EXCELIC INFOTECH

A Data Protection Company

Information Security For Manufacturing Industry

About Excelic

For some, the path to excellence is a steady march. For others, it unfolds through bursts of innovation. But for the best of the best, it’s both, disciplined improvement initiatives, marked by powerful leaps and breakthroughs. As the world’s largest professional services firm, we help organizations build value and excellence by uncovering insights that create new futures and doing the hard work to improve performance.

Excelic’s Profile - Overview

Excelic – specialist risk and compliance firm with expertise in IT risk management

Flexible “On Demand” Governance and Risk Consulting Services, Satellite presence in Middle East, India, Europe

Ex **Big 4 leadership** with combined 250+ years of professional services experience.

Risk and compliance expertise across industries, risk consulting services & operations; serving more than **100 clients across the globe**

15+ experts specialized in IT solutions with CISA, CISSP, ISO 27001, ISO 22301, OSCP certifications

15+

Seasoned Risk & Audit Professionals

10+

IT Risk Management Professionals

15+

Cyber Security Professionals

IT RISK MANAGEMENT TEAM

- Techno functional team to conduct application reviews.
- Pool of CISA, CISSP, CISM, OSCP, CEH, ISO27001 LA, CRISC and other relevant certified professionals
- Team with a good mix of industry and consultancy background
- Team with technical expertise in networks and infrastructure reviews
- Methodology aligned to the ISO 27001/ COBIT / ISF framework
- Large repository of technology risk and controls database
- Audit methodology and documentation practices aligned to the standards of international accounting bodies and industry best practices

A Snapshot of Our IT Risk Management Services

1 Cyber Risk and Security

- Cyber Risk Management
- Infra & App security assessments
- Enterprise security architecture review
- Secure SDLC review
- Identity & access management
- Cloud security and mobility security reviews

2 IT Governance and Compliance

- IT security policy & process review
- IT GRC (tools) review
- HITRUST, HIPAA, NIST, ISO alignment
- Data Governance
- GDPR & CCPA, SOX, SSAE16, PCI requirments

3 IT Risk Management

- ITRM framework design & rollout
- Third party InfoSec Reviews
- BCP & DR planning & implementation
- Software Asset Management

4 Forensic Investigation

- Evidence Acquisition
- Evidence Analysis
- Legal Documentation
- Forensic Data Reporting
- Legal Certification
- Court Depositions

5 Corporate fraud Prevention

- Know your Employees
- Company Data Protection Policy
- Review IT Security Policies
- Data Protection Process
- Data Governance
- Legal Framework

Mitigating Risk In the Manufacturing Sector

As manufacturing becomes increasingly digitized and data-driven, manufacturers will find themselves at serious risk. The complexities of multi-organizational dependencies and data management in modern supply chains mean that vulnerabilities are multiplying. Unfortunately, manufacturers in general do not see themselves to be at particular risk. This lack of recognition of the threat may represent the greatest risk of cybersecurity failure for manufacturers

Cybersecurity for the manufacturing supply chain is a particularly serious need. Manufacturing supply chains are connected, integrated, and interdependent; security of the entire supply chain depends on security at the local factory level. Increasing digitization in manufacturing— especially with the rise of Digital Manufacturing, Smart Manufacturing, the Smart Factory, and Industry 4.0, combined with broader market trends such as the Internet of Things (IoT)— exponentially increases connectedness. At the same time, the diversity of manufacturers—from large, sophisticated corporations to small job shops—creates weakest-link vulnerabilities.

The scale and variety of cyber-threats to manufacturers have grown considerably in recent years, and now range from rare and sophisticated attacks to relatively frequent ransomware risks. They often include efforts to corrupt data, steal intellectual property (IP), sabotage equipment, and disable networks. The purposes and effects of attacks vary widely, but all such incidents cost time and money to industrial firms and their customers

The Threat Landscape for Manufacturing

To manage cyber risks appropriately organizations must set risk appetite, and drive focus on what matters. Our Cyber Risk Management framework starts by understanding who might attack, why, and how.

Who might attack?

- Cyber criminals
- Hactivists (agenda driven)
- State Sponsored hackers
- Insiders / partners
- Competitors
- Skilled individual hackers
- Rogue Organizations

What are they after, and what are the key business risks I need to mitigate?

- Sabotage operations, processes and output
- Alter data and Product Designs
- Steal Trade Secrets
- Extortion
- Damage to Network and IT systems
- Cyber Espionage or IP theft
- Destroy Production Equipment or compromise it enough that output is unstable.

What tactics might they use?

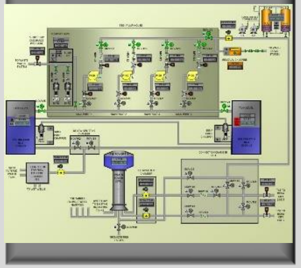
- Software or hardware vulnerabilities
- Third party compromise
- Multi-channel attacks
- Phishing and Stolen Credentials
- Business Email Compromise (BEC)
- Malware or Ransomware
- Insider Threats
- Target Infrastructure Grids like Power and Water

What enables these attacks

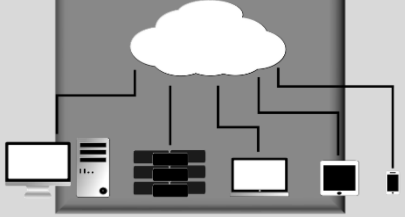
Unique Nature of CPS

Vulnerable ICS

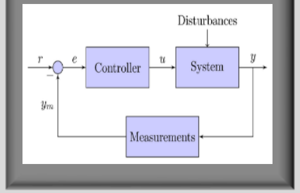
Vulnerable SCADA systems



Networked Machine, Sensors and Data

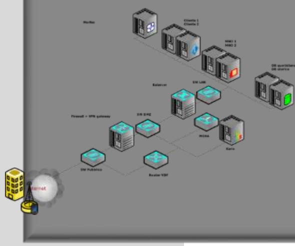


Software based controls and Monitoring

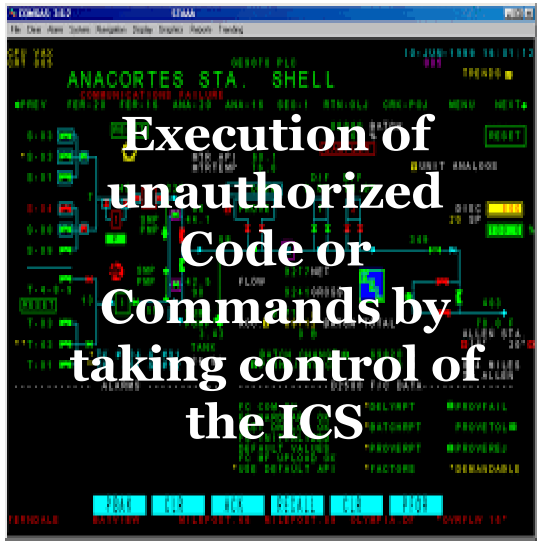


Unauthorized Access and Control

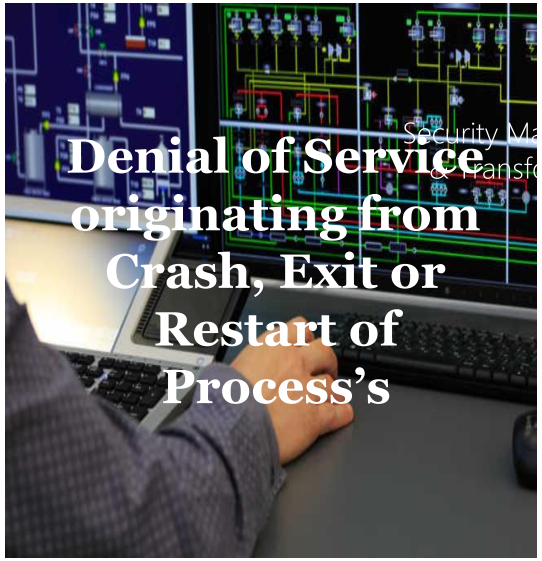
OEMs demand minimal safeguards



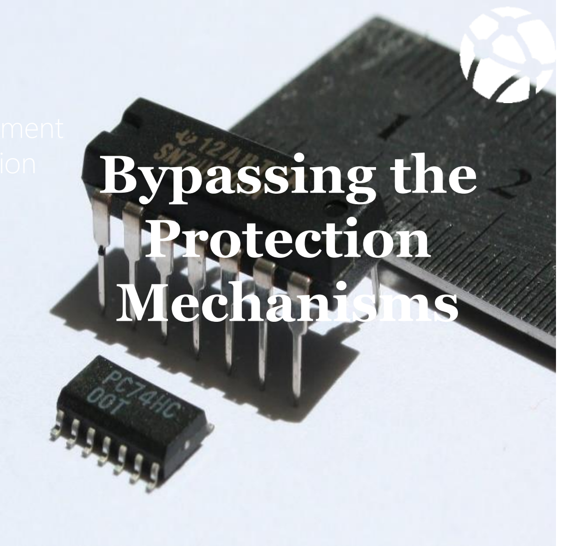
Impact of the Cyber Attacks



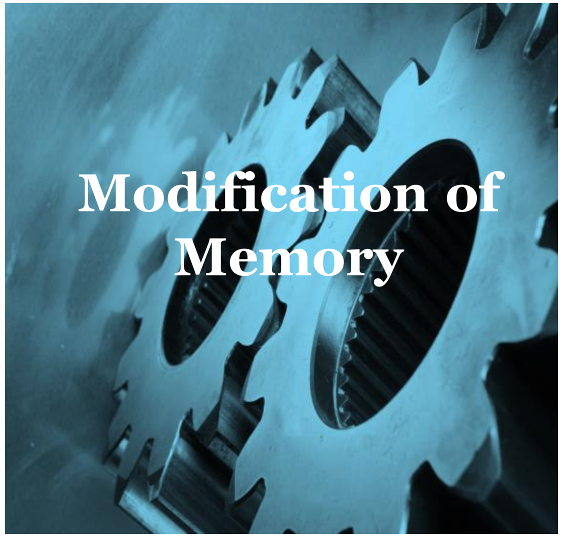
Execution of unauthorized Code or Commands by taking control of the ICS



Denial of Service originating from Crash, Exit or Restart of Process's

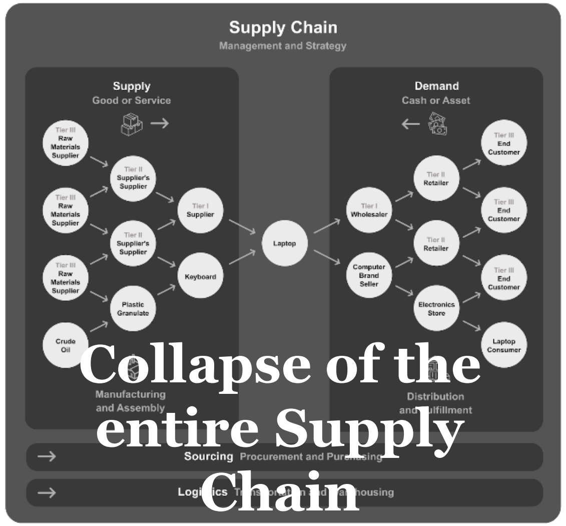


Bypassing the Protection Mechanisms



Modification of Memory

Reading of Application Data



Collapse of the entire Supply Chain

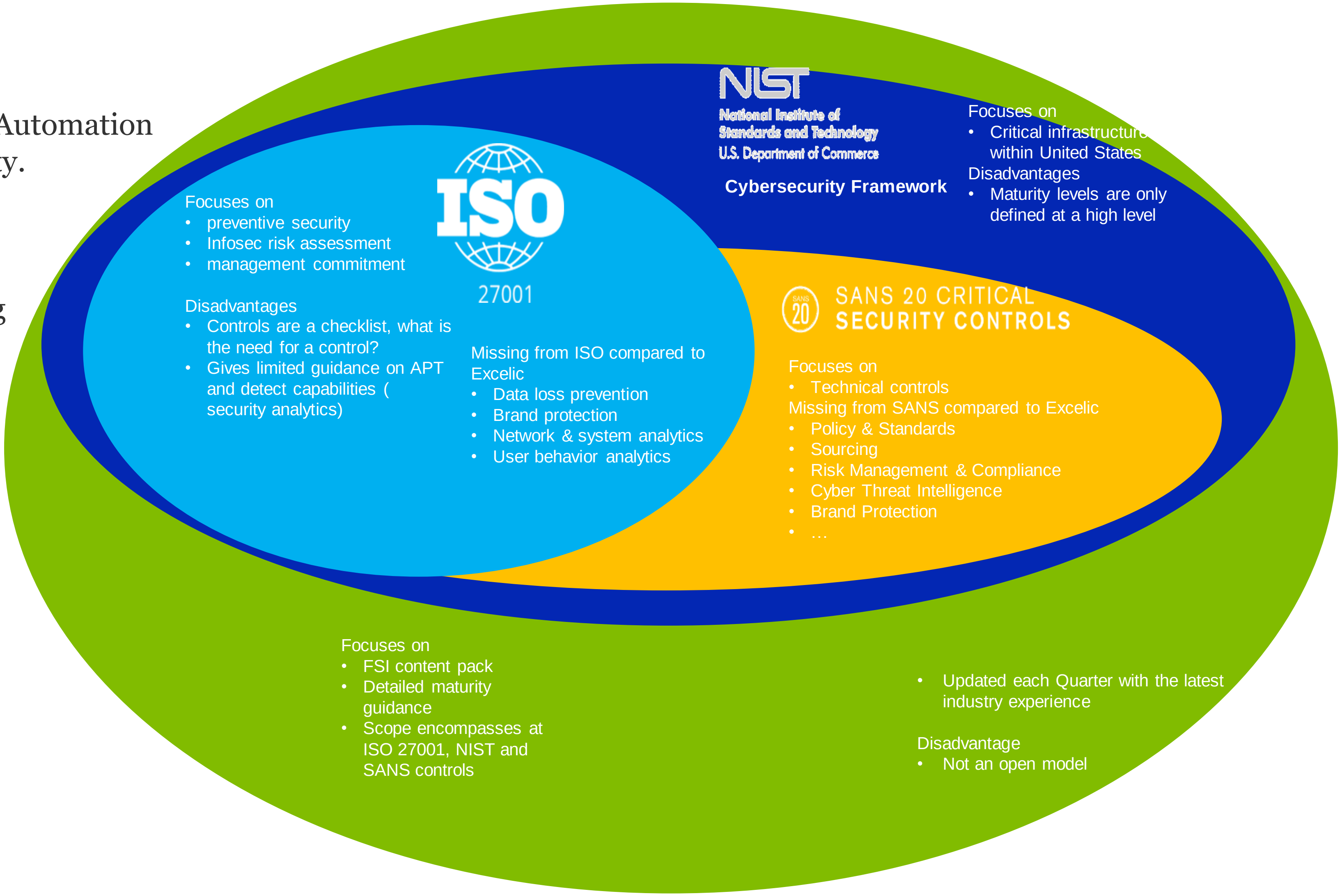
Supply Chain
Management and Strategy
Supply
Good or Service
Demand
Cash or Asset
Laptop
Keyboard
Manufacturing and Assembly
Distribution and Fulfillment
Sourcing Procurement and Purchasing
Logistics Transportation and Warehousing

Loss of Production even for a few days can lead to Millions in loss and customer trust

Compliance in Manufacturing

❖ The ISA/IEC 62443 to Secure your Industrial Automation and Control Systems with IEC 62443 cybersecurity.

❖ *ISO/IEC 27001* is an internationally recognized standard for reducing security risks and protecting information systems.



ISO 27001

Focuses on
- preventive security
- Infosec risk assessment
- management commitment

Disadvantages
- Controls are a checklist, what is the need for a control?
- Gives limited guidance on APT and detect capabilities (security analytics)

Missing from ISO compared to Excelic
- Data loss prevention
- Brand protection
- Network & system analytics
- User behavior analytics

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Cybersecurity Framework

Focuses on
- Critical infrastructure within United States

Disadvantages
- Maturity levels are only defined at a high level

SANS 20 CRITICAL SECURITY CONTROLS

Focuses on
- Technical controls

Missing from SANS compared to Excelic
- Policy & Standards
- Sourcing
- Risk Management & Compliance
- Cyber Threat Intelligence
- Brand Protection
- …

Focuses on
- FSI content pack
- Detailed maturity guidance
- Scope encompasses at ISO 27001, NIST and SANS controls

- Updated each Quarter with the latest industry experience

Disadvantage
- Not an open model

Cyber Risk Case Studies

Fischer Advanced Composite Components AG (FACC) – BEC Attack

Who

an aeronautics company in Austria, and a major designer and manufacturer of aircraft components and systems, with a client base that includes Boeing, Airbus, Rolls-Royce, Siemens SAS and Mitsubishi Heavy Industries.

Impact

Classic example of a type of BEC known as 'CEO Fraud' where fraudsters pretend to be high-level executives. Using email content that can appear legitimate and create a sense of urgency, they instruct the recipient—typically an employee that handles the company's finances—to conduct a wire transfer to a bank account they control. And contrary to usual phishing attacks that are emailed en masse, BEC scams are socially engineered and more targeted to avoid being detected as spam

What Happened

The incident occurred last January and involved a fake email that impersonated its then CEO Walter Stephan, conning one of FACC's financial department employee into wiring 50 million euros that was supposedly for one of the company's acquisition projects.

FACC, realizing that they were tricked, adopted countermeasures and was able to stop the transfer of 10.9 million euros on the recipient accounts. The rest of the money, however, has already disappeared in Slovakia and Asia

Cyber Risk Case Studies

Honda Motor – Ransomware Attack

Who

leading Japanese manufacturer of motorcycles and a major producer of automobiles for the world market. Headquarters are in Tokyo

Impact

It halted production at a domestic vehicle plant for a day this week after finding the WannaCry ransomware that struck globally last month in its computer network.

What Happened

Honda discovered on Sunday that the Wannacry virus had affected networks across Japan, North America, Europe, China and other regions. Despite efforts to secure its systems in mid-May when the virus caused widespread disruption at plants, hospitals and shops worldwide. The ransomware crypto worm , which targeted computers running the Microsoft Windows Operating System by encrypting data and demanding ransom payments in the Bitcoin Cryptocurrency.

The automaker shut production on Monday at its Sayama plant, northwest of Tokyo, which produces models including the Accord sedan, Odyssey Minivan and Step Wagon compact multipurpose vehicle and has a daily output of around 1,000 vehicles

Cyber Risk Case Studies

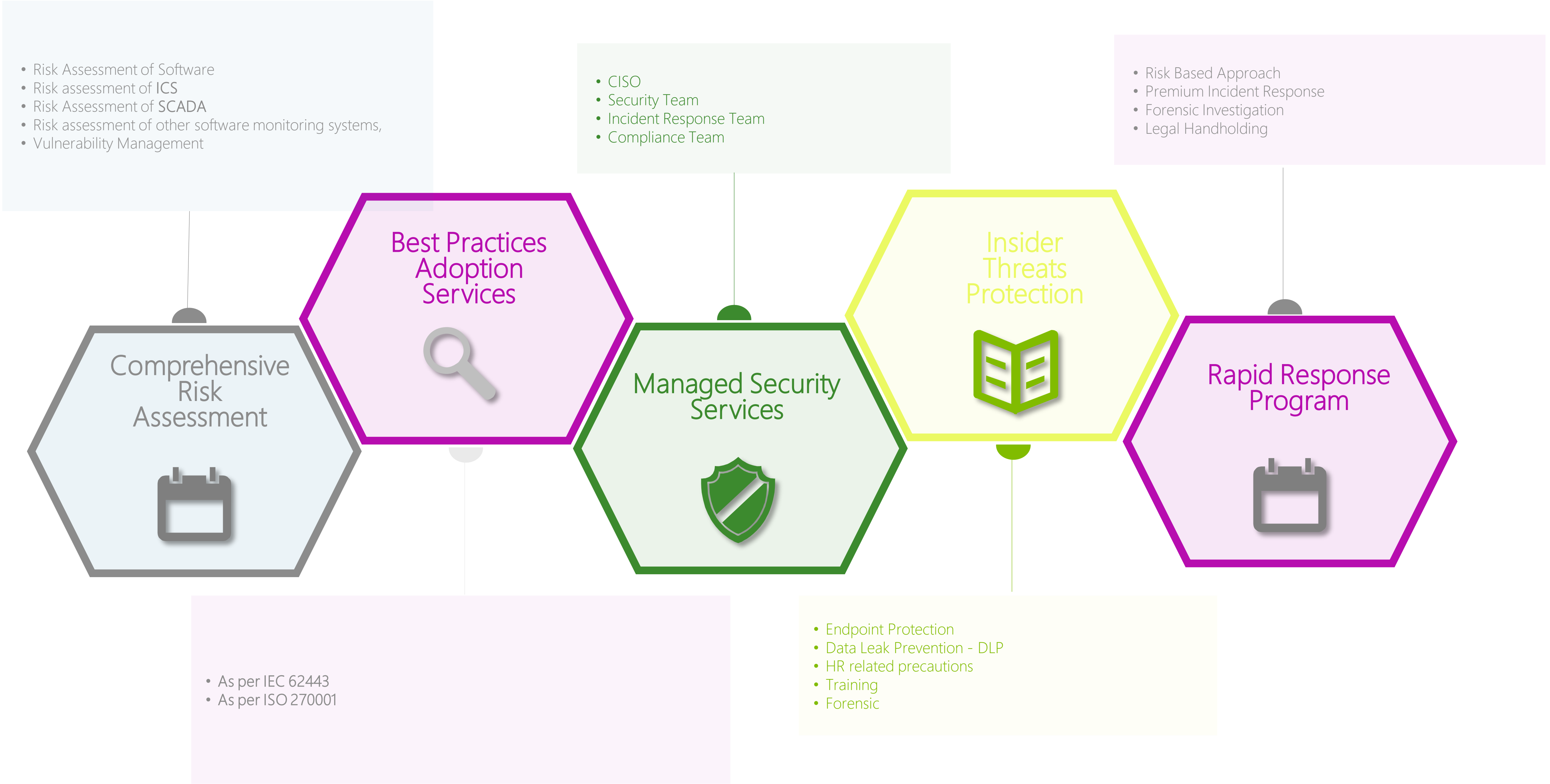
Iranian Nuclear Facilities – Stuxnet Attack

The Stuxnet Worm first emerged during the summer of 2010. Stuxnet was a 500-kilobyte computer worm that infiltrated numerous computer systems. [1] This virus operated in three steps. First, it analyzed and targeted Windows networks and computer systems. The worm, having infiltrated these machines, began to continually replicate itself. Next, the machine infiltrated the Windows-based Siemens Step7 software. This Siemens software system was and continues to be prevalent in industrial computing networks, such as nuclear enrichment facilities. Lastly, by compromising the Step7 software, the worm gained access to the industrial program logic controllers. This final step gave the worm's creators access to crucial industrial information as well as giving them the ability to operate various machinery at the individual industrial sites. The replication process previously discussed is what made the worm so prevalent. It was so invasive that if a USB was plugged into an effected system, the worm would infiltrate the USB device and spread to any subsequent computing systems that the USB was plugged in to.

Impact

Over fifteen Iranian facilities were attacked and infiltrated by the Stuxnet worm. The attack was initiated by a random worker's USB drive in the Natanz nuclear facility. Inspectors from the International Atomic Energy Agency visited the Natanz facility and observed that a strange number of uranium enriching centrifuges were breaking. The cause of these failures was unknown at the time. Later, Iran technicians contracted computer security specialists in Belarus to examine their computer systems. This security firm eventually discovered multiple malicious files on the Iranian computer systems. It has subsequently revealed that these malicious files were the Stuxnet worm. It is estimated that the Stuxnet worm destroyed 984 uranium enriching centrifuges. This constituted a 30% decrease in enrichment efficiency.

Excelic Solutions for Cyber Safe Manufacturing



Comprehensive Risk Assessment

- Risk Assessment of Software
- Risk assessment of ICS
- Risk Assessment of SCADA
- Risk assessment of other software monitoring systems,
- Vulnerability Management

Best Practices Adoption Services

- As per IEC 62443
- As per ISO 270001

Managed Security Services

- CISO
- Security Team
- Incident Response Team
- Compliance Team

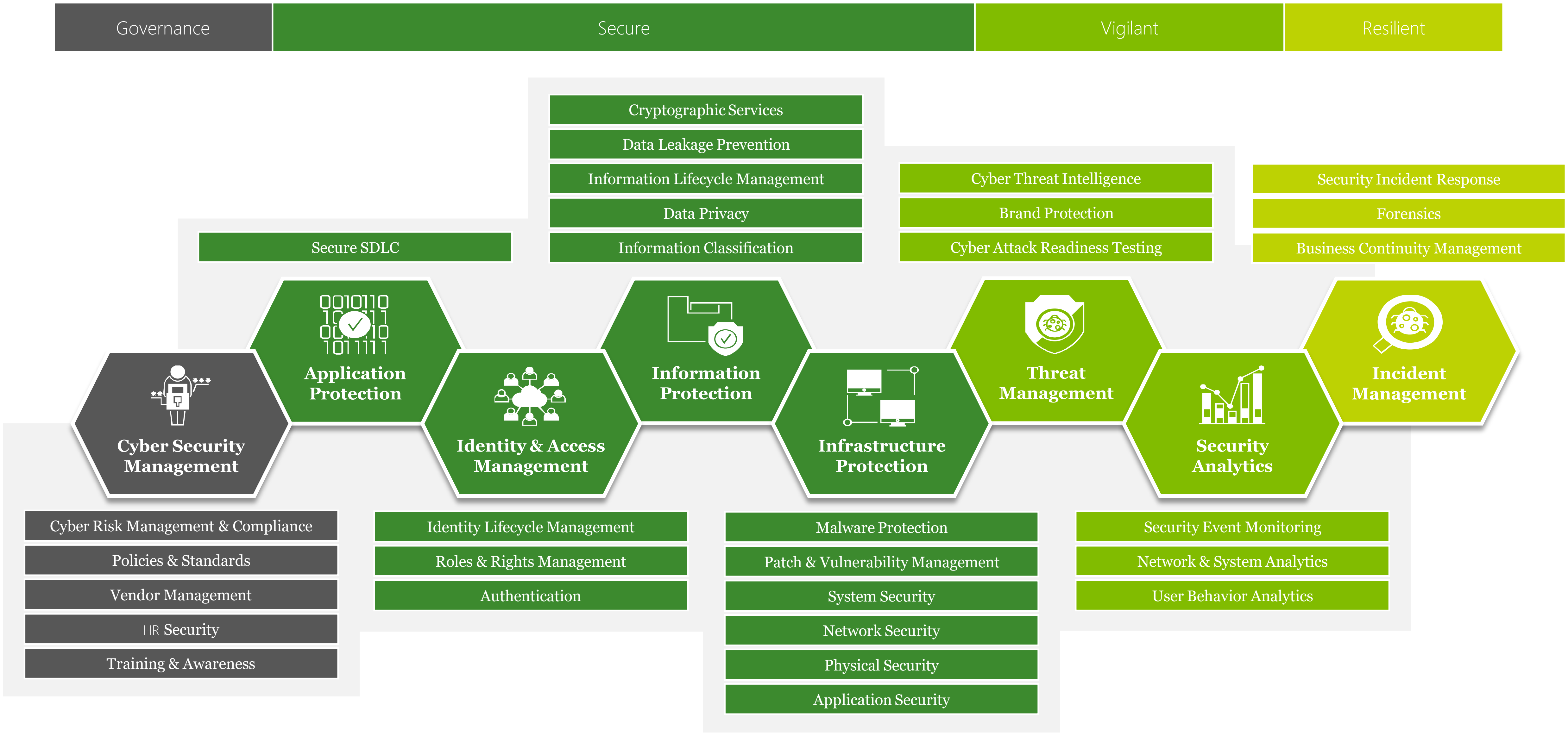
Insider Threats Protection

- Endpoint Protection
- Data Leak Prevention - DLP
- HR related precautions
- Training
- Forensic

Rapid Response Program

- Risk Based Approach
- Premium Incident Response
- Forensic Investigation
- Legal Handholding

Excelic's Cyber Security Framework & Services



Governance | Secure | Vigilant | Resilient

Cyber Security Management

- Cyber Risk Management & Compliance
- Policies & Standards
- Vendor Management
- HR Security
- Training & Awareness

Application Protection

- Secure SDLC

Identity & Access Management

- Identity Lifecycle Management
- Roles & Rights Management
- Authentication

Information Protection

- Cryptographic Services
- Data Leakage Prevention
- Information Lifecycle Management
- Data Privacy
- Information Classification

Infrastructure Protection

- Malware Protection
- Patch & Vulnerability Management
- System Security
- Network Security
- Physical Security
- Application Security

Threat Management

- Cyber Threat Intelligence
- Brand Protection
- Cyber Attack Readiness Testing

Security Analytics

- Security Event Monitoring
- Network & System Analytics
- User Behavior Analytics

Incident Management

- Security Incident Response
- Forensics
- Business Continuity Management

Corporate & Government Ties

CENTRAL BUREAU OF INVESTIGATION INDIA सत्यमेव जयते INDUSTRY IMPARTIALITY INTEGRITY

प्रवर्तन निदेशालय ED सत्यमेव जयते

महाराष्ट्र पोलीस सद्रक्षणाय खलनिग्रहणाय

GREATER MUMBAI POLICE बृहन्मुंबई पोलीस

Cyber Crime Investigation Cell

सीमा शुल्क एवं केंद्रीय उत्पाद शुल्क CUSTOMS AND CENTRAL EXCISE GOVERNMENT OF INDIA देशसेवार्थ करसंग्रह

TATA
TATA MOTORS

teltronic
a Hytera company

ADITYA BIRLA GROUP

LARSEN & TOUBRO

Kawasaki

ALSTOM
• mobility by nature •

NSE
NSEIT

DAMM
Critical communication made easy

هيئة كهرباء ومياه الشارقة
Sharjah Electricity & Water Authority

Edelweiss
Ideas create, values protect

CRRC

GT20 CANADA

EURO T20 SLAM

राष्ट्रीय सेवा योजना
NATIONAL SERVICE SCHEME

SKF®

LOVELY PROFESSIONAL UNIVERSITY PUNJAB (INDIA)
LOVELY
PROFESSIONAL
UNIVERSITY

MANDATLY
Privacy Compliance Software

BCH ™
BOMBAY COFFEE HOUSE
BANDRA | FORT

destek

DhakDhak ™
India ke Dil ki Dhadkan

ARYANS
GROUP OF COLLEGES

D Y PATIL
UNIVERSITY

JBCN
International School

BKC
Your Growth Our Mission

RP
RAM PRIYANKA
Media Entertainments

KUAUSMEDIA
ENTERTAINMENT
FILM PRODUCTION, PR, CELEBRITY, EVENT & TALENT MANAGEMENT

Polaron
TECHNOLOGIES PVT. LTD.®

LEGAL NEXTT

- Thank You