CASE STUDY

Detect, Respond, Deliver – The Greenery's fresh take on cybersecurity

The Greenery is an international fruit and vegetable company which supplies and distributes fresh produce to supermarkets, wholesalers, caterers and the processing industry year-round. Their value chain includes growers, logistics, marketing, and retail, ensuring a seamless process from farm to consumer.

The company has been in operation since 1996 and its headquarters are located in Barendrecht, the Netherlands. The Greenery is owned by the Coöperatie The Greenery.

HUNT & HACKETT

The Challenge

Imagine the scene: trucks at a standstill outside the distribution center, fruit and vegetables piled high in containers, softening and spoiling, and empty shelves in the supermarket. This is the harsh reality when a ransomware attack hits the food supply chain.

Every organization wants to avoid operational downtime, but in the world of fresh produce, where products must be delivered at precise intervals, the effects of any sort of disruption are especially acute. The perishability of the food, coupled with the sector's typically low profit margins, means most businesses would struggle to survive an outage lasting more than a few days. The Greenery is no exception.

> "We can manage one day [of downtime], maybe two days. But it will become very difficult if the whole company is shut down for three days or more. Then we have a lot of challenges, and we might not survive. That's the reality of the business we're involved in."
>
> *-Dennis Baaten, Security Officer*

Companies like The Greenery, who work across the entire food supply chain, are bound to strict delivery deadlines and food safety standards.

Any failure to adhere to these can result in reputational damage, penalties, and broad financial losses. Consequently, these companies are seen as attractive targets by cybercriminals aiming to leverage and exploit these vulnerabilities.

Ransomware is an especially popular tool used against businesses because it encrypts critical data and systems, bringing operations to a grinding halt. Given the time-sensitive nature of the fresh produce sector, companies are often incentivized to pay the ransom quickly to avoid catastrophic losses, making them prime targets for extortion.

Recognizing this risk, The Greenery set out to enact measures that would protect the business in the event of an attack. They selected Hunt & Hackett as their security partner in December 2022, opting for the Managed Detection and Response (**MDR**) and Incident Response Retainer (**IRR**) services.

"At a certain point, you see all these risks and threats in the outside world, and you start wondering what the next best step is for The Greenery to mature even further," says Baaten.

"We concluded that if we are serious about increasing our security level, we would have to do active threat monitoring and response."

Moving from reactive to proactive Managed Detection & Response (MDR)

Before partnering with Hunt & Hackett, The Greenery was working with a different managed service provider whose performance had fallen below expectations. Instead of providing real-time threat monitoring and response, the provider retroactively reported suspicious activity, sometimes a month after it was first observed.

“It eventually became more of an auditing service than a security-oriented service,” says Ferry Niemeijer, IT Manager at The Greenery.

“We would receive reports about suspicious activity seen 30 days beforehand. We really weren't happy with that way of working. We increasingly felt exposed despite our investment is the MDR service; we wanted a more proactive security partner.”

Another element putting the relationship under strain was the lack of input from their provider when making important choices. The Greenery’s security team was asked to determine their own monitoring priorities without being given any guidance or context to inform their decisions.

“We could select 20 use cases that the security service would monitor for, and more cases would cost extra. And I thought, okay, but that's not what I want,” says Dennis Baaten, Security Officer.

“That's actually terrible. Because how can I know what the biggest threats are? That is information and guidance that I expect from my security partner.”

Without any direction, The Greenery was left to narrow down a long list of use cases, sparking protracted deliberations with no clear path forward.

“It's an endless discussion. You can never win this battle because it's just the wrong approach,” adds Baaten.

Shopping for a security partner

The Greenery knew they wanted a cybersecurity partner with expertise they didn’t have in-house, and not just a “service desk forwarding tickets.” When they began their search, they created a list of criteria to guide their selection.

Central to The Greenery’s requirements was the ability to use **threat intelligence** to identify the biggest risks facing the company, allowing them to prioritise their efforts and allocate resources more effectively. They wanted the security partner to determine the threat monitoring and response priorities, unburdening the in-house team from making critical decisions without the right information.

They also hoped to find a solution that would utilise their previous security-related technology investments, such as the use of Microsoft Defender for Endpoint.

The Greenery’s Requirements	Hunt & Hackett’s Proposition
The **security partner determines the detection rules** and use cases based on their own intelligence and rule set	Hunt & Hackett looks at The Greenery’s threat landscape and determines the TTPs and tools that relevant threat actors are using. This information is translated into preventive security controls, data sources, detection logic, and response playbooks.
The **cost** of the service is **predictable**	Hunt & Hackett uses Google Chronicle as a core technology in the MDR service. Chronicle’s employee-based pricing model ensures cost predictability, unlike the data ingestion model typical of other SIEM solutions.
The partner has **security as its core business**	Hunt & Hackett’s team members are experts in cybersecurity. They regularly provide Incident Response and crisis management services to customers who have been hacked (eg. espionage, ransomware, data theft, Business Email Compromise attacks). Learnings from these cases are then applied to the MDR service.
Dutch-speaking company with the capacity to provide **on-premises support** in the event of an incident in **less than four hours**	Hunt & Hackett is a Dutch company. Therefore, communications can take place in Dutch or English, depending on the preferences of each individual partner. Hunt & Hackett’s incident handlers provide timely on-premises support when an incident occurs.
Technology agnostic and ability to work with Microsoft Defender for Endpoint	Hunt & Hackett’s offering is, to a large extent, technology agnostic, meaning clients’ existing technology investments can still be utilized. Hunt & Hackett operates with all leading EDRs, with many of their customers having deployed Microsoft Defender for Endpoint as part of their E3 or E5 licenses.

The Solution

The Greenery ultimately selected Hunt & Hackett as its security partner due to its unique proposition and approach.

“It was so refreshing to speak with Hunt & Hackett because they have a good philosophy on security. It was clear they are specialists and wanted to do things differently than other parties”, says Ferry Niemeijer, IT Manager.

Hunt & Hackett provides tailored MDR services that take an organization’s specific requirements, risk profile and threat landscape into account. By working with Hunt & Hackett, The Greenery gained insights into *who* their adversaries are, *how* they are vulnerable, and *what could be done* to protect their business.

“Before we had the MDR service of Hunt & Hackett, we didn't really know what was going on. Now I feel reassured that if something is happening, we’ll probably see it. We may not be able to entirely prevent it from happening, but we will at least have a fighting chance to do something about it”

-Dennis Baaten, Security Officer

The MDR service is delivered through a dedicated **Security Operations Centre** (SOC) which provides 24/7 monitoring of The Greenery’s IT environment.

Implementing MDR

During the implementation, Hunt & Hackett’s onboarding team appraised The Greenery’s threat landscape and translated this into specific attack methods that would need to be detected. This helps to determine which data sources, technology, and detection logic are required to cover the relevant threats.

After the handover to the SOC, the detection engineering team takes over the maintenance of this process to ensure the detection logic is continuously updated to address relevant threats.

“I wouldn’t think of going to another security service provider, ever.”

-Ferry Niemeijer, IT Manager

Managed Detection & Response (MDR)

Hunt & Hackett's cloud-native MDR service combines threat intelligence, forensic analytics directly from the SOC, and human expertise to protect organizations against (advanced) cyberattacks. The MDR platform integrates various technologies, such as Security Orchestration Automation & Response (**SOAR**), Endpoint Detection & Response (**EDR**), Security Information Event Management (**SIEM**), Honeypots and tokens. It also takes security telemetry data from network devices such as firewalls and routers. This ensures real-time visibility over an organization’s IT environment, allowing the appropriate action to be taken quickly when suspicious or malicious activity is detected.

Looking for an MDR provider? Read the MDR Buyers Guide.

Price predictability

A key differentiator in Hunt & Hackett's offering is the use of Google Chronicle as its SIEM, a core technology underpinning the MDR service.

Unlike traditional MDR solutions, that operate on a variable price model based on data volume ingestion (e.g. Microsoft Sentinel, Splunk, Palo Alto Cortex), Chronicle operates on a fixed, employee-based model. This allows for the ingestion, analysis, and storage of massive datasets and security telemetry without additional costs. In turn, this incentivizes customers to provide all the relevant data needed for real-time monitoring, detection, and response, reducing the chance that malicious activities will be missed and supporting forensic readiness requirements laid out in the NIS2 Directive.

"It was important to us that the cost of the service was predictable. When the cost is determined by the amount of data you send to your security partner, you might restrict the amount because it saves money. This directly contradicts the objective of reducing risks, as less security telemetry data also means less visibility and resilience. From a security perspective, you want to be able to send all the information that is required, to be as safe as possible."

-Ferry Niemeijer, IT Manager

Google Chronicle

With the ability to ingest, process and store vast amounts of data, Chronicle enables superior real-time detection capabilities and supports in-depth investigations when security events and incidents occur.

Hunt & Hackett leverages this extensive security log & telemetry data to create and fine-tune detection systems, rules, and processes tailored to The Greenery's specific threat landscape, allowing them to achieve comprehensive threat coverage in a cost-effective manner.

Learn more here.

NIS2 compliance

As a key player in the fresh produce sector, The Greenery is regarded as an 'Important entity' under the NIS2 Directive. NIS2 aims to strengthen cybersecurity practices across the EU by introducing several key changes. Among these, the Directive introduces significantly shorter incident reporting timelines, meaning organizations must submit incident-specific information to the national regulator much more quickly than before.

These new requirements necessitate on-demand incident response capabilities and the ability to perform root cause analysis when a cybersecurity related incident occurs.

With Hunt & Hackett's **Incident Response Retainer**, The Greenery could rest assured that around-the-clock assistance was available in the event of a cyberattack. The retainer ensures that as soon as malicious activities are detected, Hunt & Hackett's dedicated CERT team springs into action to investigate, contain, and resolve the incident.

This is also relevant for cases where the Greenery isn't directly affected, but one of their supply chain partners is. How do you manage the risks and get back to business-as-usual? Such questions can arise and are covered under the Retainer service.

The service is supported by an innovative cloud-based Incident Response lab which enables rapid data acquisition and processing, meaning investigations can be conducted more efficiently than with traditional (manual) methods.

By opting for the IR Retainer in combination with MDR, The Greenery ensured its prevention, detection, and response capabilities were aligned and functioning as a single, comprehensive system. This approach not only ensures compliance but also significantly enhances the company's resilience to a range of cyber threats.

Creating a roadmap

During the MDR implementation period, The Greenery was supported with a complementary Security Program Gap Assessment (**SPGA**) to assess gaps in the organization's defenses. This knowledge was then translated into a cybersecurity roadmap aimed at increasing The Greenery's resilience over time.

"The gap analysis helped us with structuring the work that needs to be done. We've already completed the short-term projects, we're working on the midterm now, and long -term will follow," says Niemeijer.

"It came at exactly the right time because there was really a large impulse in the organization to prioritize again and focus on the things that matter most," adds Baaten.

Security Program Gap Assessment

Hunt & Hackett's Security Program Gap Assessment (SPGA) provides detailed insights into an organization's threat landscape, as well as any potential security gaps that could be exploited by threat actors. This information is translated into security controls and used to define the organization's cybersecurity roadmap. Learn more here

The Results

- **[Threat visibility]:** The Greenery achieved real-time visibility into its digital environment through the implementation of MDR.
- **[Cybersecurity roadmap]:** The Security Programme Gap Assessment provided an overview of the company's individual threat landscape and the gaps in the company's defences, enabling the creation of a cybersecurity roadmap that builds cyber maturity and resilience over time.
- **[Forensic Readiness]:** Hunt & Hackett's Google Chronicle solution allowed The Greenery to collect and store massive amounts of security telemetry data, ensuring NIS2-required forensic readiness without the prohibitive variable costs associated with other SIEM solutions.
- **[Utilise previous investments]:** Hunt & Hackett's technology-agnostic service offering allowed the Greenery to leverage its previous security investments, including Microsoft Defender for Endpoint.
- **[Increased resilience]:** With the combination of MDR, the IR retainer, and Security Program Gap Assessment The Greenery significantly improved their maturity and ensured that it was not just compliant, but demonstrably more resilient to their specific threat landscape.

About Hunt & Hackett

Hunt & Hackett helps European companies prevent, detect and respond to today's most advanced adversaries, safeguarding them against cyberthreats and espionage. Leveraging threat modelling and data science, Hunt & Hackett builds, operates and maintains digital immune systems to protect against Advanced Persistent Threat (APT) groups and less sophisticated cybercrimes such as phishing and ransomware.

What makes us different?

[**Unique MDR offering**]: We provide tailored MDR services that go far beyond other 'off the shelf' solutions. Our MDR offering aims to operate with the speed of an attacker and the depth of a forensic investigation.

[Cloud-based Incident Response Lab]: We developed and operate the first cloud-based Incident Response (IR) lab in the Netherlands, making shorter incident response timelines a reality. This aligns with the stringent response times mandated by NIS2.

[Skills & Expertise]: Hunt & Hackett has unrivalled expertise and skills, having recruited a team of industry-recognised threat researchers, malware analysts, threat intelligence analysts, threat hunters, data scientists and hackers. They operate on the frontlines of cyberconflicts every day, and they love what they are doing.