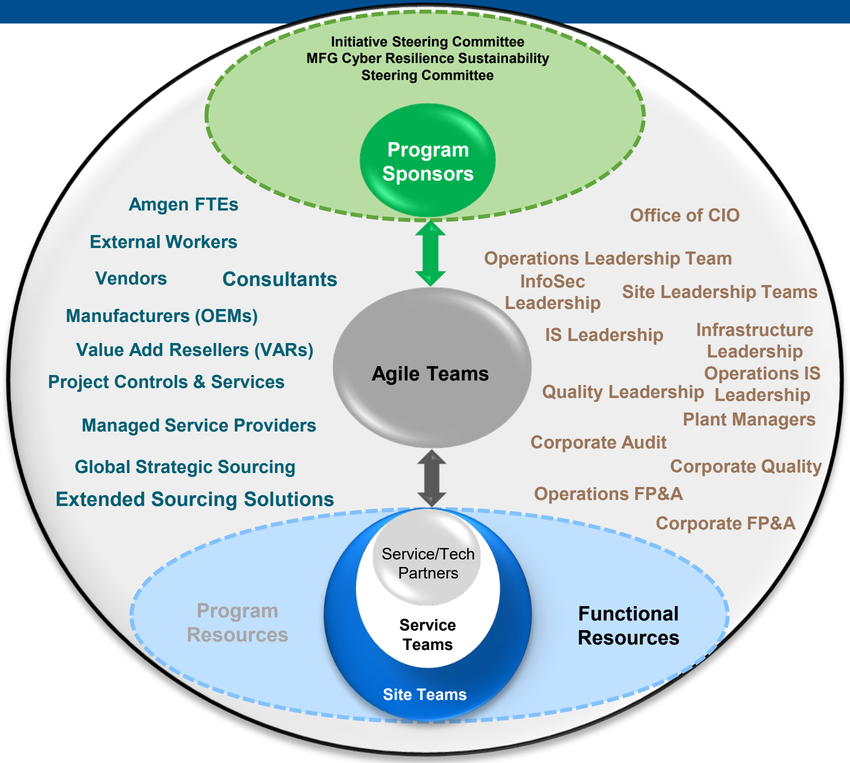


(source: https://www.scaledagileframework.com/#)

Agile Product Delivery Model

[*Scaled Agile Framework - Essential*](https://www.scaledagileframework.com/)

STAKEHOLDER LANDSCAPE



- A cohesive team with a common mission to execute the security and resilience controls for manufacturing systems
- Execution team includes resources from Operations IS, Information Security, Infrastructure, Site IS, Site Business, Service Providers, Technology Vendors, Finance, & Project Controls

ENSURE CONTINUOUS STAKEHOLDER ENGAGEMENT

WHAT IS THE SENTINELS PROGRAM?

- A long-term program to put information protection center stage and ensure staff understand their roles in protecting it

- A global community of Amgen staff creating a network of information protection: eyes and ears

- An integral part of the broader information protection initiative at Amgen

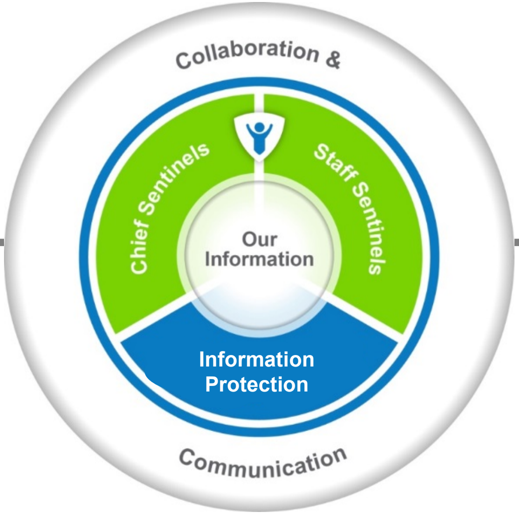
SENTINELS PROGRAM OVERVIEW

The Sentinels Program: *Staff outreach initiative; it's all about protecting our ability to serve patients.*

Our Goal: *Create a global community of staff from across the organization whose focus is to help raise local awareness about information threats and to encourage and demonstrate information protection best practices.*

Chief Sentinels

- Strategic partners with Information Protection
- Information security advocates and enthusiasts
- Thinking "global" but acting "local"
- No technical expertise required
- Instructor-led training



Staff Sentinels

- What we should all do every day as good corporate citizens:
  - ✓ Be alert
  - ✓ Detect & report issues
  - ✓ Advocate the use of information security best practices
- Annual "Security Education & Awareness Training (SEAT)"

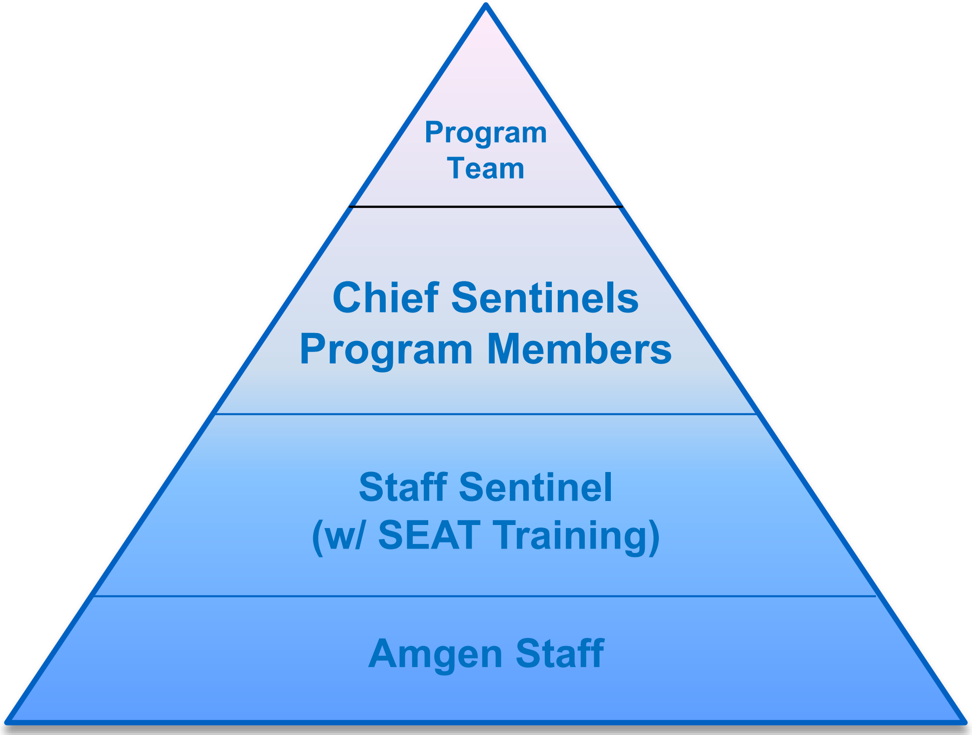
"Keep up the great work – if all companies were as progressive as Amgen, I'd have less work to do."

FBI Cyber Supervisor's comment on the Sentinels Program

AMGEN®

SENTINELS PROGRAM OVERVIEW

- **Program Team**
  - Limited Full-time/EW staff dedicated to Sentinels Program
- **Chief Sentinels (1,400+)**
  - Any staff, any function, any role
- **Amgen Staff/CWs ~38,000**
  - Mandatory Training: SEAT, Code of Conduct


Program Team
Chief Sentinels Program Members
Staff Sentinel (w/ SEAT Training)
Amgen Staff

Thank you!