waldemar .chlebik@siemens.com

# Key elements of Information Security Policy

## Information Security @ Siemens
## (Risk Management in modern organizations)

# Welcome to the Information Security Team

About us

**CoE ISEC** guides and drives InfoSec strategy, governance and execution Siemens-wide as defined by Siemens Chief Information Security Officer (CISO).

**Our Information Security Community**

- secures the biggest Active Directory service worldwide
- protects about 60 Global Data Centers, 120 Internet Access Points and over 400.000 end user devices
- remediates over 20.000 security vulnerabilities and incidents every year
- blocks over 850.000 malware emails (e.g. viruses) and 16 million spam mails every month

**Security Services steered by ISEC:**

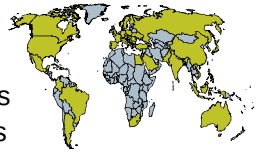
- Cyber Defense Centers (CDC)
- Vulnerability Management
- Computer Emergency Response Team (CERT, provided by CT RTC ITS)
- Corporate Security Training Service

**Security Services governed by ISEC**

- Identity Management
- Malware Protection
- Encryption
- Business Partner Access
- InfoSec Dash

**We are a global team and can leverage on know how and experience on a worldwide level**

- ~ 180 employees
  - AAE: ~25 employees
  - Americas: ~30 employees
  - Europe: ~ 125 employees



**Ongoing PR!O Program Activities**

- Rollout of global Cyber Defense Centers
- Implement risk focused governance model and re-aligned global community
- Execute Golden Nugget protection
- Enhance InfoSec Risk Management process / ACP
- Supplier Management for InfoSec
- Redesign and implement Vulnerability Management
- Design of Resource Islands
- …

**Major Regional InfoSec Projects**

- Enabling secure IT Infrastructure of the Future (IIoF), e.g. IT services in the cloud
- Piloting the protection for critical information by Data Leakage Prevention (DLP) services
- …

# Our Vision, Mission and Collaboration Principles

## Vision & Mission

The CoE Information Security drives the **strategy, governance and execution** for Siemens information Security (InfoSec) and IT Cyber Security **globally**.

We **collaborate** with IT Business Partner organizations (IT BP's) to gather and respond to business InfoSec demands, as well as to collaborate with IT Centers of Expertise (CoE's) in the implementation of InfoSec policies and solutions **to protect Siemens and its most critical assets.**

## Collaboration Principles

**We are One ISEC!**

Business Partners and CoEs have a single point of contact for all topics regarding Information Security!

We support the business to adequate protect their critical knowledge / information!

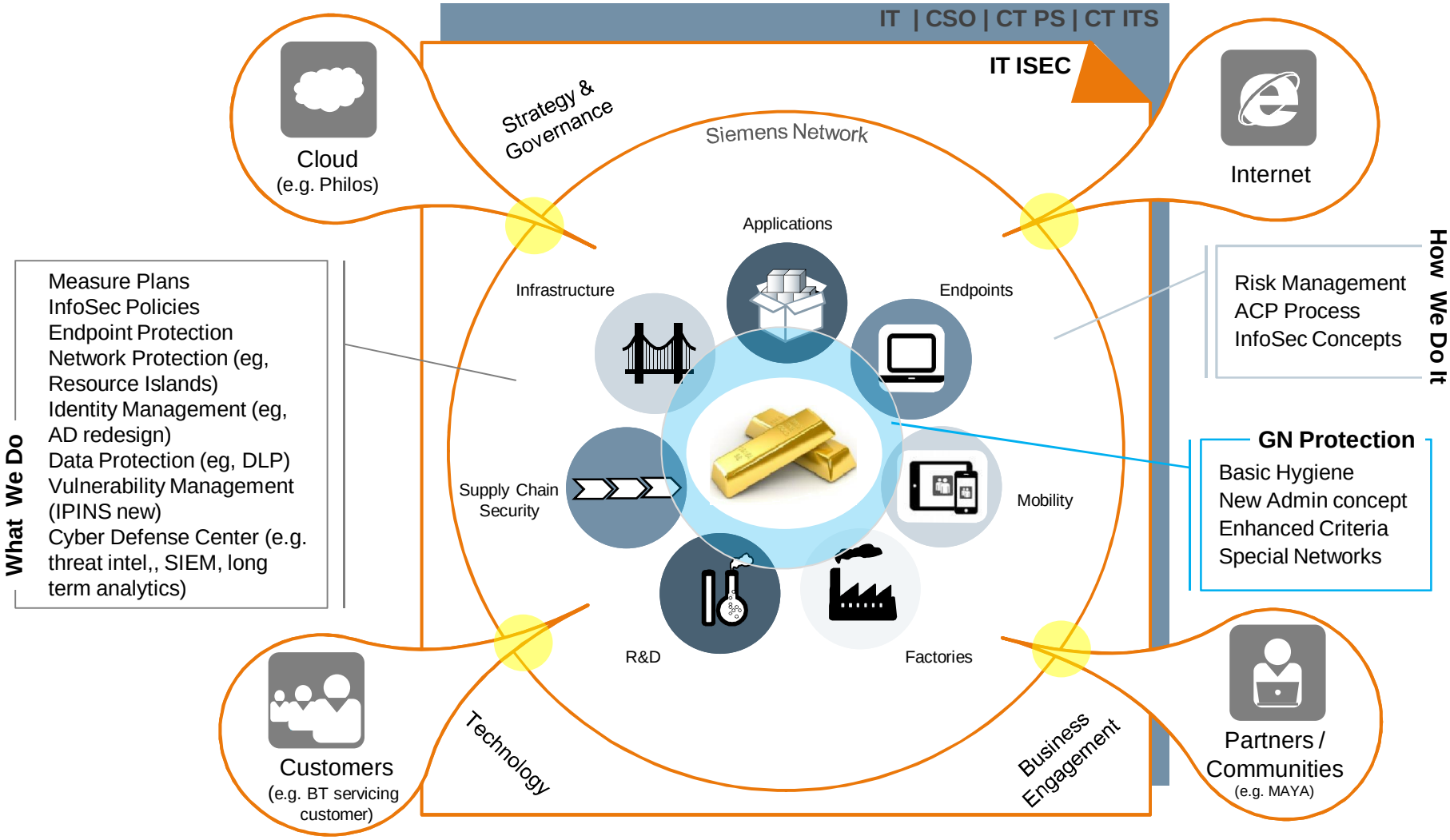
At Siemens, Siemens comes first!

We promote open, candid discussion and decision-making

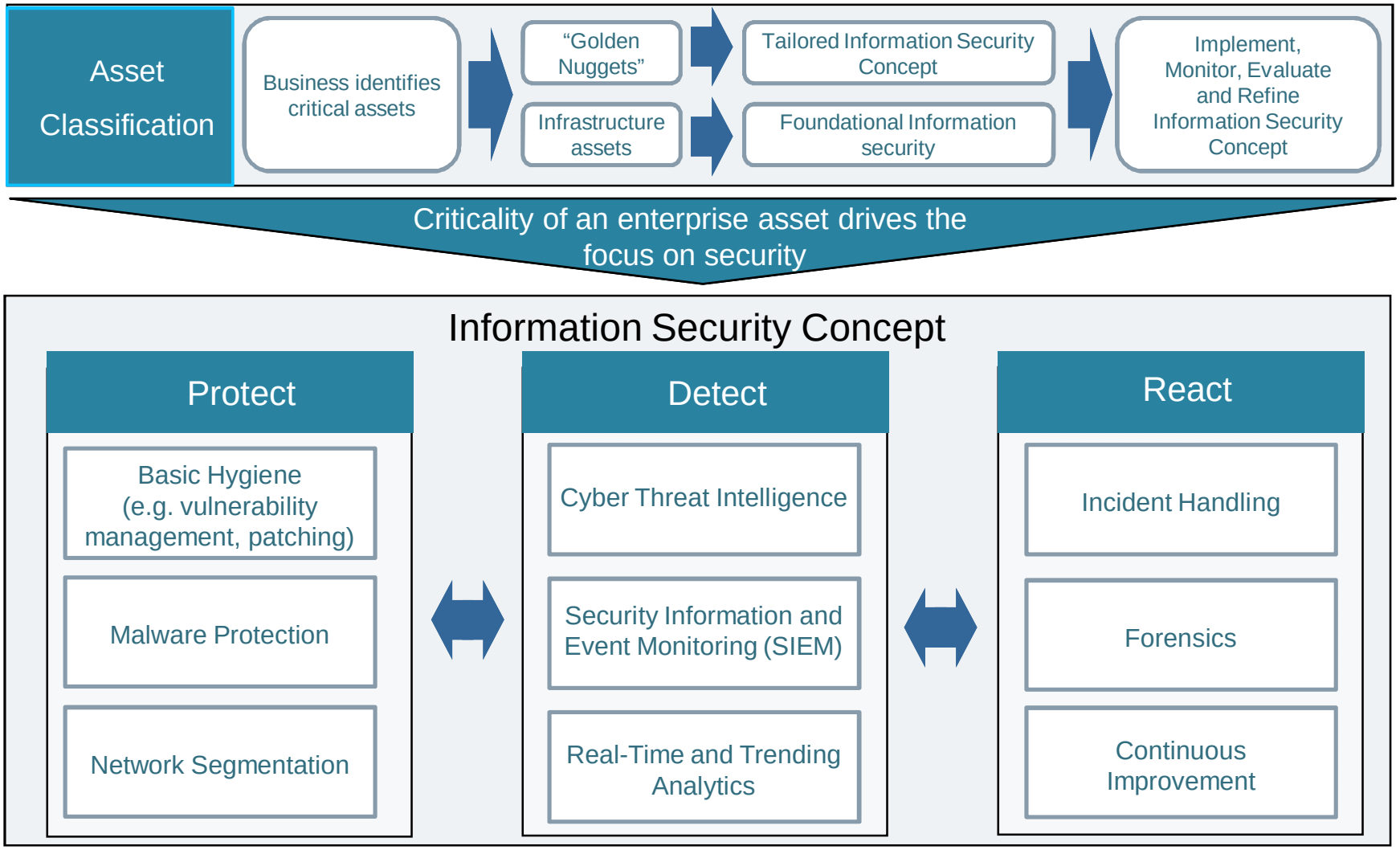
We are decisive, take moderate risks, take initiative, and are accountable

We reduce communication distortion at all levels

# Siemens InfoSec Ecosystem



# Big picture of Information Security






**IT creates business value**

# The foundation of Information Security@Siemens has already effective components *(Part 1)*

SIEMENS

## Siemens Public Key Infrastructure (PKI)

- Basis for secure communication and storage of confidential data and a precondition for trustworthy and secure transactions
- Data encryption, authentication, digital signature
- > 350.000 people equipped with PKI cards

## EAGLE - In-house high-security data center

- Highest security level
- High process maturity
- Proven organizational practices
- Carefully chosen employees
- High performance
- Regional extensions
- Flexibility & agility (e.g. Active Directory insourcing, “Geheimschutz”)

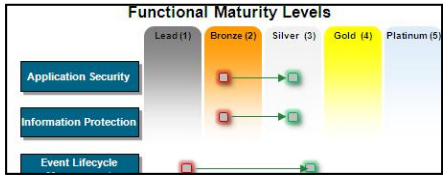
to operate Siemens’ ‘mission critical’ services globally

## Corporate Entitlement

- Provides web-based authentication for Siemens employees, external business partners and Siemens customers
- Efficiently protects approx. 600 web-based applications by using adequate authentication methods, e.g. strong 2-factor authentication (PKI) for critical applications

## AIR Program

- Initiated by the Managing Board (Tone from the Top)
- Business involvement in CEO workshops
- Outside-In Check (Booz Allen Hamilton maturity assessment) showed that InfoSec@Siemens is on the right way, but has to close some gaps







**IT creates business value**

# The foundation of Information Security@Siemens has already effective components *(Part 2)*

SIEMENS

## InfoSec Training

- Yearly web-based InfoSec training with approx. 300.000 users to raise and keep up awareness
- 10 InfoSec one pagers available - practical guidance on what needs to be observed in specific situations (e.g. social media, e-mail communication, mobile devices)
- Best practice awareness campaigns in several Sectors and Clusters


## SAP Single-Sign On

- Project initiated by the CIO Board in 02/2012 to significantly improve SAP security
- PKI login secures access through strong 2-factor authentication (PKI-login)
- Encryption of communication between SAP and environment
- Implementation completed in 09/2013

## Re-Insourcing of critical network services

- After critical events (AD, Netpro incidents) CIT decided to re-insource the crucial network services
  - Active Directory Forest Root
  - Central Administration Exchange
  - Top-level Domain Name Service

  into EAGLE
- Transition finished in 04/2013

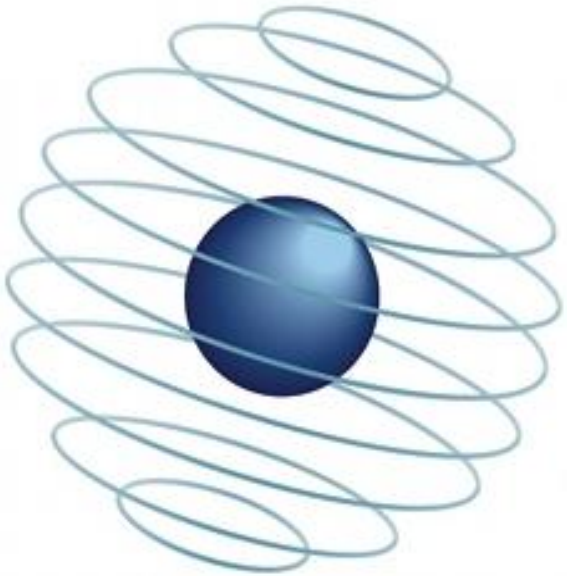
## PR!O Program

- 100% Protection is impossible, due to constantly changing threats and attacker capabilities. Therefore continous development of InfoSec is needed
- PR!O focuses on the most important topics to protect Siemens' critical assets




**IT creates business value**

SIEMENS

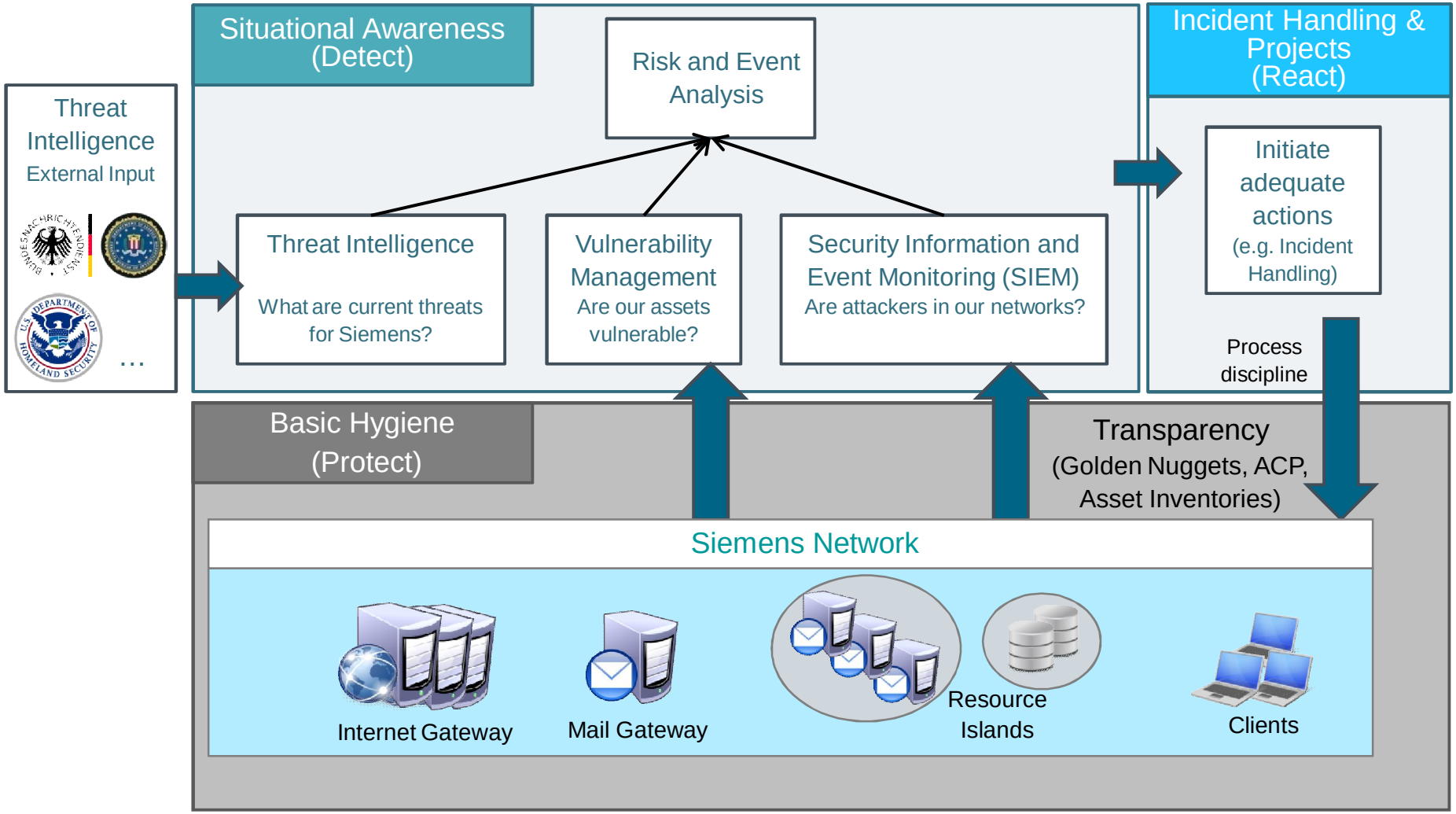


Cyber
Defense
Center

# Situational Awareness Cyber Defense Center

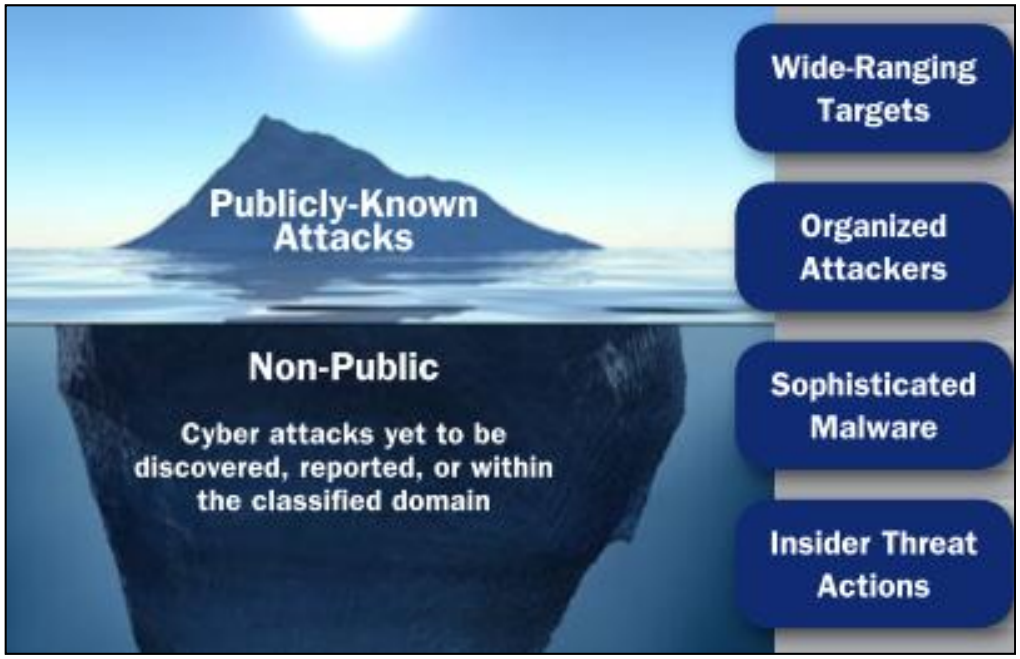
## Deep Dive

# Situational Awareness provides a comprehensive overview of the security state



# …. and the current InfoSec Threat landscape

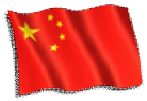
Viewpoint




## Threat Highlights

- Some is known
- A lot is unknown
- We must learn to operate in a compromised environment

**Energy Infrastructure Infiltration (Siemens software exploited)**
Russian attackers target grid operators, petroleum pipeline operators, electricity generation firms to steal data and potentially mount sabotage operations



**Supply Chain Intervention**
Chinese hackers poison inventory scanners at key worldwide logistics firms and extract shipment data ("ZombieZero")

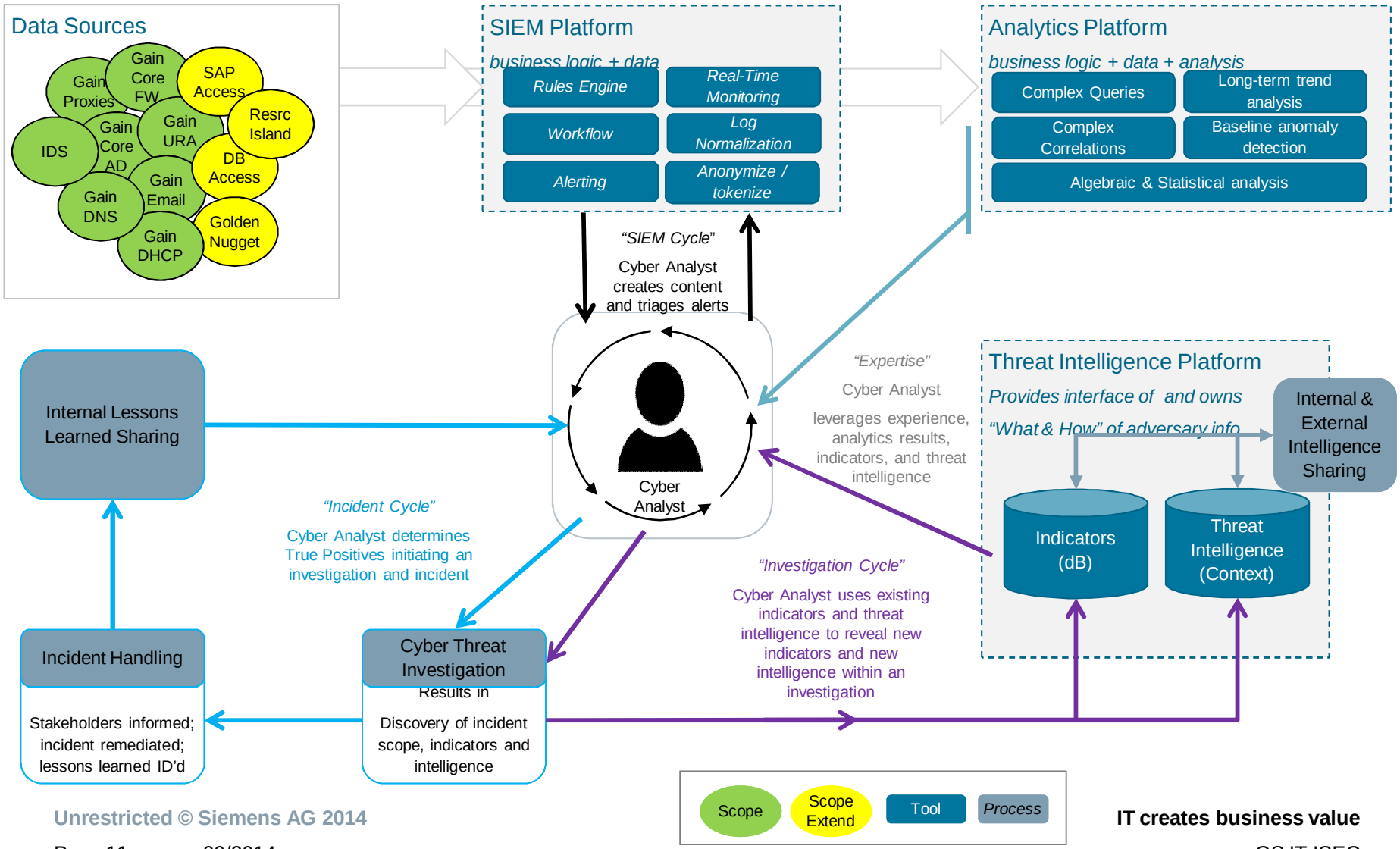

**SCADA and ICS systems Hacked**
California firm targeted by Havex, a remote access trojan, using watering hole tactics to maximize breach and install 88 variants of the malware



**IT creates business value**

# Technical & Operational

*Situational Awareness leverages robust processes, advanced tools, and experienced Cyber Analysts*



SIEMENS

# Thank you / Questions