Deloitte.

Securing the value creation with IoT

A holistic perspective on security in IoT

Authors

Deloitte: Teppo Rantanen (Partner, Global), Kristian Herland (Consultant)
Conscia Netsafe: Emanuel Lipschütz (CTO), Johanna Calais
Cisco: Andreas Edin Carlsson

conscia netsafe

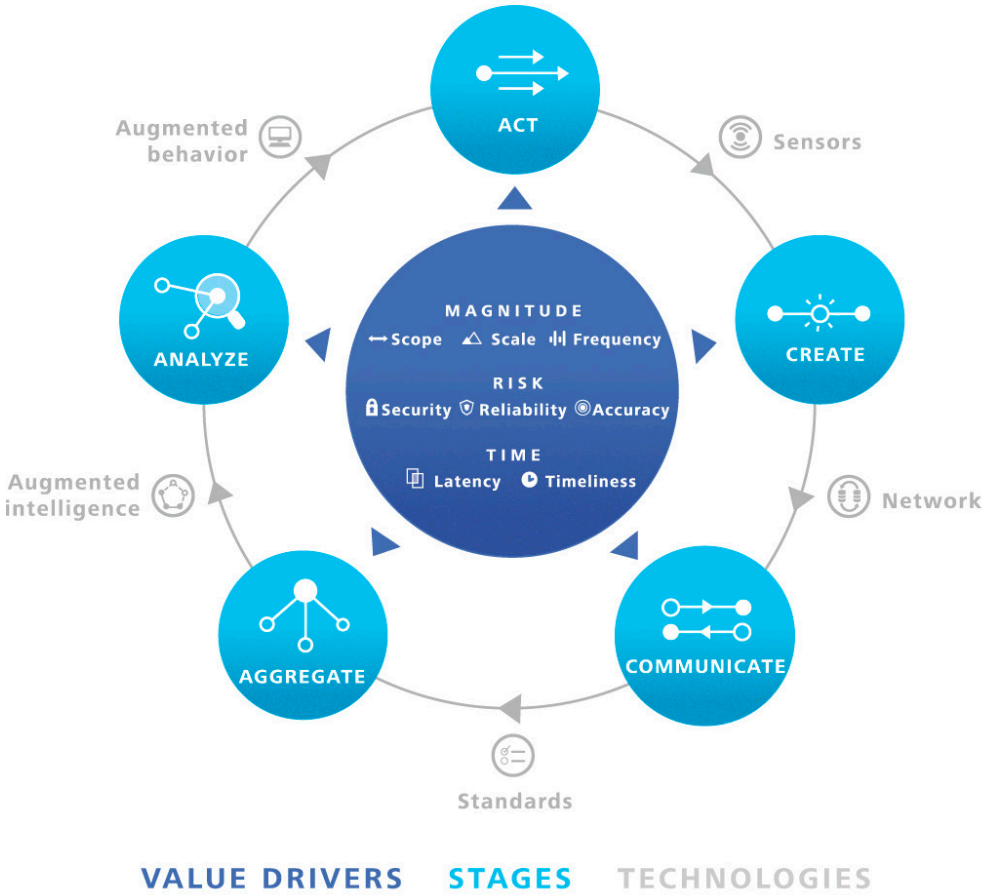
cisco

Introduction

Everybody is talking about Internet of Things (IoT), and the potential it is bringing to businesses and individuals. A defining element of the IoT is that objects are not merely smart – equipped with sensors and processing power – but also connected: able to share the information they generate. What separates the IoT from the traditional Internet is the removal of people. The Internet is powered by humans inputting data: search terms, e-retail browsing, looking up a friend's social media page. Based upon the answers, they make decisions about how to act: whether to visit the site, buy the sweater, or "like" a friend's photo.

With the IoT, the role of humans diminishes, to the point that in many cases they are removed from the equation: Machines input, communicate, analyze, and act upon the information. Using sensor detection, machines can create information about individuals' behavior, analyze it, and take action – ideally in the form of streamlined, tailored products and services or, in the case of businesses, greater efficiencies. This newfound capability is why the IoT enables enterprises and individuals alike to create value in new ways, at a faster velocity than we've ever seen (see the diagram "The Information Value Loop").

Value creation will be one of the fundamental features of IoT, whereby enterprises need to look for new business models, new ecosystems, new ways to describe their value they create and also new thoughts how to share the value.



The Information Value Loop

Note first that the value loop is a *loop*: An action – the state or behavior of things in the real world – gives rise to information, which is then manipulated in order to inform future action. For information to complete the loop and create value, it passes through the *stages* of the loop, each stage enabled by specific *technologies*. An *act* is monitored by a *sensor* that *creates* information. That information passes through a *network* so that it can be *communicated*, and *standards* – be they technical, legal, security, regulatory, or social – allow that information to be *aggregated* across time and space. *Augmented intelligence* is a generic term meant to capture all manner of analytical support, which collectively is used to *analyze* the information. The loop is completed via *augmented behavior* technologies that either enable automated autonomous action or shape human decisions in a manner that leads to improved action.

There is a dark side, however: As data are created and transmitted, this represents a new opportunity for that information to be compromised. More data, and more *sensitive* data, available across a broad network means the risks are higher and that data breaches could pose significant dangers to individuals and enterprises alike. Thanks to the IoT, data security risks will very likely go beyond embarrassing privacy leaks to, potentially, the hacking of important public systems. According to the World Economic Forum, "Hacking the location data on a car is merely an invasion of privacy, whereas hacking the control system of a car would be a threat to a life." Consequently, in addition to new ways to create and capture value through information, the rise of the IoT creates a new need to *protect* this information-based value.

We have found it highly effective to think about cyber risk management using the following paradigm:

Secure:

In the spirit of "prevention" being worth more than a "cure," effective risk management begins by preventing system breaches or compromises. The forms that effective prevention takes include controls of many layers, types, and approaches, because the potential attacks are quite effective at exploiting weaknesses never imagined by their creators. We lock our doors because thieves might enter through them. Similarly, we physically "harden" sensors on power plants to protect them from accidental or deliberate assaults, and install software firewalls to keep out hackers.

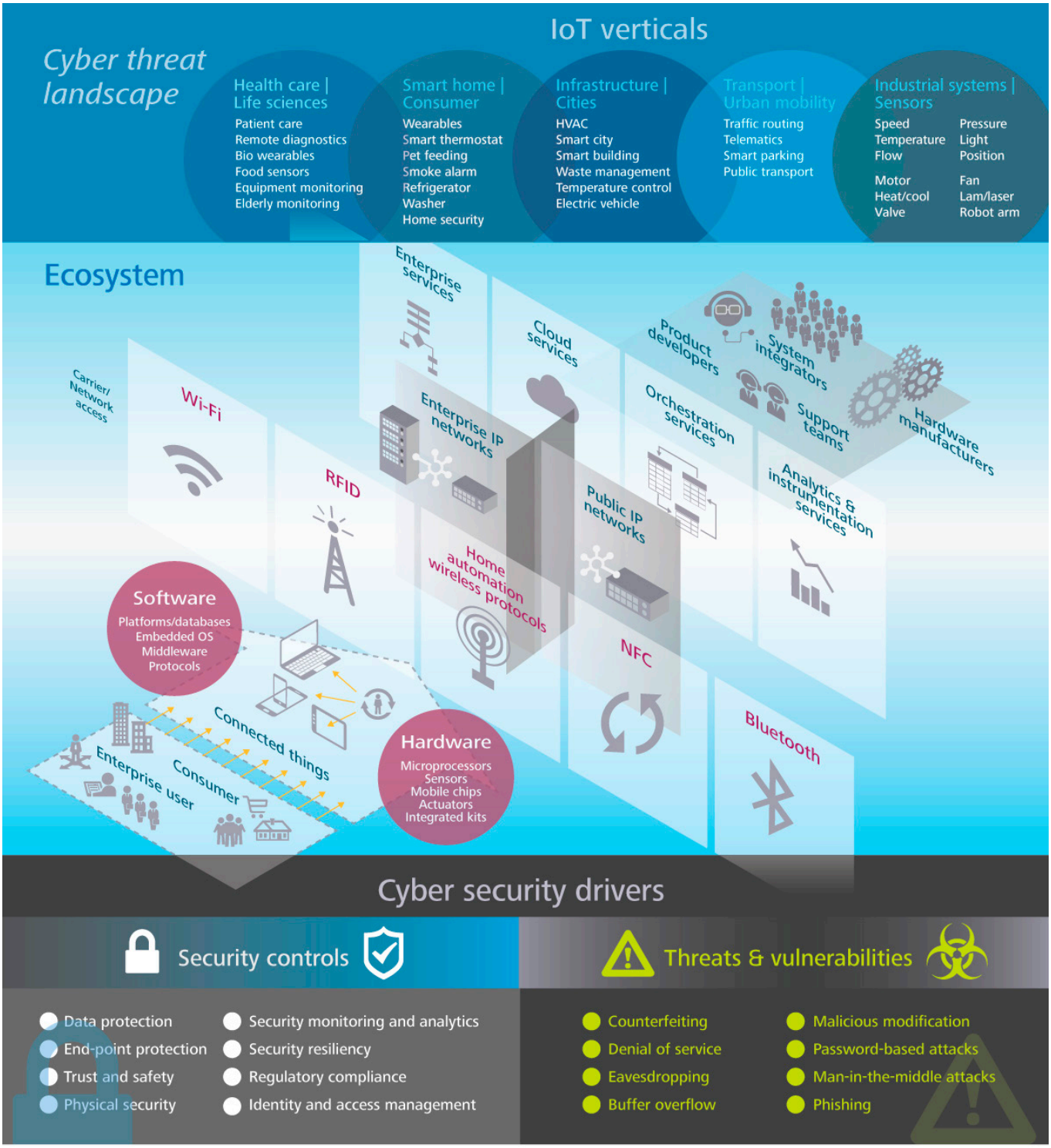
Vigilant:

Making a system secure is not a once-and-for-all proposition. Both hardware and software degrade over time due simply to age. Worse, the nature and intensity of attacks can change in ways that render previously effective security measures obsolete. And, of course, no level of security is perfect: Best efforts still leave any system vulnerable. Consequently, security must be complemented by vigilance – monitoring to determine whether a system is still secure or has been compromised.

Resilient:

When a breach occurs, limiting the damage and reestablishing normal operations are much more easily and effectively done when there are processes in place to quickly neutralize threats, prevent further spread, and recover.

Security challenges in IoT



The cyber risk landscape is inexhaustibly complex and ever changing. This figure provides a broad framework for identifying and managing a much wider range of risks arising from IoT implementations.
Source: Deloitte & Touche LLP.

Organisation & responsibilities

While IoT is currently being deployed in a widespread manner throughout different industries and enterprises, there is simultaneously a distinct lack of experience related to building and maintaining an IoT environment, let alone ensuring the security of such a deployment. Enterprises and authorities generally lack knowledge, guidelines and policies relevant to IoT deployment as well as the methods to perform appropriate vulnerability and risk analyses. In order to ensure the security of IoT solutions, a comprehensive understanding of the related business processes, operational support and the technology stack is required.

Industrial control systems (ICS) have traditionally been built on isolated networks. However, the industry trend is currently towards convergence of operational technology (OT) and information technology (IT). Responsibilities for security controls have often been divided between those working within OT and those within IT. The current convergence raises a question of where the responsibility for security should be in the future. Although the deployment of IoT solutions might be driven by business, the deepest security-related experience in enterprises is usually found in IT.

Architecture & design

The previously isolated ICS networks are now being connected to office networks and thereby to the whole internet. Industrial control networks are adopting IP-technologies as well as commercial off-the-shelf hardware and software such as Windows operating systems. As a consequence, this change forces new requirements on how companies and authorities design, implement and operate their networks, including both information technology and operational technology.

IoT solutions in the enterprise typically use technologies from several vendors, wherein both upstream and downstream supply chain partners generate data, which extend even to the end-use customer. In addition to each individual component's architectural security, the holistic security of the solution should also be given enough attention. The lack of a single, generally accepted standard governing the functioning of IoT-enabled devices is frequently a barrier to the interoperability required to realize the IoT deployments that many envision. Consequently, companies can find themselves falling back on ad hoc solutions to create the interoperability that a given IoT solution needs, which usually leads to a trade-off between creating interoperability and adequate security.

Although the deployment of IoT solutions might be driven by business, the deepest security-related experience in enterprises is usually found in IT.

Where corporate systems are beginning to receive tremendous amounts of data from various different devices and sensors, a question of trust and integrity also arises. A large part of the value of IoT deployments stems from an ability to aggregate the data, yet the sensor technologies used in an ecosystem can vary heavily. Data are generated in different formats, and sensors connect to different networks via various communication protocols. Ensuring that the received data has not been compromised or interfered with poses significant challenges.

Technology & security solutions

Due to the multi-layered nature of IoT solutions, they can include a large scale of vulnerabilities ranging from the hardware level to network access, authentication, data exchange protocols and possibly even cloud services This significantly increases the complexity of possible vulnerabilities and makes it very difficult to reliably audit the security of a solution. Traditional security models do not typically take into account the multi-layered nature of IoT, which calls for new approaches to vulnerability testing.

For example, sensors are susceptible to counterfeiting (fake products embedded with malware or malicious code); data exfiltration (extracting sensitive data from a device via hacking); identity spoofing (an unauthorized source gaining access to a device using the correct credentials); and malicious modification of components (replacement of components with parts modified to generate incorrect results or allow unauthorized access). Any or all of these compromises would leave the sensors vulnerable. Communication networks can be hacked, allowing data to be intercepted or their flow disrupted through denial-of-service attacks. Tools for performing many kinds of attacks are on-sale on the internet and can be utilized even with limited technical knowledge.

Standalone IoT devices are often characterized by traits such as small size as well as low computational capacity and power consumption, which are important enablers in their widespread deployment. However, these characteristics can also make it difficult to add traditional security measures such as robust encryption. The solutions used in ICS networks have often been designed with little focus on security, which may be partly caused by an assumption that the devices would only be used in isolated systems. However, with today's connections between the internet and ICS networks, shortcomings in basic security settings and awareness such as using default passwords, shared credentials and unnecessary administrator rights can lead to serious cyber incidents.

Connecting industrial control systems to centralized management solutions on IP networks is solving cost issues of managing the devices. However, the increased inter-dependencies between devices and processes cause an exponential increase in the possible consequences of a cyber-attack. Unfortunately, most IT security solutions and management systems are currently unable to mitigate these issues as they lack functionality to sufficiently protect IoT solutions and industrial control systems. Traditional firewalls and intrusion prevention solutions (IPS) have rarely been designed for operational technologies such as SCADA and related protocols.

Past breaches in IoT environments

Numerous public examples already exist of breaches affecting industrial control systems, for example the Stuxnet malware affecting nuclear facilities and the data theft from one of the world's leading manufacturers of chip-making equipment.

The Stuxnet malware's objective was to access and damage SCADA systems used as industrial control systems for infrastructure, monitoring and industrial processes. The worm utilized several to-date-unknown security holes in order to evade intrusion detection systems. The sabotage involved attempts to over-pressurize the centrifuges as well as over-speed the centrifuge rotors. As a result, approximately 1000 centrifuges were damaged and had to be replaced. Similar systems are widely used in oil pipelines, power plants, large communication systems, airports, ships and even military installations globally.

The other aforementioned cyber-attack's target was a global manufacturer of photolithography machines for the production of integrated circuits such as CPUs and memory chips, which consequently makes them a natural potential target for industrial espionage. When the attack became widely known and covered in the news, the company claimed the attack had made only limited damage. External analysts suggested that the attack had its origin from China – however, the true impact of the attack or the identity of the attacker have not been determined or publicly disclosed.

Traditional security models do not typically take into account the multi-layered nature of IoT, which calls for new approaches to vulnerability testing.

Minimizing risks in IoT – The solution

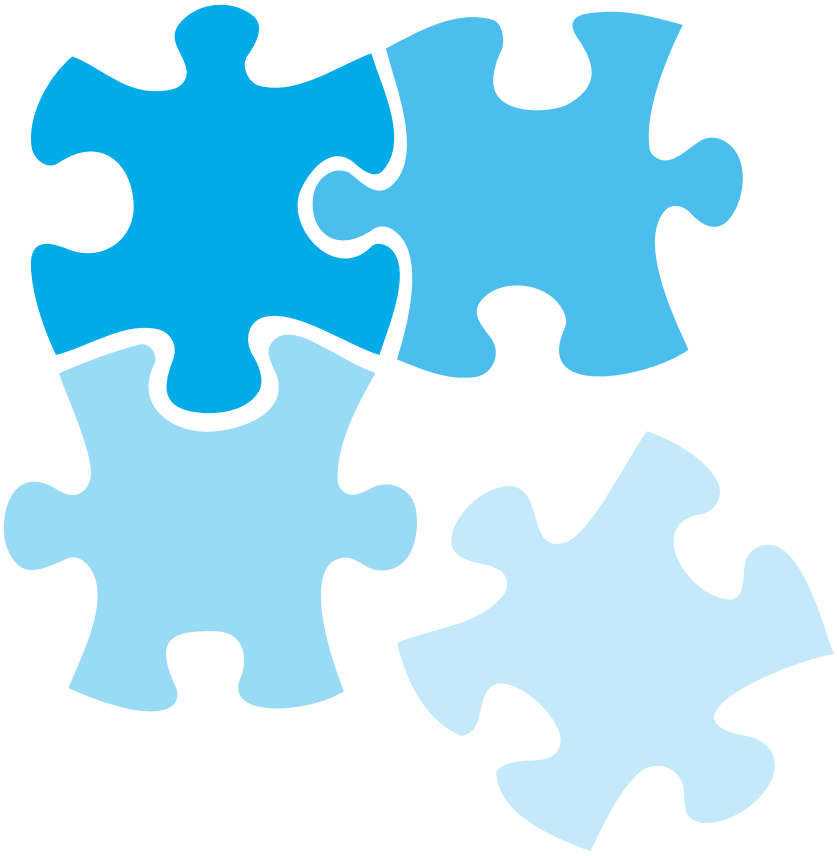
While cyber security used to be considered an issue primarily for the IT team, these days it is an agenda item for the entire C-Suite. Good information security is a continuous process which should be integrated into all business and other functions, and thereby needs strong leadership and nourishment. Ensuring that everyone including external partners is onboard with the security mission is imperative, as an organization's security culture is fundamentally made up of the individual employees' awareness and attitude.

As previously exemplified, IoT applications are diverse and so are the challenges in security. There is no silver bullet solution to mitigate every threat. Most importantly, companies that establish an IoT strategy should adopt a holistic approach to security that involves the complete infrastructure, starting with the design. The security framework for IoT needs to involve several security mechanisms, and the framework needs to cover device *authentication, authorization, access control, segmentation, firewalls and intrusion prevention,* and lastly an adequate *security management system* to control and monitor the security mechanisms.

Authentication is central to verify the identity of any device connected to the IoT environment. The authenticated device identity is the basis of trust, and different IoT devices will have different means of authenticating. *Authorization* on the other hand means leveraging the authenticated identity to grant privileges based on policies, and *access control* ensures that only the authorized information can be shared or gathered. As IT and OT environments converge and become interconnected, it is crucial to design the converged environment according to security best practices – divided into zones and then further *segmented* based on functional requirements and security classification. Each zone should use specific security mechanisms to mitigate threats.

While general security solutions usually have very limited understanding of and access to IoT protocols, IoT-specific security appliances allow inspection and policy enforcement of protocols specific to these environments. Requests sent to devices can be interpreted and controlled based on payload, rather than being limited to mere access control. This means that unintentional or malicious instructions can be prevented by the security appliance, avoiding malfunction of sensitive instruments. Management solutions such as Cisco Lancope StealthWatch can monitor every traffic flow (IP) on the network, and thereby detect connection attempts, malware, credential abuse and unavailability, amongst other events. Even though every incident cannot be prevented, by reducing the time required to detect an incident, the effects of cyber-attacks and the delay to return to normal operation can be minimized.

In order to select the appropriate security framework and mechanisms, it is necessary to embrace best practices from 25 years of the industry's IT-security experience, but also new best practices for converged IoT environments. The design of an IoT environment needs to meet the functional, technical and business requirements, and implement a non-compromised design to mitigating current security threats. Conscia Netsafe, a Swedish Cisco Gold partner and design expert company, follows a proven design process for infrastructure and security solutions. The four main steps in the design process are:



1. Preparations and high level design

Firstly, the project scope, business outcomes, functional needs and technical requirements are determined. Secondly, the product specifications are drafted including a project budget. The high level design is discussed, documented and agreed to by all stakeholders.

2. Low level Design

The aim of the low level design is to cover the complete technical solution in detail. It includes in-depth technical documentation such as an explanation of all the technologies involved, its purpose, technical functions and all configurations. The low level design is mutually signed off prior to going into next phase.

3. Proof of Concept

The third phase comprises functional validation of the solution. The technical design is tested, validated and documented against hardware and software components, and the security framework is evaluated through security penetration testing. Any deviations from the plan or failed tests, implies a revision of the design or product specification.

4. Tailored training

Lastly, but nevertheless as important a step as the technical solution, the customer needs to be prepared to operate the solution in a production environment. Therefore, the last step in the design process is to provide a tailored training in order for the customer to master the technical concepts, and the implemented technical solution.

By carefully following this design process, Conscia Netsafe delivers timely design projects on budget, with a solid and validated solution based on customer requirements and agreed business outcome.

Conclusions

While the adoption of IoT solutions is soaring, organizations are becoming more and more vulnerable to cyber security threats. With the increasing amount of connected devices and the convergence of operational technology and information technology, the stakes in cyber security are higher than ever. Major breaches regularly cause severe financial damages, not to mention physical-world-consequences, which could potentially endanger human lives. Security has traditionally not been able to keep up with technological development, and unfortunately, this still applies to IoT. Improvements are needed everywhere from high-level organization and leadership of security, to solution architecture and security technology. In order to catch up with the technological progress, IoT requires a new approach to security. A holistic security framework involving all stakeholders is essential, especially in IoT environments with numerous involved parties. Awareness of the security challenges and commitment to their mitigation should be basic requirements from all parties involved in any lifecycle stage of an IoT environment. In order to ensure the security of an IoT environment, a complete security architecture and design is needed as a foundation.

Deliverables

Partner consortium that can help your company with secure IoT strategy.

Deloitte

Deloitte helps organizations plan and execute an integrated cyber approach to harness the power of information networks to enhance business operations, increase mission performance, and improve customer support, without compromising security or privacy.

Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries and territories, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's more than 200,000 professionals are committed to becoming the standard of excellence.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Conscia Netsafe

Conscia Netsafe is an agile Swedish systems integrator and Cisco Gold partner. Conscia Netsafe is one of the prime experts in the Nordics in designing, deliver and support solutions for Datacommunication, IT-security and Datacenters. The business value Conscia Netsafe brings to the table is;

World class expertise
An Expert consultant organization with focus on customer business outcome, and that holds one of the highest level of certification-grade amongst partners in the Nordics. Conscia Netsafe is no. 1 Partner in the world with most certified design experts*, only Cisco holds more.

Inventory & Compliance Management Portal
With about 30.000 development hours invested in the unique customer portal, the customer can manage its complete product inventory, product lifecycle, get a dynamic security analysis, as well as gain expert-recommendations for the customers installed base. For customers signing a service agreement for product maintenance, the compliance and security portal is included without extra costs.

*Source: http://orhanergun.net/global-ccde-list/

Cisco

Cisco delivers intelligent cybersecurity for the real world, providing one of the industry's most comprehensive advanced-threat protection portfolios of solutions across the broadest set of attack vectors. Cisco's threat-centric and operationalized approach to security reduces complexity and fragmentation while providing superior visibility, consistent contr°l, and advanced threat protection before, during, and after an attack.

Cisco is the worldwide leader in helping companies seize the opportunities of tomorrow by delivering the amazing results that come from connecting the previously unconnected. Cisco is empowering countries, cities, industries and businesses around the globe to move faster in order to keep pace with digital transformation and the move to the Internet of Everything (IoE). With approximately 70,000 partners, Cisco is very well positioned to provide our customers with next generation networking, security, data center, and collaboration products and solutions that help them achieve their desired business outcomes