NTT Security

Technical Insight

Advanced Analytics with Artificial Intelligence: Machine learning combats advanced attacks

Traditional signature-based prevention controls such as antivirus software, IDS signatures, and reputation blacklists remain necessary components of a perimeter-based cyber defense capability against 'known threats' – if they are maintained in the right way.

To improve their defensive capabilities beyond signature-based detection, many organizations have also invested in advanced malware defense products, such as sandbox technologies. But to continuously detect new and unknown threats requires organizations to aggregate the output of all their individual security devices and analyze this data in a precise internal and external context – one that works at the right speed and scale for the business. Maintaining a sustainable security posture that drives value from every technology investment and combats advanced attacks, requires a new approach to analytics.

To get more value from point solutions and move beyond reactive defenses, NTT Security's Advanced Analytics Managed Security Services (MSS) should be the next step on your security road map. Our extensive, early investment in advanced analytics has demonstrated the value of sophisticated algorithms based on machine learning. Fine-tuned with feedback from our team of specialists – who constantly look beyond the perimeter of each client, analyzing over 40 percent of internet traffic – these services use insight from our global threat feeds and sophisticated network of honey pots. Our proven ability to detect advanced attacks, combined with analysis from our security experts, means clients receive actionable notifications with all the frustrating false positives removed. As a result, organizations have more time to both detect and respond to attacks, using less resources.

Gaining visibility beyond the perimeter

In a rush to improve visibility to what may be trying to harm us beyond the perimeter, the information security industry has created a myriad of cyber threat data services and products. But finding a way to turn this host of data into real-time actionable intelligence is proving elusive and expensive. The SANS Institute has highlighted the shortage of standards and interoperability of feeds, but also the lack of context.[1] It warns that, as organizations add data sources, detection and response capabilities may actually decrease as resources are wasted on an explosion of false positives.

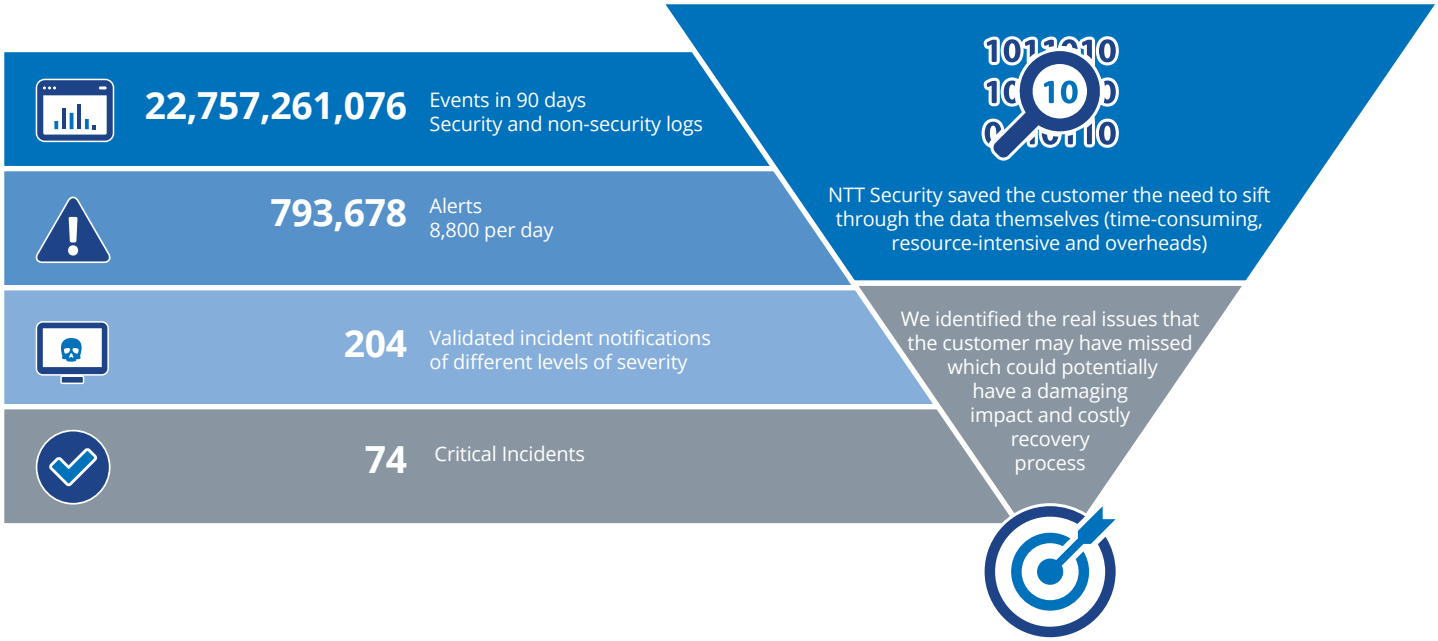
Helping security teams to gain visibility beyond the perimeter does not mean adding to their workload by compiling a threat feed shopping list. In fact, quite the reverse.

Our Advanced Analytics MSS service is underpinned by a range of threat intelligence sources, offering a breadth and depth of visibility that would be very difficult for any individual organization to establish or analyze effectively. As well as this growing range of intelligence feeds, due to NTT Security's integration, our global MSS infrastructure gives our analysts and clients access to immediate insight into specific attacks impacting relevant businesses or verticals across the globe.

But having better visibility beyond the perimeter is not a goal in itself. The value Advanced Analytics provides is focus – by detecting new and unknown attacks, and removing false positives from incident notifications and reporting. As shown in Figure 1 below, while the client receives qualified incident notifications based on investigations by a security analyst, there are no alerts that the client needs to investigate. Out of 204 notifications, 74 were systems successfully breached. The remaining notifications include investigations concluding that the attack was unsuccessful, or other findings that need remediation by the client in order to reduce risk. Our Advanced Analytics service saves the client time and overheads by sifting through the data, as well as saving potentially huge recovery costs by spotting threats that may have been missed.

1. SANS Institute, Securing Web Applications Made Simple and Scalable

Figure 1: Finding the malicious needle in the haystack.
By using state-of-the-art artificial intelligence, machine learning and global threat intelligence to detect and human enrichment to validate, we transform mountains of data to pinpoint what's important to your business, saving you time and money



Detection of new and unknown threats

As the above example demonstrates, the only way to respond to the ever-changing threat landscape is to transform the efficiency of detection and response. But how can organizations take billions of logs and alerts and turn this barrage of data into action? We have the answer – our Advanced Analytics service.

Attackers continuously attempt to avoid traditional detection techniques by constantly changing their malware and infrastructure. However, the overall behavior is still inherently the same. This is where behavior modeling provides such enormous value in detecting new and unknown attack types. Our analysis engine finds that malicious needle in the haystack, and the remaining few false alarms are removed by our security analysts during the incident investigation phase. Even if an organization can apply machine learning techniques, it is very difficult for them to access the breadth of data necessary for active detection and protection. This is why so many organizations seek a service partner to provide this level of real-time intelligence.

It is no longer good enough for organizations to say that they did not know that they had been breached. As recent mega data losses have shown, the longer the timeframe, the larger the loss of confidence and reputation – let alone remediation and compliance costs.

What is Machine Learning?

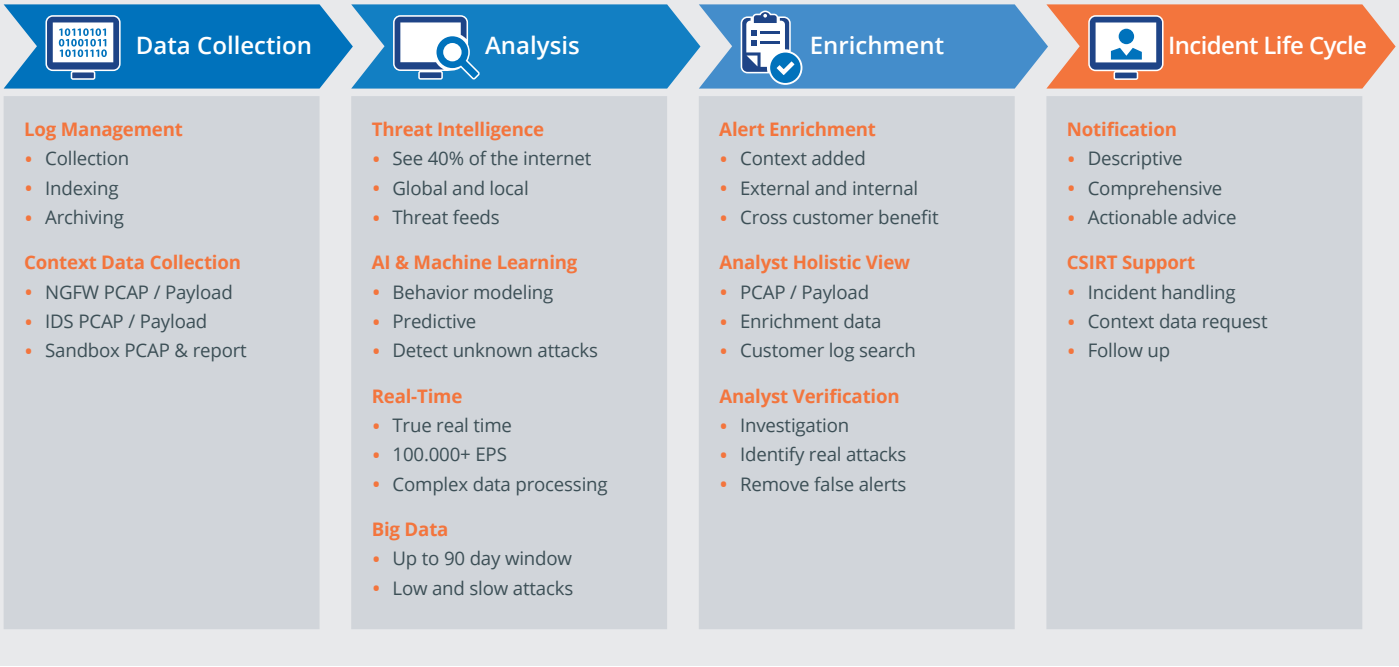
Machine learning (ML) is a subset of artificial intelligence – giving computers the capability to learn without being explicitly programmed. ML is widely used in many sectors, with deep learning delivering value across many analytical applications that need to work at speed and scale.

At NTT Security, we focus on proven supervised and unsupervised ML techniques – taking extraordinary care to ensure that we use accurate labels when training our advanced cyber analytics models. In order to build models that detect malware designed to bypass state-of-the-art intrusion detection systems, we need the deep and wide exposure to malicious and benign activity patterns that our global infrastructure provides.

Before we build any models, we collect, clean, normalize and label our data. These pre-processing steps are vital, as incorrect labels or otherwise 'dirty' input samples can introduce bias and/or variance into the model and impact performance. Our team of security analysts plays a vital role in correctly labeling data. While the majority of labels emanate from our honey pot and sandbox environments across the global NTT family, our security analysts receive comprehensive access to all the evidence before assigning a label. This has allowed our analysts to gradually build trust in the models and not treat the ML as a 'black box'. As we develop several ML models using supervised learning, feedback and input from our analysts is essential.

The use of ML not only dramatically increases detection of unknown attacks, but also allows our analysts to focus on high-value security analytics rather than the repetitive tasks demanded by traditional Security Information and Event Management (SIEM) solutions. This is a vital step towards greater efficiency and application of the analysts' skills, which as we all know, are in short supply.

Figure 2: Advanced Analytics value chain



Actionable incident notification and reporting

As the above example demonstrates, to make a difference to our clients, we strive to provide actionable incident notification and reporting. It does not matter how clever the technology or analysts are if we cannot deliver informed, contextual, real-time insight into the risks that will impact our clients' businesses. And we can, and do, every day

Advanced Analytics in action

The value of new visibility

- Having detected an attack through our log and PCAP analytics, we immediately notified an Advanced Analytics client that there was a high probablility that an employee's laptop had been compromised.
- Keeping this machine under review, we did not witness any backdoor communication or other activity that could 100% verify that the machine had been breached. The client had problems getting hold of the machine as the employee was traveling.
- 24 hours later an AI & Machine Learning based rule (DGA – Domain Generated Algorithm rule) detected hidden backdoor communication from the same client. This allowed us to verify that the machine had been compromised. With this notification, the client confidently took the machine offline, wiped it and re-installed the operating system and programs. 'Sleeping' after initial compromise is a typical malicious attack technique to avoid detection. In this instance, the attack slept for exactly 24 hours and 17 minutes.

How we make a difference

Detecting this backdoor communication is impossible using a blacklist, or any other static rule, as the domain name generated is designed for 'one time' use. This is just one example of where applying a DGA algorithm developed using ML transforms the detection and notification of attacks. NTT Security was the first to put this type of detection into production and deliver the value of this visibility to its clients.

Conclusion

With our Advanced Analytics powered MSS, evasion becomes much harder for cyber criminals. We have led the industry as the first organization to apply artificial intelligence (AI) and machine learning to information security as part of our annual investment of $3.5 billion in R&D. We combine these technologies and the analysis insight within our Managed Security Services. Armed with contextual intelligence, our clients can focus resources on reducing risk and providing strategic advice to their organizations, rather than drowning in data and reacting to false positives.

Despite the industrialization of malware, we have not lost the cybersecurity battle. NTT Security Advanced Analytics helps our clients regain control of malware detection and response – with greater visibility beyond the perimeter to improve their security posture and proactively mitigate complex and emerging threats.

Benefits of the NTT Security Advanced Analytics service:

- Detects attacks that would otherwise go unnoticed
- Combines machine learning and human enrichment to reduce false positives
- Improved overall security posture
- Drives efficiency of incident response and management
- Frees resources from operational tasks to focus on strategic projects

About NTT Security

NTT Security seamlessly delivers cyber resilience by enabling organizations to build high-performing and effective security and risk management programs, with controls that enable the increasingly connected world and digital economy to overcome constantly changing security challenges. Through the Full Security Life Cycle, we ensure that scarce resources are used effectively by providing the right mix of integrated consulting, managed, cloud, and hybrid services – delivered by local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest information and communications technology (ICT) companies in the world. For more information, visit **www.nttsecurity.com**

To learn more about NTT Security and our unique services for information security and risk management, please speak to your account representative or visit: **www.nttsecurity.com** for regional contact information.