25 August 2023

Cyber Security in Smart Agriculture Technology

Snode

TABLE OF CONTENTS

Introduction

Agriculture is one of the oldest fields of human activity, and is the backbone of most countries, providing enormous employment opportunities to the community as well as goods manufacturing and food supply. It is an essential element of modern society. The UN estimates that agricultural production accounts for 70% of freshwater consumption, 38% of land use and 14% of greenhouse gas emissions. [1] It identifies agriculture and food consumption as one of the most important drivers of environmental pressures, especially habitat change, climate change, water use and toxic emissions.

It is anticipated that by 2050 global population will be increased from the current 7.7 billion to 9.2 billion, urban population will be rise by 66%, arable land will be declined by approximately 50 million hectares, global GHG emissions (source of CO2 – promotes crop disease and pest growth) will be increased by 50%, agri-food production will be declined by 20%, and eventually, food demand will be increased by 59 to 98% posing an imminent threat to food security and adequate food availability. To satisfy the increasing food demands, agricultural practitioners worldwide will need to maximise agricultural productivity involving crop and livestock farming. [2] Additionally climate change; changes in temperature, erratic monsoon, and unpredictable weather patterns and precipitation levels among many others; impacts agriculture in a big way. In fact, crop production is projected to decrease in many areas in the 21st century owing to such climate variations. [3]

Agriculture has undergone several revolutions, which improved the sector's efficiency and profitability. The plant domestication (10,000 BC) led to the world's first societies and civilization. In recent centuries, agricultural mechanisation (1900 and 1930) introduced machines and implements to mechanise work, increasing farmworker's productivity. The Green Revolution (1960s) enabled farmers to use new crop varieties and agrochemicals. In the late century and early century (1990 to 2005), biotechnology allowed the creation of plants with pre-selected traits, such as increased yield and resistance to pests, drought, and herbicide. Now, the digital revolution could help humanity to survive and thrive long into the future. [4]

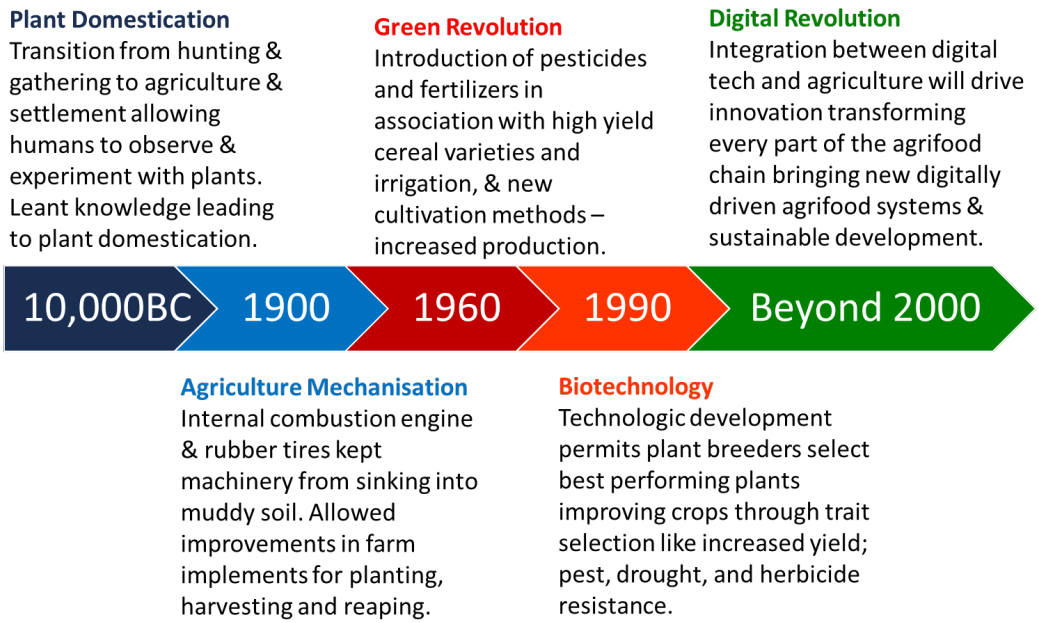

Figure 1 The Evolution of Agriculture [4]

The agriculture industry faces a lot of challenges, most of which are quite significant in terms of the impact on the future of the planet. These include:

- **Land Management** - The usage of synthetic fertiliser, pesticides, and insecticides for agriculture drastically reduces the fertility of the soil. This makes the soil degrade in quality, reducing the growth rate which in turn has to be fixed by using more fertiliser, pesticides, and insecticides. The usage of synthetics also seeps into and pollutes the water sources nearby.
- **Climate Change** - Intensive agriculture calls for aggressive reclamation of land from forests and this not only reduces forest cover but increases the production of greenhouse gases causing climate changes and a rise in temperature. While the change in temperature and climate affects us, it also affects the growth and harvesting of plants and crops worldwide.
- **Resource Depletion** - Agriculture involves a lot of machinery that requires other resources in order to be built and run – for example, metal for the parts and petroleum for the fuel. This just adds up as a bigger cause for environmental harm in the end rather than helping reduce it.
- **Increasing Carbon Footprint** - Farming produces a lot of waste and by-products. Take the case of organic farming which is thought to have a positive impact on the ecosystem and healthier plants, it however adds to the increasing temperature and climate change phenomenon since it takes up a lot more land compared to traditional farming methods. So, farms all over the world are forced to either be more optimised or follow traditional methods of farming which also are harmful to the ecology in the long run.
- **Biodiversity** - The increase in population leads to the ramping up of agricultural production in order to feed the growing numbers. This, in turn, leads to the conversion of non-agricultural lands such as forests, into agricultural land. The reclamation of forest land leads to the reduction of the biodiversity of that particular area which has effects on the flora and fauna.

Digital technologies have advanced more rapidly than any innovation in our history – reaching around 50 per cent of the developing world's population in only two decades and transforming societies. Throughout history, technological revolutions have changed the labour force: creating new forms and patterns of work, making others obsolete, and leading to wider societal changes. [5] Industry 4.0, also known as the fourth industrial revolution, is revolutionising, and reshaping every industry. It is a strategic initiative characterised by a fusion of emerging disruptive digital technologies such as Internet of Things (IoT), big data and analytics (BDA), system integration (SI), cloud computing (CC), simulation, autonomous robotic systems (ARS), augmented reality (AR), artificial intelligence (AI), wireless sensor networks (WSN), cyber-physical system (CPS), digital twin (DT), and additive manufacturing (AM) to enable the digitization of the industry. [6] The agricultural domain has demonstrated a rapid technological growth in recent years by engaging a variety of these technologies, taking advantage of robust and trustworthy connectivity and the variety of ways in which, the technologies can combine. For example, the development of smart and precision agriculture applications in order to reduce the existing risks and maximise the production efficiency. The integration of these technologies in agriculture is sparking the next generation of industrial agriculture, namely, agriculture 4.0 – also termed smart agriculture, smart farming, or digital farming. These innovations are only some of the notable achievements that have come as a result of the huge growth of ICT capabilities.

The digital transformation of agriculture can play a huge role in addressing the challenges discussed. Industrial IoT devices, robotics, satellite connectivity, artificial intelligence and cloud-edge platforms are driving the acceleration of the sector and integration of these technologies can provide the following benefits:

- Crop monitoring, decreasing the overall costs,
- Logistic and qualitative traceability of food production combining decision making processes with real-time data for reducing the waste of inputs and overall costs,
- Capitalising on Big Data resources, at hardware and software level, establishing new agriculture communities in urban and rural areas,
- Generating novel business models in the sector, creating a new retailer–consumer relationship,
- Automatic irrigation systems development that adjusts operations based on the humidity, temperature and soil moisture values which are retrieved through the embedded sensors,
- Collection of environmental parameters, in an automatic way using IoT, which are usable for further analysis,
- Big Data analytic processes and tools for enhancing productivity using decision support systems.[7]

However, smart agriculture is still emerging and has a low level of security features. Future solutions will demand data availability and accuracy as key points to help farmers, and security is crucial to building robust and efficient systems. Since smart agriculture comprises a wide variety and quantity of resources, security addresses issues such as compatibility, constrained resources, and massive data need to be considered. Conventional protection schemes may not be useful for agricultural systems, creating extra demand and opportunity. In this paper we discuss the various technologies used in smart agriculture. We then discuss recent attacks on the agriculture sector and the risks associated with smart agriculture. Finally, we provide advice on how to deal with these risks.

Smart Agriculture Technologies

Agriculture has tremendous potential to shape the future of our planet by tackling the greatest challenge the world has seen. To produce enough safe, nutritious food for all, while caring for our animals, and sustaining our land, air, and water for future generations. While agriculture is currently the least-digitised industry in the world, Agri-tech has seen a fourfold growth of investment since 2014, with $2 billion invested in farming tech startups globally in 2018. [8]

The smart agriculture market is projected to reach USD 25.4 billion by 2028 from USD 16.2 billion in 2023, at a compound annual growth rate (CAGR) of 9.4% from 2023 to 2028. Surging use of modern technologies in agriculture and rising adoption of IoT, ROVs, and AI in aquaculture farming are among the key factors driving the growth of the Smart Agriculture market.[9] North America is the most dominant market for Precision Agriculture globally. This trend is followed by Europe, some countries in the Asia Pacific region like Japan, China, South Korea, India and certain other countries like Brazil, Argentina, Cuba and South Africa. [10]

Historically technological revolutions have changed the labour force: creating new forms and patterns of work, making others obsolete, and leading to wider societal changes. Digital technologies have advanced more rapidly than any innovation, reaching around 50 per cent of the developing world's population in only two decades and transforming societies. Technological advancements have had an incredible impact on the agriculture industry. Today's agriculture routinely uses sophisticated technologies such as robots, temperature and moisture sensors, aerial images, and GPS technology. These advanced devices agriculture systems have boosted productivity, profitability and food safety, enhanced traceability and quality control and increased precision input of antibiotics and fertilisers. There are environmental benefits as well, such as reducing emissions, waste, and land disturbances.

The Significance of Precision Agriculture

Precision farming uses modern technologies such as satellite imagery or field mapping to improve crop quality and profitability. Moreover, it optimises the use of traditional resources. Therefore, this agricultural management system contributes to the development of sustainable agriculture, allowing to solve both economic and ecological problems, which are becoming more acute.

Among the technologies used in such a system are GPS, drones, and satellite images. Based on this data, farmers receive information on all key issues: crop status, weather forecasts, environmental changes, etc. Listed are just some of the benefits of such a control system:

- diversifying management decisions for individual field parts,
- minimising the cost of materials and resources, like water, seeds, fuel, etc.,
- maintaining soil health by reducing the number of pesticides,
- lowering agriculture's dependence on weather conditions,
- maximum realisation of the genetic potential of the produced crops,
- All these advantages of precision farming allow farmers to improve the quality of products significantly and, at the same time, reduce their costs.[11]

Precision livestock farming (PLF) is the use of advanced technologies to optimise animal production. It allows farmers and ranchers to consistently collect information at the animal level to recognize sick animals, increase feed efficiency, and save on labour, feed costs, and time. This is enabled by technologies that allow for the customization by animals for functions such as automated milking systems, electronic feeding, and health monitoring. In both crop and livestock agriculture, precision agriculture provides environmental benefits by reducing required inputs, minimising energy use, and reducing waste. Due to its tendency to reduce labour and inputs, precision agriculture also provides economic benefits to farmers.

Field precision agriculture is enabled by precision geolocation, remote sensing, and the mapping of soils, nutrients, crop conditions and the location of weeds and pathogens. On the ground this is accomplished with farm machinery that utilises Variable Rate Technology (VRT), yield monitoring, Auto-Steering, guidance, navigation, and on-board computers and networking capabilities. Below are descriptions of the technologies used in crop and livestock production.

Internet of Things (IoT)

Internet of things (IoT) refers to a variety of interrelated computing devices, sensors, appliances, and machines connected with the internet, each having unique identities and capabilities for performing remote sensing and monitoring.

In the agricultural domain, IoT devices in the physical layer gather data related to environmental and crop parameters such as temperature, humidity, pH value, water level, leaf colour, fresh leaf weight, etc. The transmission of this data takes place in the network layer, the design of which depends on the selection of suitable communication technologies relevant to the field size, farm location, and type of farming method. RFID (radio frequency identification) and NFC (near field communication) technologies are increasingly being implemented in agricultural systems for tracking agricultural products. GPRS or mobile communication technology (2G, 3G, and 4G) are used for periodic monitoring of environmental and soil parameters. To store data, cloud computing techniques are employed in the service layer. This data is then used in the application layer to build smart applications used by farmers, agriculture experts, and supply chain professionals to enhance farm monitoring capacity and productivity.[2] Just like crop monitoring, there are IoT agriculture sensors that can be attached to the animals on a farm to monitor their health and log performance. Livestock tracking and monitoring help collect data on stock health, well-being, and physical location.

IoT technologies are one of the reasons why agriculture can generate such a big amount of valuable information. It is estimated that, with new techniques, the IoT has the potential to increase agricultural productivity by 70% by 2050. The main advantages of the use of IoT are achieving higher crop yields with less cost. For example, studies from “OnFarm” found that for an average farm using IoT, yield rises by 1.75% and energy costs drop 17 to 32 dollars per hectare, while water use for irrigation falls by 8%. [12]

Global Positioning System (GPS) and Geographic Information Systems (GIS)

GPS refers to ground-based technology permitting growers to gather data with accurate location information in real-time. GPS is suitable for the following tasks:

- mapping of irrigation systems, fields, and roads,
- detection of areas with problem plants,
- soil testing in specific field areas,
- the tractor driving with a parallel steering system,
- VRA for precise seed and fertiliser application.

Also, GPS in precision agriculture allows for controlling agricultural machinery. For example, with its help, growers can drive tractors in poor visibility due to rain or fog.

Geographic Information Systems operate with object details and location data to create maps, including digital ones. GIS in precision agriculture permits farmers to view records, such as soil survey maps and plant characteristics traditionally grown in the region. Satellite images and aerial photographs provide additional information. Another handy feature of GIS is analysing multiple farm management options by comparing and manipulating data layers. [13]

UAVs And Dusters

Aerial technologies for crop management are based on using unmanned aerial vehicles (UAVs). Thus, farmers can monitor the yield's condition without scouting all fields in person. The use of drone technology in modern farming is growing at an unprecedented rate as more agriculturists rely on technology's ability to key tasks. With drones, farmers can capture data of their entire farmland, all from the comfort of a single take-off zone. Drones with high-tech capabilities even allow farmers to enhance efficiency in certain aspects of the farming process. The technology can be used from crop monitoring, planting, and livestock management to crop spraying, irrigation mapping, and more. Using UAVs or drones in precision agriculture is a more progressive solution. They are controlled remotely and consume less fuel. Moreover, precision agriculture drones can analyse the field thoroughly, conducting complex multispectral, thermal, and hyperspectral soil analyses.[14]

Robotic Technology

Robotic farm labour technology appears to be a viable choice for precision agricultural needs because it can do monotonous tasks without sacrificing accuracy. The autonomous performance of such robots would allow for continuous field management and improved agricultural productivity and efficiency as a result of the robot's ability to gather information about its environment on its own. Autonomous devices operated remotely via telemetry are currently the most well-known and successful agricultural robotic technology [15]. Currently agricultural robots can carry out various tasks, such as planting and harvesting crops, weed control using chemical or mechanical tools, application of pesticides, soil analysis, and milking livestock [16].

Agri-robotic systems provide multiple emerging opportunities that facilitate the transition towards net zero agriculture. Additionally, robotics could impact sustainable food production systems to (1) increase nitrogen use efficiency, (2) accelerate plant breeding, (3) deliver regenerative agriculture, (4) electrify robotic vehicles, (5) reduce food waste. [17]

Smart Sensors

Weather conditions, plant moisture, soil temperature and fertility, pest infestations, and weed locations can all be determined with the help of agriculture sensor technology. The use of this data assists growers, agri-consultants, insurers, and others involved in the agricultural sector in making more informed decisions, leading to more output from farms at lower costs.

Satellite remote sensing allows growers to observe the yield health using satellite images. They provide up-to-date information on moisture stress, disease, structural anomalies, and nutrient levels. Modern precision agriculture satellite imagery has a high spectral resolution, allowing growers to get the most accurate data. An essential benefit of this method compared to GPS and UAVs is the absence of additional fuel and labour costs. [14]

Artificial Intelligence & Machine Learning

AI, which has advanced rapidly over the past two decades, encompasses a broad range of technologies capable of performing human-like cognitive processes, such as reasoning. It's trained to make these decisions based on information from vast amounts of data.

The autonomous-farming industry is beginning to boom, with approximately 200 AI-based agricultural startups in the U.S. alone. Examples of artificial intelligence on farms include self-driving tractors and combine harvesters, robot swarms for crop inspection and autonomous sprayers. Indoor farming companies are using AI and computer vision to collect data on crops and adjust the environment for optimal nutrition and flavour. They also use robots to harvest the food. Machine vision and artificial intelligence is used to differentiate crops from weeds, allowing for targeted herbicide application and less human labour. In livestock farming, deep learning technologies can keep watch on the behaviour of animals to ensure that they are sleeping, eating, drinking, and ruminating sufficiently.[18]

Big Data

For every industry, big data analysis is becoming an integral business strategy. In fact, The Global Big Data and Business Analytics Market is expected to grow from USD 192.24 billion in 2019 to USD 446.42 billion by the end of 2025. Big data analysis helps businesses to differentiate themselves from others and increase revenue. Through predictive analytics, big data analytics provides businesses customised recommendations and suggestions. The agriculture industry is moving quickly toward digital adoption and increasing the use of data and analytics. The Global Agriculture Analytics Market accounted for $590.03 million in 2018 and is expected to reach $2,461.65 million by 2027. [19] Farmers are embracing Big Data to automate, gather insights, and ultimately help them make better decisions. For example, smart sensors gather real-time information and share it with cloud servers where advanced analytical tools combine weather, pricing models, and operational data from farm equipment. The informed insights then guide farmers' decisions.

The features that Big Data brings are computing analytics, web and mobile technologies, visualisation, modelling, and simulation. Predictive insights, in the form of soil risk analytics supported by Big Data Farming, enable farmers to continuously test their soil and make adjustments based on insights from their farms. Farmers today can use Big Data to help

understand and predict crop maturity, by using satellite imagery, weather data and other factors. They can also use this information to determine the best time to harvest their crops, deliver fertiliser or irrigation. This allows them to lower the costs so that they can deliver a more consistent, high-quality product to their customers. [20]

Cloud Computing

Cloud computing enables businesses across sectors to evolve their operations through automation and remote access. Cloud computing-based technology can act as a breakthrough and game changer for big data storage, retrieval, and analysis. For example, the data required for precision agriculture can be easily stored and aggregated in the cloud, rather than on local servers. In the field, this data can be collected by cloud-connected wireless sensors and analysed in the cloud, providing real-time information and decision-making support for farmers to understand crop conditions.

The implementation of IoT sensor technology and monitoring tools is also being supported by the cloud. Cloud offers high storage capacity and can store a vast amount of agricultural data from a wide range of sources. For example, satellite imagery, climatic and crop data, or market data can be aggregated and computed quickly. [21]

Cloud computing technology can also assist in centralising all agricultural related data banks (soil-related, weather, crop, farmers, technology, agriculture marketing, fertilisers, and pesticide information) in the cloud. Time series remote sensing images can show historical agricultural information leading to better production decisions. The fast processing and expeditious processing of the information will enable farmers to respond precisely and in a timely manner for better crop growth and yield, whilst maintaining crop quality. Various Cloud platforms include Google Earth Engine (GEE), Akasai, IBM Bluemix, Microsoft Azure, Amazon Web Services, Alibaba etc. [22]

Smart Farming Software & Mobile Apps

Smart farming systems combine both machinery parts like sensors and drones and software segments like programs and mobile applications. The second part of this complex gives farmers access to the data received from the devices they use and allows them to configure and manage equipment. Properly selected smart farming platform allows specialists to process the received data quickly, make the most effective decisions, and adjust their actions in real-time. For example, programs and mobile applications can recommend the most profitable planting plan based on crop rotation historical data, gathered from satellite images and technical recommendations for growing specific types of crops.

Smart farming apps and platforms take agricultural analytics to a whole new level. With their help, farmers optimise their processes throughout each season, increasing the enterprise's profitability, reducing labour costs, and contributing to protecting the environment. [23]

An Industry Under Attack

The advances in agriculture-related technology have brought along with them an increase in cyber threats. Before the rise of multinational consolidated agribusinesses, much of the world's food was produced by small farmers and ranchers serving a local community. Today the same economies of scale that have fuelled the rise of large corporations in other sectors are applied to food production and distribution. Historically the food/agriculture sector has not been a notable target for cybercriminals. However, threat actors today see the world's dependence on a well-established food supply chain as an opportunity to achieve their nefarious aims. These aims are commonly financial gain but also include acts of political terrorism and social hacktivism. There is clearly work to be done in areas where the food/agriculture sector has been lax in its cyber protection policies and procedures.

The food and agriculture industry covers a broad spectrum of companies that provide a variety of products and services. Large farms and ranches use automated and connected systems for everything from tractor autosteer systems to crop moisture testing to automated distribution warehouses. Many of the companies that make up the nation's food supply chain are interdependent. A stoppage or slow down during harvest season, for example, can reverberate throughout the entire industry as food processing plants and distribution networks feel the effects of events that may have happened weeks or months earlier. Retail stores and restaurants need an easily accessible and reliable source for food products. Any disruption can result in price spikes or shortages that affect people's lives.

Notable Industry Attacks

There have been some high-profile cyber-attacks on the food and farming industry in recent years. Here are a few examples:

- **John Deere** - In 2017, the manufacturer of agricultural equipment experienced a data breach that exposed the sensitive data of over 1,000 customers, including names, addresses, phone numbers, and licence plate numbers. More recently at a presentation at DEF CON an Australian hacker known as Sick Codes presented one of the first public efforts to hack John Deere's farming equipment, 'jailbreaking' the 4640 John Deere tractor display. 'Jailbreaking' is a term to describe the removal of restrictions that hardware manufacturers have put in place to stop hardware owners from running unauthorised software on the device's hardware. The ability to remotely install Doom and run it on a device shows how deep in the source code a hacker can gain access to and control the vehicle. Once this point has been reached, the hacker has conquered the device in terms of hacking; and has full control over the device. [24]
- **JFC International** - In March 2021, JFC International revealed that it had been hit by a ransomware attack that disrupted several of its IT systems. JFC is a major distributor and wholesaler of Asian food products and serves the European and US markets. The company said the attacks impacted JFC International's Europe Group. They were able to resume normal operations soon after notifying law enforcement, employees, and business partners about the incident. [25]
- **Loaves & Fishes** - Non-profit food provider Loaves & Fishes offers nutritionally balanced groceries to individuals and families experiencing a short-term crisis through a network of mobile "drive-through" style food distribution sites. In August 2020, they announced

that sensitive customer information was exfiltrated during the more widespread Blackbaud attack. Blackbaud, a provider of software and cloud hosting solutions, stopped a ransomware attack from encrypting files but still paid a ransom demand to keep the hackers from publishing protected information about their clients – one of whom was Loaves & Fishes. Blackbaud said they have no evidence that the data was sold online, but the potential exists for that to happen at any time. [26]

- **Home Chef** - Owned by Kroger Foods, Home Chef is a startup that provides food ingredients, meal kits, and recipes to its customers. Security researchers said in May 2020 that they found usernames and passwords belonging to Home Chef users for sale on the dark web. Soon after, the Chicago-based company said a security incident had resulted in the compromise of information about an undisclosed number of its customers. This type of security event poses no danger to the food supply but is a risk to consumers of these services. [27]
- **Harvest Sherwood Food Distributors** - In May 2020, data that surfaced on a Tor hidden service called the Happy Blog indicated that hackers deploying REvil ransomware attacked Harvest Sherwood Food Distributors. The attackers stole critical data from the company and threatened to disclose it publicly. REvil is the same ransomware that is later used against JBS Meats. The attackers managed to steal around 2,600 files from the food distributor. The stolen data included cash-flow analysis, distributor data, business insurance content, and vendor information. There were also scanned images of driver's licences of people in the Harvest Sherwood distribution network.[28]
- **Brazilian Agriculture Sector** - In May 2020, Brazil's agriculture sector was targeted by a cyber-attack that impacted several of the country's major food companies. The attack disrupted the companies' operations and led to concerns about the impact on Brazil's agricultural exports.[29]
- **India's Agriculture Infrastructure** - In September 2020, the Indian government announced that it had identified a cyber-attack on its agriculture infrastructure. The attack was detected in the midst of the country's agricultural reforms, which had led to widespread protests by farmers.[30]
- **Fonterra** - In November 2020, New Zealand dairy co-operative Fonterra faced a ransomware attack carried out by Egregor ransomware group. The attack resulted in the compromise of several thousand personal files, however, no ransom was paid. In July 2021, the New Zealand government revealed that the agriculture industry in the country had been targeted by cyber criminals. The government's National Cyber Security Centre issued a warning to farmers and other agriculture sector stakeholders to be vigilant against cyber threats.[31]
- **Australian Winemakers** - In December 2020, several Australian winemakers reported that they had been targeted by a ransomware attack. The attack disrupted the companies' operations and led to a loss of data. [32]
- **SolarWinds** - In December 2020, a cyber-attack attributed to Russian state-sponsored hackers hit SolarWinds, an IT company whose software is widely used in the agricultural sector. The SolarWinds hack, which compromised multiple U.S. government agencies and private companies, also impacted the agricultural sector. The U.S. Department of Agriculture (USDA) confirmed that its National Finance Center (NFC) was one of the organisations affected by the hack.
- **JBS** -In June 2021, Meatpacker JBS, one of the world's largest meat producers, suffered a cyber-attack that caused the company to shut down its US and Australian operations. The attack was carried out by Russian hackers, and JBS had to pay a ransom of $11

million to get their systems back online. The FBI confirmed that the REvil ransomware was used in the cyberattack. The JBS hack set off a domino effect that quickly spread across the US. Wholesale meat prices soared as the balance between supply and demand immediately became out of whack. Farms and ranches could not get their animals to market, and the resulting oversupply drove wholesale prices down. Restaurants and resellers could not get processed and packaged meat. The corresponding scarcity drove consumer prices skyward. [33]

- **Attacks on Grain Cooperatives** - According to the FBI, in the fall of 2021, six grain cooperatives faced ransomware attacks. Attackers used a variety of ransomware variants, such as Conti, BlackMatter, Suncrypt, Sodinokibi and BlackByte. Some attack victims had to completely halt production, while others lost administrative functions. In February 2022, a feed milling company reported two incidents in which a malicious actor gained access to company systems and may have attempted to launch a ransomware attack. The attempts were detected and stopped before encryption occurred. More recently, in March 2022, a Lockbit 2.0 ransomware attack was unleashed against a multi-state grain company. The company provides grain processing, seed, fertiliser, and logistics services that are critical during the spring planting season.[34]
- **Crystal Valley Cooperative** - The Minnesota agricultural firm was targeted in a ransomware attack in September 2021 and was forced to take systems offline due to cybersecurity incidents. The attack left Crystal Valley unable to mix fertiliser or fulfil orders for livestock feed.[35]

Russian hackers also levelled a ransomware attack on an Iowa farming co-op in September 2021, demanding $5.9 million to unlock the computer networks used to keep food supply chains and feeding schedules on track for millions of chickens, hogs, and cattle. New Cooperative in Fort Dodge, Iowa, US, was forced to take its computer network offline to isolate the incursion and shuttered its soil-mapping software as a precaution.[36]

- **Wilmar International** - In February 2021, Singaporean agribusiness giant Wilmar International faced a malware attack originating from a North Korean sponsored hacking group called Lazarus. This attack disrupted the company's operations, but no data compromise was reported.[34]
- **Coop** - In July 2021, Swiss supermarket chain Coop experienced a major cyber-attack that caused widespread disruptions to its IT systems. The attack affected Coop's cash registers, production facilities, and warehouses, leading the company to temporarily shut down its operations.[38]

As seen in the examples of previous cyberattacks in this sector, the world's food supply chain is fragile and dominated by a relatively small number of large food companies. Because cyber threat actors aim to shut down production, thereby threatening people's lives, food production networks and food company business networks are at risk. Shutting down any massive food production or distribution business creates an intolerable condition that provides the cybercriminal with an insurmountable advantage. Companies and authorities know that they must resolve the situation quickly to avoid societal turmoil. It is imperative for companies to adopt proactive cybersecurity measures to safeguard against these threats.

Cyber Security and Smart Agriculture

Overall, agritech technologies have the potential to transform the agriculture industry by improving efficiency, sustainability, and profitability. However, the adoption of these technologies also brings new challenges and considerable cybersecurity risks.

The Agritech Threat Environment

There are several cyber risks associated with the use of technology in the agricultural sector or agritech. Here are some of the most common risks:

1. **Lack of Security Measures:** With the increasing adoption of agritech gadgets and solutions, there are increased vulnerabilities due to the lack of security measures, including improper authentication and authorization, weak passwords, and unpatched software.
2. **Internet of Things (IoT):** The use of sensors, drones, and other IoT devices in agritech has increased the attack surface for cyberattacks in agriculture. IoT devices can be exploited by attackers to gain access to sensitive data and devices.
3. **Data breaches:** With the use of internet-connected sensors, drones, and other devices in agritech, there is always a risk of data breaches. Hackers can target these devices and obtain access to sensitive information such as crop yields, animal health records, and financial information. The vast amount of agricultural data with sensitive information stored in systems can attract cybercriminals, who can exploit this data for financial gain by selling the data on the dark web.
4. **Ransomware**: Ransomware attacks involve accessing the device and encrypting the data, holding it hostage until the ransom is paid. Such an attack can cause significant financial and operational damage to an agricultural company. Ransomware attacks in agriculture can be extremely damaging, as they can result in the loss of data or the disabling of the system until the ransom is paid.
5. **Supply Chain Breaches**: Cyberattacks targeted the weakest links in the supply chain of agricultural products can disrupt the entire process and cause massive damage. Hackers targeting agritech supplier chains with weaker security can gain access to more significant data ultimately reaching their intended target.
6. **Malware**: Malware can be installed on systems that are connected to the internet in order to steal sensitive information, disrupt operations, or enable unauthorised access to the systems.
7. **Social Engineering**: Social Engineering is an attack vector that relies on the psychology of the victim, tricking them into downloading malicious software or providing sensitive information.
8. **Phishing Attacks**: Phishing scams are a common technique used by hackers to trick employees or contractors into revealing sensitive information or opening infected attachments leading to unauthorised access. Phishing scams are a frequently used tactic to trick employees into revealing sensitive data or transferring funds to an attacker's accounts.
9. **Insider Threats**: Insiders such as employees or contractors with granted access to company data and systems can cause unauthorised access, data theft, or network exploitation. Employees can exploit their privileged access within the agritech system to steal data or subvert the system.

10. **Poor password management**: Weak or common passwords can lead to unauthorised access in agricultural technology and put sensitive data at risk.

It is important to take measures to mitigate these cyber security risks by implementing security measures such as access controls, encryption, securing supply chains, and involving employees in regular cybersecurity training which will help to protect the agricultural sector from these threats.

Attacks against agriculture stakeholders of all sizes have annually increased since 2018 in proportion to the digital transformation and modernization of the sector. In Information Security, risk can often be quantified according to scenarios and impacts against mission-critical assets' confidentiality, availability, and integrity. In 2018 the US Department of Homeland Security released a report to raise awareness of 'Threats to Precision Agriculture,' which designated the top threats to confidentiality, integrity, and availability in the US Food and Agriculture sector respectively as theft of intellectual property and data, targeted disruption and data-driven attacks, and signal loss and data bandwidth limits common in rural communications networks.[39] Similarly, in 2020, the UK National Cyber Security Centre (NCSC) created a 14-page guide, 'Cyber Security for Farmers', to help educate sole traders, small to medium-sized operators, and large-scale commercial farms on cybersecurity and cyber-hygiene fundamentals.[40]

Attacks against farms and other agriculture infrastructure became more frequent in 2022 and will continue to increase as food and agriculture infrastructure modernises. However, the vast majority of targeted or opportunistic attacks can be mitigated through fundamental cybersecurity and cyber-hygiene best practices.

Cyber Threat Scenarios

The confluence of various technologies used in smart agriculture and the multitude ways in which they interact, along with the drastically increased attack surfaces that can be targeted by a variety of threat actors motivated by different goals (politics, profit, opportunity, sabotage) leads to a multitude of scenarios requiring contemplation. The technologies and threat scenarios detailed next are by no means meant to be a comprehensive list but should provide a good indication of the breadth and type of cyber-attacks that need to be considered for adequate protection.

Leaking of Confidential Farm Data

Companies such as farm consultancies, farm advisors, agrichemical firms and Original Equipment Manufacturers (OEMs) maintain databases containing information about farms. These can contain sensitive information about yield quantities and prices, costs of agrichemicals, feed and equipment, livestock and crop health and pesticide use. Leaking of this confidential data could occur due to an insider attack leading to theft and publishing of data, accidental public exposure by a company or a deliberate outsider attack on the network of a company hosting an agricultural database. While a number of motivations for an attack exist, specific reasons include:

- Animal welfare activists wishing to 'expose' evidence of abuse,

- Misuse of data, for example to understand potential market drivers or to identify struggling farms with underutilised land that could be bought at lower than the standard market price.

Loss of Availability of Distribution and Storage Systems

Food storage and distribution relies on various technologies to achieve a Just-in-Time system and meet food standards. While the network is tolerant to the loss of individual assets, the loss of availability of key IT systems for a large distributor would likely have a significant impact because any non-digital fall-back system would be unable to achieve an equivalent level of performance. The type of technologies that could be targeted include:

- Loss of HVAC systems in storage warehouses,
- Loss of SCADA systems, such as equipment used to move goods,
- Loss of availability or integrity of logistics software,
- Remote immobilisation of distribution vehicles (e.g. via telemetry systems).

While a number of motivations exist, specific reasons include:

- Targeting of live transportation of poultry by 'extreme' animal welfare activists who believe that animals are better off dead than living in a farmed environment. As poultry transportation relies on forward movement of the vehicle to provide ventilation, immobilisation of the vehicle over a sufficient period can lead to death of animals via overheating or asphyxiation,
- Nation-state attacks to economically and socially weaken another state,
- Organised criminal gangs manipulating markets by influencing the share price of publicly listed companies.

Loss of Availability of Processing Systems

Food processors can use automated SCADA systems on their production lines, which are often exposed to the internet. These systems are vulnerable to cyber-attacks. While a number of motivations exist, specific reasons include:

- Targeting of meat and poultry abattoirs by animal welfare activists wanting to cause financial and reputational harm,
- Ransomware attacks by cyber criminals.

The loss of a facility's production system in a food sub-sector dominated by a few large companies could result in high financial harm to the affected company and the farms that supply it.

Compromised Integrity of Food Assurance Systems

Several of the food assurance systems have web portal interfaces to databases that allow users to view or submit information relating to the movement of livestock, food and animal products, and accreditation of organisations within the food network. Specific motivations include:

- Targeting of livestock farms and meat and poultry processors by animal welfare activists. This could be by direct financial harm to the victims or by attempting to change

consumer habits by undermining consumer confidence in meat and poultry safety or animal welfare standards,
- Exposure of the falsification of records by unscrupulous processors, who may be attempting to profit through non-conformance to food standards,
- Nation-state attacks intending to economically and socially weaken another state.

A cyber-attack on the integrity of the food assurance systems could undermine consumer confidence, which would have a high financial impact on food companies and potentially a significant impact to the wider economy.

Farm Management Software

Farm management software aids the farmer in managing and optimising the operations of a farm. It provides functionality such as traceability, insight and means to improve profitability, and tracking and monitoring of farm workers and assets. The software can run on a PC, tablet, or phone, and can be hosted locally or in the cloud. Some software packages can interface directly with industry portals such as BCMS and ARAMS, and services from farm advisors, agronomic firms, and satellite service providers (e.g. Landsat). They can integrate with precision agriculture devices such as Unmanned Air Systems (UAS), weather stations and other remote sensors. A cyber-attack could result in the following scenarios:

- Leaking of confidential data that puts the business at a competitive disadvantage
- Leaking of confidential data that is misused by prospectors wishing to buy underperforming land at below market price
- Leaking of confidential data that aids organised criminal gangs in stealing farm assets
- Loss of integrity resulting in financial loss due to reduced yields or production efficiency, putting the business at a competitive disadvantage
- Loss of availability resulting in financial loss due to reduced yields or production efficiency. This would likely only have a limited effect on an individual farm, with fresh produce being at higher risk due to smaller harvesting windows. Attacking multiple users via software updates or a cloud hosting platform would magnify the impact, which could motivate cyber criminals to target service providers with ransomware-type attacks.

Agricultural Ground Vehicles

There are a wide range of farm vehicles, with the more common types broadly categorised as follows:

- Tractors and implements
- Harvesters
- Sprayers
- Telescopic handlers
- All-terrain vehicles
- Farm robots

Modern farm vehicles contain networked digital microcontrollers, making use of automotive standard Electronic Control Units (ECUs) linked with Controller Area Network (CAN) buses. Farm vehicles can be equipped with autosteer, which uses Global Navigation Satellite Systems(GNSS) to autonomously control the direction of travel. There are a number

of attack surfaces that could be exploited in order to carry out a cyber-attack. The high levels of momentum and traction of these vehicles can result in catastrophic collisions with people or other assets. While a number of motivations exist, specific reasons include:

- Terrorism – attacking buildings and roads to cause injury, death, and destruction,
- Nation-state attacks against the electrical power CNI assets, with power pylons and electrical substations in and around farmland potentially targeted.

Modern farm vehicles can come equipped with telematics units, which send diagnostic and usage data to the OEM but can also include harvester yields and geo-location. A common use case for this functionality is to provide diagnostic alerts to the OEM for servicing. The telematics systems on some vehicles are capable of sending control commands to the vehicle to enable remote deactivation or to optimise combine thresher settings. A cyber-attack could result in the following scenarios:

- Leakage of telematics data leading to the disclosure of confidential information on production efficiency, crop health and yields, which puts the farm at a competitive disadvantage,
- Unauthorised access to the telemetry system allowing an attacker to command sub-optimal combine harvester thresher settings. This could result in reduced yields and loss of income to the farmer, putting them at a competitive disadvantage. It is likely that the operator would notice yields that are significantly lower than expected, but with a limited harvesting window, the ability to rectify this within sufficient time may be limited,
- A malicious script being planted on an ECU that provides malicious commands to the throttle and auto-steer,
- A ransomware attack carried out by an organised criminal gang, leading to the installation of malicious ECU software update that 'bricks' the ECU, immobilising the farm vehicle. This would require a replacement ECU to be fitted in order to return the vehicle to service. The severity, and likelihood of a ransom being paid would increase if timed to occur during a critical period in the season, such as during the harvest window.

Remote Connected Sensors

Remote connected sensors typically fall within two categories:

- Agronomic sensors
- Livestock sensors

Agronomic sensors include typical weather station measurements such as air pressure, temperature and humidity, wind speed and direction, and rainfall. They can also measure soil moisture, temperature and salinity, leaf wetness and solar radiation. Moisture sensors are more common on fresh produce farms, where irrigation may be required. These sensors can utilise different wireless standards including ZigBee, LoRaWAN and 2G/3G/4G mobile networks. Livestock sensors are typically limited to dairy herds due to equipment costs, used to monitor feeding, rumen health, lameness, oestrus, and calving. Leg-mounted pedometer sensors can provide further insight into animal health and activity. Cyber-attack scenarios that could be of significant severity are:

- Loss of integrity of animal sensors so that they provide inaccurate oestrus information. This could result in missed breeding cycles, with financial impact on a farm. Motivations

include manipulation of the market by cyber criminals and animal welfare activists wishing to financially harm the livestock industry,
- Loss of integrity of moisture sensors, resulting in inadequate irrigation of fresh produce and reduced yields, which puts the farm at a competitive disadvantage.

Livestock Farming Infrastructure

The level of digitisation of livestock farms is lower than for crop farms but there is still a diverse mixture of technologies in use within the infrastructure. These can be broadly categorised into the following:

- Feeding
- Milking
- Segregation gates
- Animal monitoring
- HVAC

Cyber-attack scenarios of significant severity include:

- Unauthorised access to IP cameras, enabling criminal gangs to plan and time theft of farm assets for maximum success. Malicious disabling of IP cameras would reduce the likelihood of thieves being apprehended,
- Loss of integrity of automatic milking parlours, resulting in incorrect dumping of milk by the milking machine, contamination of the milk storage vessel with cleaning product or spoiling of milk through incorrect refrigeration settings, which would impact yields and competitiveness of the farm,
- Loss of availability of automatic milking parlours resulting in an inability to milk cows and cows drying off, leading to significant financial harm to dairy farms. Dairy farms or OEMs could be targeted with a ransomware-type attack by cyber criminals or by animal rights activists,
- Loss of integrity or availability of HVAC systems, leading to large losses of poultry or pigs, particularly if targeted on a hot day, resulting in significant financial harm to farms. Farms could be targeted with ransomware-type attacks by cyber criminals or by extreme animal rights activists.

Aquaculture Infrastructure

While the application of science in aquaculture is advanced, there is only limited digitisation of the farming processes. The types of technologies used include:

- Environmental control
- Feeding
- Fish grading
- Vaccination

The amount of environmental control depends on the type of farming – Recirculatory Aquaculture Systems (RAS) are the most sophisticated, controlling acidity, oxygenation, temperature, lighting, and ammonia levels. The vaccination of larger fish can be performed automatically, with commercial solutions using vision systems. The various aquaculture equipment can be monitored by a single software solution or implemented as a SCADA

system. A loss of integrity or availability of the environmental control systems on a RAS farm is the most obvious threat scenario. This could lead to reduced yields or a large loss of animals, causing significant financial harm to the farm. They may be targeted by a ransomware-type attack by cyber criminals, extreme animal rights activists or wild fishery farmers that blame aquacultures for spreading lice and genetic introgression within their stock.[41]

Confidentiality, Availability, and Integrity (CIA)

The cyber threat will increase in severity and likelihood as new technologies are adopted by the agri-food sector. Not only should we be preparing for this growing cyber threat in order to protect the day-to-day functioning of the food industry but also to ensure that they do not delay the adoption of technologies that are urgently needed by mankind. Adhering to the CIA principles is a key part of effective cybersecurity practices in agritech, and any violation to them can result in major cybersecurity incidents such as data breaches, system outages, and reputational damage to the company. As a result, adopting these principles can help to mitigate risks and ensure smooth operation in agritech.

Confidentiality, Availability, and Integrity (CIA) are three key information security principles that are critical in ensuring the safety of data and systems in agritech. These principles help to safeguard sensitive data, minimise risk, and ensure systems remain secure and operational.

1. **Confidentiality** - This principle is concerned with protecting sensitive data from unauthorised access, modification, or deletion. This means that agritech companies should ensure that data are only accessed by authorised personnel and use strong access control and encryption techniques to safeguard sensitive data such as financial records, customer personal information, and research data. Keeping data private is essential to farms and other businesses that engage in precision agriculture to increase crop output. Yield data, farming methods and other proprietary information are vital to remaining competitive.
2. **Availability** - This principle ensures that data and systems are always available to authorised personnel when needed. In agritech, availability is particularly important since delays or disruptions can have massive consequences on supply chain management, crop yields, and livestock welfare. The compromise of farm equipment communication and guidance systems could lead to problems tending crops and livestock on a timely basis. Infrastructure designed to maintain availability could include backup power generators, redundancy in internet connectivity, compute resources, data storage facilities, and disaster recovery plans.
3. **Integrity** - This principle ensures that data and systems are accurate and maintain their intended state. It's essential to protect sensitive data from modification or deletion by third-party unauthorised access. Data collection and analysis helps farmers make decisions that impact food supply at the local, regional, or national level. Any lost or adulterated data could lead to significant downstream disruption. Agritech companies can maintain data integrity by deploying access control measures and system permissions, verifying data inputs and outputs, using robust anti-malware solutions, and gradually monitoring data and file changes on a regular basis.

The Fundamentals of Agritech Cyber Security

Agritech cyber security refers to the measures and practices that are put in place to protect the technology and data used in the agriculture industry from cyber threats. The agriculture industry is increasingly reliant on technology, from precision agriculture to supply chain management, and the data generated by these technologies can be valuable to cyber criminals. The food and farming industry is vulnerable to cyber-attacks because it heavily relies on digital technology for various processes such as inventory management, logistics, and distribution. These systems are interconnected, and a compromise in one system can lead to a security breach in the entire network. Effective agritech cyber security requires a comprehensive approach that addresses the unique risks and challenges faced by the industry. Here are some key considerations for agritech cyber security:

1. **Risk Assessment**: A thorough risk assessment is critical for identifying and addressing potential vulnerabilities in an agritech system. This assessment should include an analysis of the data being collected, how it is being stored, and who has access to it.
2. **Security Controls**: Implementing appropriate security controls is essential to protect against cyber threats. This can include measures such as firewalls, intrusion detection systems, and multi-factor authentication.
3. **Employee Training**: Cybersecurity is a shared responsibility, and employees play a critical role in maintaining a secure system. Training employees on cybersecurity best practices, such as how to recognize phishing emails, can help reduce the risk of a cyber-attack.
4. **Data Encryption**: Encryption can help protect sensitive data from cyber criminals. Data encryption should be used for data at rest and in transit.
5. **Incident Response**: Having a plan in place for responding to a cyber-attack is critical for minimising the impact of a breach. This plan should include procedures for identifying and containing the attack, as well as steps for recovery and remediation.
6. **Third-party Risk Management:** Third-party vendors and contractors can pose a risk to agritech systems. It is important to vet third-party vendors thoroughly and ensure that they adhere to appropriate security practices.

Overall, effective agritech cyber security requires a holistic approach that addresses the unique risks and challenges faced by the industry. By implementing appropriate security measures and procedures, agritech companies can help protect themselves from cyber threats and minimise the risk of a data breach or cyber-attack.

How Snode Can Help

Snode Technologies can provide cybersecurity services to agricultural technology companies or agritech. Companies in this sector need to be vigilant about the security risks of their technology solutions and customer data, making cybersecurity essential to their continued growth and success. Snode's cybersecurity services can help agritech companies detect, monitor, and mitigate cyber threats that could affect their operations. Some of the areas where Snode's cybersecurity solutions can be applied in Agri-tech include:

1. **IoT devices** - These devices can be vulnerable to cyber-attacks, especially when they lack proper authentication and authorization. Snode's machine learning algorithms can detect anomalous behaviour in IoT networks that may indicate an intrusion attempt. Snode's machine learning algorithms detect anomalous behaviour through the use of AI engines, analysing both network and endpoint logs.
2. **Cloud Applications** - Cloud applications have become a popular platform for agritech solutions, which can be vulnerable to attacks, either from external or internal threats. Snode's advanced threat detection and response techniques can help agritech companies protect their cloud infrastructure. Snode provides a rapid response team to ensure operational continuity in the event of a disruption or breach.
3. **Data security** - Agritech companies also need to protect their sensitive data, including crop yields, soil nutrient data, financial records, and customer personal information. Snode's threat monitoring can detect and respond to data breaches and attacks on sensitive company information. Snode provides continuous monitoring, detection, and response to cyber threats proactively through a combination of advanced technologies and human expertise.
4. **Supply Chain Management** - The agricultural industry relies heavily on complex supply chains that can become a possible occasion susceptible to cybercriminals. Snode can monitor and identify suspicious communication attempts leading to supply chain disruption or sabotage.
5. **Risk Management** - Snode can provide agritech companies a risk assessment to build and implement a cybersecurity framework to mitigate potential negative outcomes. Snode works with clients to understand their exposure to cybersecurity risks, evaluate the level of risk, and develop a plan to manage it.

By providing these cybersecurity services, Snode can help agritech organisations protect their data, systems, and operations from cyber threats, enabling them to focus on their core business of developing innovative technology solutions to improve agriculture practices.

Just as fences need to be erected around cattle and sheep as a protective perimeter, IoT and other networked devices, servers and websites need to be protected. Weather events like droughts or floods can heavily affect the results of any agribusiness. Innovations in technology such as the Internet of Things (IoT), smart sensors and self-driving machinery have helped to reduce that impact by making operations more efficient and cost-effective. However, with great technology comes great risk. To prevent cyber-attacks, the food and farming industry should prioritise the security of their digital infrastructure. This can be done by implementing measures such as firewalls, intrusion detection systems, and regular system updates. Additionally, it is essential to train employees on cybersecurity best practices and to conduct regular risk assessments. In the event of a cyber-attack, it is

important to have a response plan in place to minimise the damage. This includes having backups of critical data, isolating infected systems, and notifying relevant authorities.

As these technologies become more internet-connected, the opportunity for hackers to use these connections for malicious purposes increases and it is essential that cyber security measures are implemented and prioritised to meet these threats.

About Snode Technologies

Snode Technologies is a cyber defense company, operating out of Centurion, South Africa. Snode's defense model consists of people, processes, and expert technologies to provide superior real-time threat detection.

Snode's Guardian platform offers cyber threat intelligence empowering informed, data-driven, risk-based decision-making. It encompasses:

- Breach intelligence – insight into what attackers do once inside, how customer security controls fail
- Machine intelligence – with 80 global points of presence, thousands of malicious events per hour are collated
- Operational intelligence – experts validate alerts, and the continuous monitoring provides a unique perspective on identifying emerging global threats within specific industry verticals
- Adversary intelligence – intelligence analysts are entrenched within the mindset of an attacker and offer clients visibility into motives and trends

Our technology is next generation breach detection, offering real-time, contextual behavioural analytics to monitor and identify suspicious behaviour.

Authors

Nithen Naidoo

CEO and Founder of Snode Technologies

Nithen Naidoo is the CEO and founder of Snode Technologies. As a cyber security evangelist, with over 20 years of experience, Nithen provides cyber defence solutions globally, and most recently was recognised by the prestigious AfricArena tech accelerator as an Emerg-ing Entrepreneur of 2021. Nithen is also a sought-after public speaker.

Neeshal Munga

Information Security Specialist

Neeshal is an Information Security specialist proficient in IT industry best practices and compliance guidelines. With 13 years of related experience working on various research projects, she has expertise in various areas of Information Security and IT, covering a broad range of areas including: Open-Source Software (OSS), Open-Source Business Models, Information Security (specifically Risk Management and Controls, Computer Security Incident/Emergency Response Teams (CSIRTs/CERTs), Security Policies, Social Network Security, and OSS Security).

References

[1] NCC Group. "Cyber Security in UK Agriculture". 2020, https://research.nccgroup.com/wp-content/uploads/2020/07/agriculture-whitepaper-final-online.pdf.

[2] Abbasi, Rabiya, et al. "The Digitization of Agricultural Industry – a Systematic Literature Review on Agriculture 4.0." Smart Agricultural Technology, vol. 2, Dec. 2022, p. 100042.

[3] Cropin. *"Building Climate Resilience and Adaptation with Agritech"*. 15 July 2019, https://www.cropin.com/blogs/agriculture-technology-is-transforming-the-way-we-counter-climate-change.

[4] Rettore De Araujo Zanella, Angelita, et al. "Security Challenges to Smart Agriculture: Current State, Key Issues, and Future Directions." *Array*, vol. 8, Dec. 2020, p. 100048.

[5] Nations, United. "The Impact of Digital Technologies." United Nations, https://www.un.org/en/un75/impact-digital-technologies. Accessed March 2023.

[6] Aceto, Giuseppe, et al. "A Survey on Information and Communication Technologies for Industry 4.0: State-of-the-Art, Taxonomies, Perspectives, and Challenges." *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, 2019, pp. 3467–501.

[7] Demestichas, Konstantinos, et al. "Survey on Security Threats in Agricultural IoT and Smart Farming." *Sensors*, vol. 20, no. 22, Nov. 2020, p. 6458.

[8] "The Internet of Cows: How AgriTech Is Tearing up the Rules of Food." *Vodafone.Com*, https://www.vodafone.com/news/technology/the_internet_of_cows. Accessed 16 Mar. 2023.

[9] *Agritech Market Size & Share Report, 2021-2028*. https://www.adroitmarketresearch.com/industry-reports/agritech-market. Accessed 16 Mar. 2023.

[10] Research, Straits. "Precision Agriculture Market Size Is Projected to Reach USD 19.24 Billion by 2030, Growing at a CAGR of 14.95%: Straits Research." *GlobeNewswire News Room*, 1 Aug. 2022, https://www.globenewswire.com/en/news-release/2022/08/01/2489650/0/en/Precision-Agriculture-Market-Size-is-projected-to-reach-USD-19-24-Billion-by-2030-growing-at-a-CAGR-of-14-95-Straits-Research.html.

[11] Smart Farming And Its Technologies Application In Agriculture. 21 Oct. 2022, https://eos.com/blog/smart-farming/.

[12] Saiz-Rubio, Verónica, and Francisco Rovira-Más. "From Smart Farming towards Agriculture 5.0: A Review on Crop Data Management." *Agronomy*, vol. 10, no. 2, Feb. 2020, p. 207.

[13] Smart Farming And Its Technologies Application In Agriculture. 21 Oct. 2022, https://eos.com/blog/smart-farming/.

[14] Wired, Industry. "Top 6 Use Cases of Drones Changing the Modern Society." *Industry Wired*, 1 Feb. 2020, https://industrywired.com/top-6-use-cases-of-drones-changing-the-modern-society/.

[15] Agricultural Technology For New & Advanced Farming Solutions. 16 Mar. 2023, https://eos.com/blog/agricultural-technology/.

[16] Prabhugaonkar, Akhilesh. "3 Types of Agricultural Robots That Are Improving Global Productivity." *Robotics 24/7*, https://www.robotics247.com/article/3_agricultural_robots_types_improving_global_productivity. Accessed April 2023.

[17] Pearson, Simon, et al. "Robotics and Autonomous Systems for Net Zero Agriculture." Current Robotics Reports, vol. 3, no. 2, June 2022, pp. 57–64. Springer Link, https://doi.org/10.1007/s43154-022-00077-6.
[18] Gonzalez, Wendy. "Council Post: How AI Is Cropping Up In The Agriculture Industry." Forbes, https://www.forbes.com/sites/forbesbusinesscouncil/2023/02/02/how-ai-is-cropping-up-in-the-agriculture-industry/. Accessed 4 May 2023.
[19] Drzaic, Ana. "What Is Agri Big Data Analytics and Why It Matters." Proagrica, 1 Oct. 2020, https://proagrica.com/news/what-is-agri-big-data-analytics-and-why-it-matters/.
[20] "Significance of Big Data in Farming." KG2, 4 May 2022, https://kg2.com.au/significance-of-big-data-in-farming/.
[21] Research, GlobalData Thematic. "Agriculture Technology Is More Accessible through the Cloud." Verdict, 30 Jan. 2023, https://www.verdict.co.uk/agriculture-cloud-technology/.
[22] Cloud Computing for Agriculture Application | Frontiers Research Topic. https://www.frontiersin.org/research-topics/40358/cloud-computing-for-agriculture-application. Accessed April 2023.
[23] Smart Farming And Its Technologies Application In Agriculture. 21 Oct. 2022, https://eos.com/blog/smart-farming/.
[24] Tractor Hacking a Case to Increase Cyber Security in Agtech. https://www.bdo.com.au/en-au/insights/food-agribusiness/articles/cyber-security-must-be-prioritised-in-australia-s-agricultural-sector-following-viral-tractor-hack. Accessed April 2023.
[25] Paganini, Pierluigi. "Distributor of Asian Food JFC International Hit by Ransomware." Security Affairs, 2 Mar. 2021, https://securityaffairs.com/115150/malware/jfc-international-ransomware-attack.html.
[26] "Blackbaud Security Incident." Loaves & Fishes Food Pantry, 20 Aug. 2020, https://loavesandfishes.org/blackbaud-security-incident/.
[27] Whittaker, Zack. "Home Chef Confirms 8 Million User Records Stolen in Breach." TechCrunch, 20 May 2020, https://techcrunch.com/2020/05/20/home-chef-data-breach/.
[28] Cyware Labs. "REvil Ransomware Targeted Sanitary Components Supplier | Cyware Hacker News." Cyware Labs, http://cyware.com/news/revil-ransomware-targeted-sanitary-components-supplier-e2a41c63. Accessed April 2023.
[29] "Brazil Agriculture—Response and Resilience of Food Security under Dual Shocks in 2020: Oil Price Collapse and the COVID-19 Pandemic." Policy Center, https://www.policycenter.ma/publications/brazil-agriculture-response-and-resilience-food-security-under-dual-shocks-2020-oil. Accessed 4 May 2023.
[30] Nanda, Prashant K. "Cyberattacks Surged 3-Fold to 1.16 Mn Last Year in India." Mint, 23 Mar. 2021, https://www.livemint.com/news/india/as-tech-adoption-grew-india-faced-11-58-lakh-cyberattacks-in-2020-11616492755651.html.
[31] "Fonterra Targeted by Hackers." NZ Herald, 4 May 2023, https://www.nzherald.co.nz/business/fonterra-targeted-by-hackers/6PEVEZEO5AI6O2W2RS7HJ6WMTM/.
[32] Kirby, Steven. "Incident: Taylor's Winery Targeted By Hackers | 5AU 97.9." Australian Information Security Awareness and Advisory, 31 Mar. 2021, http://kirbyidau.com/2021/03/31/incident-taylors-winery-targeted-by-hackers-5au-97-9/.

[33] Bunge, Jacob. "Meat Buyers Scramble After Cyberattack Hobbles JBS." Wall Street Journal, 1 June 2021. www.wsj.com, https://www.wsj.com/articles/meatpacker-jbs-hit-by-cyberattack-affecting-north-american-australian-operations-11622548864.
[34] "Ransomware Attacks on Agriculture Potentially Timed to Critical Seasons." Security Intelligence, https://securityintelligence.com/news/ransomware-attacks-agriculture/. Accessed April 2023.
[35] Crystal Valley Farm Coop Hit with Ransomware. 22 Sept. 2021, https://threatpost.com/crystal-valley-farm-coop-hit-with-ransomware/174928/.
[36] Bogage, Jacob, and Laura Reiley. "Russian Hackers Target Iowa Grain Co-Op in $5.9 Million Ransomware Attack." Washington Post, 22 Sept. 2021. www.washingtonpost.com, https://www.washingtonpost.com/business/2021/09/21/new-cooperative-hack-ransomware/.
[37] Reporter, Staff. "80% of Organisations Experienced Ransomware Attacks in 2021." Singapore Business Review, 13 Apr. 2022, https://sbr.com.sg/news/80-organisations-experienced-ransomware-attacks-in-2021.
[38] "Major Swedish supermarket chain hit by cyberattack" The Local, https://www.thelocal.se/20210703/major-swedish-supermarket-chain-hit-by-cyberattack . Accessed April 2023.
[39] cyberagmin. "Future Food Security Depends on Modern Security Controls." CyberAgTM, 27 Jan. 2023, https://cyberag.org/2023/01/future-food-security-depends-on-modern-security-controls/.
[40] Cyber Security for Farmers. https://www.ncsc.gov.uk/guidance/cyber-security-for-farmers. Accessed April 2023.
[41] "Staying Secure in a Changing Agricultural Landscape." Mynewsdesk, 5 Sept. 2019, https://newsroom.nccgroup.com/news/staying-secure-in-a-changing-agricultural-landscape-388411.

Snode

www.snode.com

info@snode.com

+27 12 880 0989