STATE OF NEW YORK

DIVISION OF TAX APPEALS

In the Matter of the Petitions of **SECUREWORKS, INC.** for Revision of Determinations or for Refund of Sales and Use Taxes under Articles 28 and 29 of the Tax Law for the period September 1, 2011 through November 30, 2015.	: : : : : :	DETERMINATION DTA NOS. 828328 AND 828329

Petitioner, Secureworks, Inc., filed petitions for revision of determinations or for refund of sales and use taxes under articles 28 and 29 of the Tax Law for the period September 1, 2011 through November 30, 2015.

A consolidated hearing was held in Albany, New York, on January 23, 2020, with all briefs to be submitted by July 17, 2020, which date began the six-month period for issuance of this determination. Petitioner appeared by Ryan, LLC (Charles Rice, Esq., of counsel). The Division of Taxation appeared by Amanda Hiller, Esq. (Stephanie Scalzo, Esq., of counsel). After reviewing the entire record in this matter, Jessica DiFiore, Administrative Law Judge, renders the following determination.

ISSUES

I. Whether petitioner's services are protective and detective services subject to sales tax pursuant to Tax Law § 1105 (c) (8).

II. Whether, in the alternative, petitioner's services are information services subject to tax pursuant to Tax Law § 1105 (c) (1).

FINDINGS OF FACT

1. Petitioner, Secureworks, Inc., is an information technology (IT) security services provider that offers managed and monitored security services, giving customers information to prevent, detect, respond to, and predict cyberattacks. Petitioner's customers get visibility to potential threats in the critical areas of their IT infrastructure. Petitioner is headquartered and has its principal address in Atlanta, Georgia.

2. Several of petitioner's services have a management component and a monitoring component. When petitioner is performing management services, it is making changes to the device or software to help the customer keep the device or software operating properly. Petitioner's monitoring services involve reviewing the events that a device or software is producing and advising customers when they should investigate an event further. The components of a security infrastructure generate thousands of events each day. Petitioner helps its customers determine which events require their attention. Most of petitioner's services are sold as a monitoring service or as a monitoring service, plus management.

3. When petitioner discovers a new threat actor as part of its managing and monitoring services, the threat actor is included in its threat intelligence services, which are described below.

4. Petitioner manages and monitors firewalls. These services are sold as annual subscriptions. A firewall is a security device that is connected to a customer's network. The firewall controls the connections that are allowed access into the customer's network and the connections from the customer's network to outside the company. The firewall is configured to block unauthorized access to a customer's computer. Vulnerabilities arise when certain connections need to be allowed through the firewall, creating an opportunity for unauthorized

access. Petitioner does not sell the firewall with its managing and monitoring service. Its customers purchase firewalls from other manufacturers.

Firewalls generate security events that indicate when someone is connected to a site or when a connection has been blocked. Petitioner monitors those events and notifies its customers when it thinks they should be aware of an event and investigates further for things such as a virus or software designed to gain unauthorized access to a computer system to disrupt or damage the system. Petitioner does not identify who is attempting the unauthorized access or assess any damage that was done.

Petitioner's website provides that "[f]irewall management is resource-intensive and requires a high level of expertise to prevent unauthorized access and costly breaches. Devices must be provisioned, deployed, upgraded and patched to keep up with the latest threats." Managing a firewall includes updating a firewall's security policies and configurations, implementing software upgrades and performing patch maintenance. This service involves petitioner obtaining the software upgrade or patch from the manufacturer and testing it to determine whether it will help prevent the latest threats. If petitioner thinks the upgrade or patch is beneficial, it will work with the customer to determine when to apply it and petitioner will apply it for the customer. The management service also includes petitioner configuring the firewall with intelligence from its "global visibility" and Counter Threat Unit (CTU) research to look for signatures or patterns in the network traffic for signs of malicious intent. This is referred to as "policy management." This includes integrating information from petitioner's Attacker Database of Internet Protocol (IP) addresses associated with known threats.

Petitioner performs this same service for "Integrated Appliances." These are referred to in the industry as next generation firewalls. They are firewalls that do more than just monitor the

network connections. These devices may be able to serve other security functions such as operating as an intrusion detection system, which is explained below.

5. Petitioner provides network intrusion detection/prevention services, including an Advanced Endpoint Threat Detection (AETD) monitoring service, and monitoring and/or managing Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) and iSensor services. Petitioner's AETD service is based on endpoint intelligence developed by petitioner's CTU research team. Under the AETD service, petitioner provides constant detection and analysis of potential threats to a customer's endpoints, such as a server, laptop or desktop, so that it can respond quickly and whenever necessary. As stated on petitioner's website "AETD goes beyond identifying a threat to accessing extensive intelligence on threat actors and their tradecraft, helping you to accelerate your response by pinpointing exactly which systems are compromised, how it happened and how you can repair them." Petitioner claims that it knows what to look for and can detect more threats than its competition. Customers have access to petitioner's hosted cloud solution that sends alerts through telephone or email depending on the severity level of the issues.

6. For petitioner's managed and monitored IDS/IPS service, petitioner provides proactive administration 24 hours a day, 365 days a year. Petitioner's security experts perform all activities to keep the devices operating at peak performance. IDS and IPS look for patterns in the traffic that may show that someone is trying to breach or compromise a client's network. The IDS or IPS include a hardware device or software that can create and/or monitor security events. One piece of equipment, or software, can be configured to be either an IDS or an IPS. The customer will install or configure it differently based on how the customer wants it to function. An IDS looks at the network traffic watching for signs of malicious intent. It records

the connections, but it cannot prevent a connection. An IPS acts like a firewall, where traffic has to go through it, and it can be configured to block access to the client's network. The IPS has to be in the middle of the network traffic so that it can stop the connections when it detects something malicious. If a customer purchases an IDS or an IPS device from a company other than petitioner, petitioner will provide management and/or monitoring services for it.

Petitioner's management and monitoring services to IDS and IPS are similar to the services petitioner provides for a firewall. When managing the device, petitioner configures the IDS or IPS device to look for signatures or patterns in the network traffic for signs of malicious intent. Petitioner then maintains this configuration. Policies are continuously assessed and updated to prevent threats from accessing petitioner's customer's networks. Like with their service to firewalls, petitioner also tests any patches from the manufacturer of the IDS and IPS and installs them.

When monitoring the device, petitioner tracks events produced by the IDS or IPS and evaluates them to determine whether its customers need to investigate an event further. The events the IDS and IPS produce will indicate whether there was malicious intent. They do not confirm whether there has been a breach of a customer's network. This service does not identify the person causing the breach or the damage done by any breach.

7. Petitioner sells a product called an iSensor, which is an IDS or IPS that petitioner sells as part of a managed and monitored service. There is no separate charge for the iSensor. Customers install their own iSensor. When installed as an IPS, an iSensor performs the same functions as a firewall.

8. Petitioner offers a security event monitoring service that involves monitoring of information security activity across a customer's network. Petitioner refers to this service in its

brief as "Server/Network Infrastructure Monitoring" and a similar but more limited service as "SIM On-Demand Server/Maintenance Infrastructure." The primary difference between these two services is that the Server/Network Infrastructure Monitoring service offers a human component where, if petitioner finds something worth a customer's attention, it will call the customer any time, day or night. The SIM on-Demand service only communicates issues to the customer through the customer portal.

Petitioner gives its customers a virtual Counter Threat Appliance (CTA) or an Inspector that connects to a customer's network to capture events from servers and network devices, including routers, firewalls, and intrusion detection systems to reveal security threats. The customers are responsible for directing the events to the CTA, which condenses them and sends them back to petitioner for analysis.

The service is provided to customers using petitioner's Counter Threat Platform (CTP). The CTP provides health checks on managed and monitored devices. The CTP can aggregate events from most devices. The CTP technology processes event information to identify events of interest. The CTA or Inspector will compare events to known malicious activity and known normal activity. Security experts then conduct further analysis and escalate security incidents to customers. Customers can view the events and incidents through petitioner's customer portal, which features integrated business intelligence and analytics tools to assist customers in making better security decisions.

9. Petitioner also offers a subscription for a log retention service. Logs are repositories that collect security events that come from devices such as firewalls, IDSs, IPSs, servers and routers. Petitioner's website provides that "[e]very security appliance, business-critical system, noncritical server and endpoint . . . generates extensive event logs daily that must be managed to

provide an early warning system for fast response to security events." Petitioner offers a LogVault, which is a device that customers connect to their network and stores all of their events. Petitioner also offers virtual log retention appliances. There is one combined charge for the LogVault and the service. Petitioner helps the customer configure and implement the LogVault or software, it monitors it to ensure it is operating properly, and it patches and upgrades it periodically. Petitioner also manages log retention devices purchased from other vendors. Petitioner reports the events created through its customer portal.

10. Petitioner also offers a Log Monitoring Service. This service involves the effective management and monitoring of log retention appliances. The service includes the same initial tasks as the log retention service of configuring and implementing the retention appliance and ensuring it is operational. This service also then involves monitoring and analyzing customers' events generated across their networks. Petitioner reviews the events and notifies its customers of anomalies that aid in a customer's response to threats. Petitioner also uses this information when compiling data for its Threat Intelligence Service.

11. Petitioner's Threat Intelligence Service is a subscription service. The goal of this service is to educate customers about the likelihood that their organization will be breached. Petitioner's witness testified that Threat Intelligence "is a collection of information services that we provide to our clients related to the threat landscape." The knowledge for these services comes from the internet, a national vulnerability database, common feeds that contain information about new vulnerabilities, and any new threat actor petitioner discovers as part of its managing and monitoring services it provides to its customers. This service allows customers to take advantage of petitioner's threat intelligence knowledge acquired through access to thousands of client environments around the world. Customers access this service through

petitioner's customer portal or a data feed. The primary components of the Threat Intelligence Service are its Vulnerability Data Service, its Threat Analysis Service, its Advisory Data Service and its Monthly Security Intelligence webinars.

In petitioner's Vulnerability Data Service, customers are provided with detailed descriptions and analysis of current vulnerabilities. Vulnerabilities are software flaws that may be exploited to allow a malicious user or code to attack the software or operating system. Vulnerabilities are processed from public and private data feeds, enriched by petitioner's researchers and reported to customers through the customer portal. This service is different from petitioner's Vulnerability Scanning Service which is explained more fully below and is unique to the vulnerabilities present on a single customer's network.

The Threat Data Service component of petitioner's Threat Intelligence Service involves petitioner's CTU research team publishing a detailed breakdown of malware or threats twice a month. Petitioner's Advisory Data Service component involves petitioner providing reports analyzing attack data across petitioner's monitored security devices, including threats targeting many of its customers. Petitioner's Monthly Security Intelligence Webinar is open to all of petitioner's customers who subscribe to the Threat Intelligence Service and involves the CTU research team hosting a monthly webinar security briefing where it describes current security threats and reviews current security concerns and hacker activities.

Petitioner also provides Threat Intelligence Service customers a data feed of its Attacker Database. The database, which is updated daily, includes attack information, such as lists of malicious IP addresses and domains, processed from thousands of monitored security devices. This service is an add-on service that is charged separately.

12. Petitioner also offers a Targeted Threat Hunting Service. This service involves performing searches of a customer's networks and endpoints, such as laptops or tablets, to identify the presence of vulnerabilities and entrenched threat actors operating on a customer's environment. Petitioner's service assists its customers in determining how the threat got there, what its purpose is, and who may be behind it. Pursuant to petitioner's website, petitioner will also "provide specific guidance on appropriate response and remediation steps to contain and eradicate the threat and actor from your environment." Petitioner will also give recommendations on security improvements. This service complements security event monitoring.

13. Petitioner also offers Enterprise Brand Surveillance, which is one of its add-on Threat Intelligence Services. The service consists of researchers conducting research and analysis to report and alert on security threats that are specific to a customer. Petitioner will analyze publicly accessible resources on the internet and use "open source intelligence" collection capabilities and other research capabilities. "Open source intelligence" was defined by petitioner in its service description as "any non-classified, unclassified, or publicly available information, as opposed to information that is acquired through covert or clandestine means for official purposes." Non-proprietary sources of information are used to acquire and synthesize data. Customers will give petitioner key words or terms and petitioner will search different portions of the internet, including surface web, which is the normal part of the web, and dark web and deep web, where more criminals are present.

Petitioner will provide its customers with a report of its findings through an encrypted email. Petitioner will report and alert on security threats that are specific to the customer on a monthly basis. The information collected is representative of what an attacker could compile

about a customer's organization, to either capitalize on the information for malicious purposes or to serve as a basis for a future attack against a customer's organization. The customer can use the information to detect and prevent threats and threat actor activity. The components of the service involve a threat profile, monthly monitoring reports, monthly update meetings and monitoring and alerting. The reports are only provided to the customer who requests it.

14. Petitioner offers a Vulnerability Scanning Service that scans network devices, servers, web applications, databases and other assets both at a customer's place of business and in cloud environments to find exposures to exploitation by threat actors so that its customers can eliminate them. Petitioner's website provides that vulnerabilities can arise daily within networks, web applications, and databases, due to software defects or system misconfigurations. This service is delivered using petitioner's CTP and consists of automated and recurring vulnerability scanning and delivery of such scanning, along with remediation workflow tools. The customer portal features integrated business intelligence and analytics tools to assist its clients in obtaining meaningful insights and perspectives to make better IT security decisions. Petitioner's clients can run reports on demand using the client portal.

Included with this service is a license to use the scanning product Qualys, 24-hour access through petitioner's customer portal, and 24-hour access to petitioner's counter threat operations center, to enable customers to ask questions related to the service. Petitioner also provides a quarterly telephone review of each customer's scan results.

15. Petitioner also provides incident response services. When a customer concludes that there has been a breach, it can hire petitioner to analyze, contain and help the customer recover from the breach.

16. For all of petitioner's monitoring services, when petitioner finds something that the customer needs to be apprised of, it generates a ticket that goes to the customer in petitioner's customer portal. If it is something petitioner believes is worth a customer's immediate investigation, petitioner will call the customer if it is in the customer's service agreement, and the customer will begin its own investigation to determine whether the event was a threat.

17. Another service petitioner provides is resident security operations. For this service, petitioner provides one of its employees to work at a customer's offices. Each agreement for the services performed by the resident security operations is custom to the customer. However, the most common usage involves petitioner's employee working at the customer's office receiving phone calls from petitioner regarding events and reviewing the events created by a client's equipment and then determining whether the customer should be notified of the event or if another device in the customer's network that petitioner may not have access to blocked the threat. On its website, petitioner states that its "expert residents can help you design, implement, and manage full-scale security programs to protect your organization against cyber threats."

18. On June 27, 2014, the Division of Taxation (Division) sent a letter to petitioner scheduling an appointment at petitioner's office in Texas for February 9, 2015, to commence a sales and use tax field audit of its business for the period September 1, 2011 through August 31, 2014. The Division's letter requested that all books and records pertaining to petitioner's sales and use tax liability for the audit period be available for review. Enclosed with the letter to petitioner was an Information Document Request (IDR), requesting specific records including the general ledger, cash receipts journal, federal income tax returns, state tax returns, purchase invoices, sales contracts providing details/support for the invoiced charges, fixed asset purchase invoices, cash disbursements journal, bank statements, canceled checks and deposit slips for all

accounts, and exemption documents. In response to the IDR, the Division received some electronic sales information prior to the scheduled February 9, 2015 visit.

19. On September 14, 2015, October 13, 2015, and January 14, 2016, the Division sent a second IDR, requesting service orders/invoices and line item descriptions, such as service level agreements, service descriptions, and terms and conditions that are provided as explanation to the customer for each item number that they are purchasing on the service order/invoice. This was requested because the sales records were provided to the Division in Excel, and the line items that were charged did not have a description to determine what sale or service was being provided to the customer. The Division was provided with a few sample invoices when at petitioner's offices in Texas, but was not provided any additional invoices during the course of the audit. The Division did receive additional documents explaining some of the descriptions relating to some of the charges.

20. The Division also sent petitioner a letter on January 14, 2016, advising petitioner that the Division expanded the audit period from September 1, 2011 through November 30, 2015. The January 14, 2016 copy of the second IDR included the expanded audit period as the sale tax quarters being covered. A third IDR was also sent on January 14, 2016, requesting all of the records requested in the first IDR for the expanded audit period.

21. On March 11, 2016, the Division sent petitioner a fourth IDR, again requesting descriptions for the line item charges, including those that are available on petitioner's website. Petitioner directed the Division to the company's website for an explanation of the services they offer. Contracts, service level agreements, terms and conditions, and service descriptions relating to petitioner's service charges were not provided.

22. Petitioner ultimately provided the Division with a spreadsheet listing the categories of service petitioner provided, followed by a description of that service, and a link to petitioner's website for more information about the service. The categories included: Professional Service, Log Retention, Monitoring, Network Intrusion Detection/Prevention, Firewall, Scanning, and Threat Intelligence Information service. The Professional Service category was described as "Professional consulting services typically billed on the basis of time and expenses incurred." Log Retention was described as the capturing and archiving of network events for future analysis by the customer. Monitoring and Network Intrusion Detection/Prevention were both described as "network monitoring services." The firewall service was described as "management, monitoring, and maintenance of network firewall." Scanning was described as "[s]canning of network to identify and isolate viruses, malware, or other potential threats." The Threat Intelligence Information Service was described as "typically delivered in the form of periodic reports to client regarding threats."

23. In January, February and March of 2017, the Division sent three additional IDRs regarding the location of devices petitioner was servicing. Petitioner asserted that some of the devices it was servicing were being billed to New York addresses but were located outside of New York and were not subject to sales tax. The Division requested the IP address information for these devices.

24. The Division's review was split between customers with in-state addresses (in-state customers) and customers receiving services in-state but having billing addresses outside the State (out-of-state customers). Because some customers with billing addresses in New York had devices located outside of the state, the Division believed that there were customers where the

bill was being sent to them in other states, but the devices were located in New York, and should be taxed.

25. Ultimately, the Division issued a separate assessment for in-state customers and out-of-state customers. On May 26, 2017, the Division issued to petitioner a notice of determination with assessment ID L-046509898, which asserted $1,098,799.27 in additional sales and use taxes due, plus interest, for the period September 1, 2011 through November 30, 2015, for petitioner's in-state customers. The Division's assessment was the result of a detailed review of petitioner's records.

26. After notice number L-046509898 was issued, petitioner provided the Division with additional IP address information for petitioner's in-state customers that had devices outside of New York despite being billed in New York, and exemption certificates for two of petitioner's other customers. After reviewing the additional documentation, assessment L-046509898 was reduced to a total tax due of $932,892.50, plus interest.

27. Because petitioner did not provide the requested information regarding the IP addresses for petitioner's customers before the audit was closed, the Division used the sales information from petitioner for the sales billed to in-state customers and the reductions made on those sales for devices that were then shown to be located outside of New York, and calculated an error rate of 32.99 percent. The Division then multiplied the quarterly sales made to customers who were billed outside of New York by the 32.99 percent error rate for the entire audit period, to determine the calculated taxable sales and ultimately, the tax due on petitioner's sales to out-of-state customers. The Division issued a second notice of determination on May 26, 2017, with assessment ID L-046509501, assessing tax due for petitioner's customers who

were billed outside of New York but who had devices in New York, for a total tax due of $12,352,700.56 plus interest.

28. After the assessment was issued, petitioner provided the Division with IP address information for its out-of-state customers. The tax was then calculated using the total percentage of devices that were shown to be in New York for each customer, multiplied by the total charges for that customer, and that was the amount that was then subject to tax. These adjustments resulted in the tax due being reduced from $12,352,700.56 to $215,394.04 for assessment L-046509501.

SUMMARY OF THE PARTIES' POSITIONS

29. Petitioner argues that its services are neither protective and detective services, nor information services. Petitioner asserts its services do not stop or try to stop access to a customer's computer system. Petitioner contends that its services are not protective because they do not guard or protect its customers' computer systems and data. Petitioner also argues that its services are not detective because those services relate to examining and identifying persons, groups of people, or corporations with regard to their whereabouts and petitioner does not identify wrong-doers or quantify damage caused by a breach as part of its service.

Petitioner claims its services are not taxable information services because it merely turns over events to its customers coming from the various computer devices. Petitioner also argues that any information gleaned from events created on a customer's equipment are personal and individual in nature and not an information service subject to tax. Petitioner alleges that its Enterprise Brand Surveillance service involves information that is explicit and proprietary to a specific customer and that it does not sell such information to anyone else. Petitioner acknowledges it may be argued that its Threat Intelligence Service is not personal or individual

in nature but asserts that the information in the reports could affect a specific customer which makes the nature of the information personal.

30. The Division asserts petitioner's services are taxable protective services. It contends that protective services include services intended to protect against unauthorized access, or malicious activity, and also include monitoring for unauthorized access or vulnerabilities that threat actors could exploit. The Division argues that if petitioner's services are not found to be taxable protective services, they are taxable information services. The Division asserts that petitioner collects and compiles cyber threat intelligence and disseminates it through databases and intelligence feeds. The Division also argues that petitioner's services are taxable information services because it takes the intelligence it finds, compiles it and furnishes its customers with the resulting information through threat warnings, alerts, tickets and other reports.

CONCLUSIONS OF LAW

A. Tax Law § 1105 (c) (8) imposes tax upon the provision of:

> "[p]rotective and detective services, including, but not limited to, all services provided by or through alarm or protective systems of every nature, including, but not limited to, protection against burglary, theft, fire, water damage or any malfunction of industrial processes or any other malfunction of or damage to property or injury to persons, detective agencies, armored car services and guard, patrol and watchman services of every nature other than the performance of such services by a port watchman licensed by the waterfront commission of New York harbor, whether or not tangible personal property is transferred in conjunction therewith."

B. "The language of the statute 'is the clearest indicator of legislative intent and courts should construe unambiguous language to give effect to its plain meaning'" (***Matter of the Walt Disney Co. and Consolidated Subsidiaries***, Tax Appeals Tribunal, August 6, 2020, quoting ***DaimlerChrysler Corp. v Spitzer***, 7 NY3d 653, 660 [2006]; ***Matter of Watchtower Bible and***

TractDecision Society of New York, Inc., Tax Appeals Tribunal, July 16, 2020). However, when the words are ambiguous, other methods of determining legislative intent should be considered, including a review of statutes in para materia, or involving the same subject matter (***see*** McKinney's Cons Laws of NY, Book 1, Statutes §§ 76, 92, 221; ***Matter of AlliedBarton Security Services Inc.*** [***AlliedBarton***], Tax Appeals Tribunal, February 16, 2016).

C. "In questions of statutory interpretation where the issue is the imposition of a tax, the statute cannot be read to allow the government to tax anything more than the clear terms of the statute allow" (***id.***, citing ***Matter of Grace v New York State Tax Commn***., 37 NY2d 193, 196 [1975], ***lv denied*** 37 NY2d 816 [1975]). Additionally, when the question presented is strictly statutory construction, there is no cause to rely on the expertise of the administrative agency (***see DaimlerChrysler Corp.***, 7 NY3d at 660).

D. As article 28 of the Tax Law does not define protective or detective services, it is appropriate to look at statutes involving the same subject matter (***see AlliedBarton***; ***Compass Adjusters & Investigators v Commissioner of Taxation and Fin. of State of NY***, 197 AD2d 38, 41 [1994]). It is proper to consider the definition of "Watch, guard or patrol agency" provided in General Business Law § 71 (2) (***see id.***). As relevant here, that definition states that such terms

> "shall mean and include the business of watch, guard or patrol agency and shall also mean and include, separately or collectively, the furnishing, for hire or reward, of watchmen or guards or private patrolmen or other persons to protect persons or property or to prevent the theft or the unlawful taking of goods, wares or merchandise, or to prevent the misappropriation or concealment of goods, wares or merchandise, money, bonds, stocks, choses in action, notes or other valuable documents, papers, and articles of value, or to procure the return thereof or the performing of the service of such guard or other person for any of said purposes."

This definition is consistent with the language provided in Tax Law § 1105 (c) (8), which provides that protective and detective services include alarm or protective services of every nature and guard, patrol and watchmen services of every nature (***see*** Tax Law § 1105 [c] [8]).

E. A review of the language in both Tax Law § 1105 (c) (8) and General Business Law § 71 (2) shows that petitioner's managing, monitoring, and scanning services, are protective services subject to tax. These services specifically include managing and/or monitoring a firewall or integrated appliance, petitioner's AETD monitoring service, managing and/or monitoring IPS or IDS, including the iSensor, security event monitoring, log monitoring, Targeted Threat Hunting and Vulnerability Scanning.

When petitioner manages firewalls, IPS, or any integrated appliances, it takes the existing device or software and uses its experience in the industry and information collected from its customers and elsewhere to configure the device's security policies to prevent connections from threat actors. This constitutes preventing the theft, unlawful taking or damage of goods within the meaning of Tax Law § 1105 (c) (8) and General Business Law § 71 (2). Additionally, petitioner protects its customer's network by configuring these devices and IDS to result in the creation of events when certain outside connections are made. Petitioner also tests patches and upgrades produced by the device manufacturer to determine whether it will help prevent the latest threats. If petitioner decides such modifications will improve its level of protection, petitioner will update the device.

Petitioner argues that managing these devices does not include blocking access to a customer's computer system or data and, therefore, the service alone does not protect or guard a customer's computer. However, petitioner's management services do just that. While petitioner may not take overt action to block connections through a firewall or an IPS at the moment they

are being attempted, by configuring these appliances to determine who is allowed access, and maintaining them to ensure they are operational with the most current policies, petitioner is proactively protecting and guarding petitioner's network from threats. Configuring an IDS is also done to ensure it is monitoring for suspicious activity to protect a customer's network. The purpose of managing these devices and software is to protect or guard a customer's network from malicious activity. Therefore, such services are taxable protective services.

F. To the extent the Division is arguing petitioner's management services are information services subject to tax, the argument is rejected. Tax Law § 1105 (c) (1) imposes tax upon the receipts from every retail sale of an information service, defined as follows:

> "The furnishing of information by printed, mimeographed or multigraphed matter or by duplicating written or printed matter in any other manner, including the services of collecting, compiling or analyzing information of any kind or nature and furnishing reports thereof to other persons, but excluding the furnishing of information which is personal or individual in nature and which is not or may not be substantially incorporated in reports furnished to other persons . . . ."

Ensuring the operation of a customer's protective devices and configuring and updating them to maximize their ability to perform does not involve the furnishing of information subject to tax within the meaning of Tax Law § 1105 (c) (1).

G. Petitioner's monitoring services are also protective and detective services subject to tax pursuant to Tax Law § 1105 (c) (8). In monitoring firewalls, IDS, IPS, and performing AETD services, security event monitoring, and log monitoring services, petitioner reviews the events created by these devices or software and reports any suspicious activity to its customers either through the customer portal, or, depending of the significance of the threat and the level of service provided, by calling the customer and notifying them of the threat. Petitioner argues that these monitoring services do not qualify as protective services because it does not identify who is attempting the unauthorized access, does not stop the access, and does not assess any of the

damage that was done. However, stopping the access or assessing the damage done are not the exclusive ways a service can be found to be protective or detective. Explicitly included among the protective services subject to tax pursuant to Tax Law § 1105 (c) (8) are "all services provided by or through alarm . . . systems of every nature." Reviewing events with the sole purpose of notifying customers when, based on its experience, petitioner believes a certain event may be a threat to petitioner's network, is an alarm system included within the meaning of the statute.

H. The Division argues that petitioner's monitoring of firewalls, IDS, IPS, and endpoints through its AETD service constitutes a taxable information service because petitioner furnishes its clients with the resulting information through threat warnings, alerts, and tickets. However, in these instances, petitioner is merely relaying the events or alerts that are generated that should be reviewed by the customer. Where a service provider is simply converting information received from one form into another, such service is not a taxable information service (***see ADP Automotive Claims Servs., Inc. v Tax Appeals Trib.***, 188 AD2d 245, 248 [3d Dept 1993], ***lv denied*** 82 NY2d 655 [1993]). Here, petitioner is reviewing the events created by the devices and entering the ones its clients should be aware of into the customer portal. Petitioner is not adding information or intelligence to these events. Accordingly, such service is not an information service subject to tax pursuant to Tax Law § 1105 (c) (1).

I. Petitioner's Vulnerability Scanning Service and Targeted Threat Hunting Service are also protective services subject to tax. Petitioner's Vulnerability Scanning Service scans a customer's devices to find exposures for exploitation by threat actors. Petitioner notifies its clients of weaknesses within the petitioner's network that need to be remedied before a threat actor can take advantage of such weaknesses to access and potentially damage the customer's

network. Like petitioner's Vulnerability Scanning Service, its Targeted Threat Hunting Service involves performing searches of a customer's networks and endpoints, such as laptops or tablets, to identify the presence of vulnerabilities and entrenched threat actors operating on a customer's environment. In regard to both services, petitioner is not just looking at a customer's network and giving a summary of what it finds, it is scanning the customer's network and using its expertise in the area for the purpose of identifying any potential exposures, and discovering the presence of any threat actors, so that its customers can make changes to better protect their environments. Protective services subject to tax include protective systems of every nature (***see*** Tax Law § 1105 [c] [8]). These services are taxable protective services that prevent the theft of property.

J. Petitioner's Vulnerability Scanning Service and Targeted Threat Hunting Service are integrated services. Both are providing protective services subject to tax pursuant to Tax Law § 1105 (c) (8) and information services encompassed in Tax Law § 1105 (c) (1). In petitioner's Vulnerability Scanning Service, in addition to identifying specific exposures that pose the greatest risk, through advanced reporting functionality, petitioner's portal also provides reports of insights and perspectives to answer its customers' vulnerability management questions and assists its customers in making better security decisions. Petitioner's Targeted Threat Hunting Service involves searching for the presence of malware or threat actors, and it also includes providing guidance on appropriate response and remediation steps where threat actors are found.

Where services are integrated, the primary function of the service controls the taxability (***see Matter of SSOV '81 Ltd.***, Tax Appeals Tribunal, January 19, 1995). To determine a service's taxability, the analysis focuses on the service in its entirety, as opposed to reviewing the service by components or by the means in which the service is effectuated (***see id.***). The primary

function of both petitioner's Vulnerability Scanning Service and its Targeted Threat Hunting Service is to protect its clients' networks from malicious activity. The information services provided by petitioner to its customers in performing these services are incidental aspects of the overall protective service and are not separately taxable.

K. Assuming, arguendo, that the primary functions of petitioner's Vulnerability Scanning Service and Targeted Threat Hunting Service were information services, the next inquiry is whether they are excluded from tax as personal and individual in nature and not substantially incorporated in reports furnished to others (***see*** Tax Law § 1105 [c] [1]; ***Wegmans Food Markets, Inc. v Tax Appeals Trib. of the State of New York***, 33 NY3d 587, 594 [2019]). Where the question is whether taxation is negated by a statutory exclusion, "'the presumption is in favor of the taxing power'" (***Id.***, quoting ***Matter of Mobil Oil Corp. v Finance Adm'r of City of N.Y.***, 58 NY2d 95, 99 [1983]). Here, the information is gleaned from each individual client's network. Petitioner issues reports in the customer's portal advising them of their exposures or if a threat has been found and how to remediate. Accordingly, the reports are personal or individual in nature. However, such information is or may be incorporated in reports furnished to others (***see*** findings of fact 3 and 11). Therefore, if the primary function of petitioner's Vulnerability Scanning Service and Targeted Threat Hunting Service is to provide an information service, such services are subject to tax pursuant to Tax Law § 1105 (c) (1).

L. Petitioner's Incident Response Service is also a protective and detective service subject to tax. When a customer discovers there has been a breach, it can hire petitioner to analyze, contain, and help the customer recover from the breach. By containing the breach, petitioner is preventing it from spreading to or accessing more of a customer's network. Analyzing and containing the breach constitutes protection against additional theft or unlawful

taking of goods within the meaning of Tax Law § 1105 (c) (8) and General Business Law § 71 (2).

M. Contracts for petitioner's resident security operations service are custom. However, it was described by petitioner as generally similar to its monitoring service except that petitioner places an employee at the customer's office to monitor the events created by the various systems and receive phone calls from petitioner regarding events. Generally, the resident employee would determine whether the customer should be notified of the event or would review the customer's events created for other devices to determine whether another device in the customer's network that petitioner may not have access to blocked the threat.

It is presumed that all receipts for the enumerated services provided in Tax Law § 1105 (c) are subject to tax until petitioner proves otherwise (***see Wegmans Food Markets, Inc.***, 33 NY3d at 594). While the specific resident operations contracts for which tax was assessed during the audit period were not made a part of the record, the common service provided by residents consists of the same monitoring services concluded above to be subject to tax as protective and detective services (***see*** finding of fact 17; conclusion of law H). Accordingly, by not submitting evidence that the services provided by the residents that were assessed during the audit period were not the same as those found taxable above, petitioner has failed to meet its burden of establishing that its resident operations services that were assessed were not protective and detective services subject to tax.

N. Relying on the Tax Appeals Tribunal's decision in ***AlliedBarton***, petitioner asserts its services are not taxable protective or detective services because they do not amount to guarding or protecting property. Petitioner's interpretation of the Tribunal's holding in ***AlliedBarton*** is too narrow. In ***AlliedBarton***, the Tribunal held that checking visitors' identification and issuing

them passes to enter a building did not rise to the level of protective and detective services encompassed in Tax Law § 1105 (c) (8). It did not, however, establish a rule, as petitioner asserts, that guarding property is the only act that constitutes a protective and detective service encompassed within Tax Law § 1105 (c) (8). In fact, when analyzing the protection service at issue in ***AlliedBarton***, the Tribunal acknowledged that alarm systems were among the services the statute was intended to include. Accordingly, petitioner's reliance is misplaced and its argument that its services are not protective or detective services subject to tax because it does not guard property is rejected.

O. Petitioner's Threat Intelligence Service is not a protective or detective service subject to tax pursuant to Tax Law § 1105 (c) (8). This service involves the dissemination of information generally to all subscribers. It does not involve assessing, monitoring or managing an individual client's network to prevent theft or damage by malicious actors. It does not involve any action for the purpose of protecting its customer's networks. It is an information service subject to tax pursuant to Tax Law § 1105 (c) (1).

Petitioner concedes that its Threat Intelligence Service "is a collection of information services that we provide to our clients related to the threat landscape." Where information is added to basic data that provides a customer with intelligence it did not originally have, such service is an information service (***see ADP Automotive Claims Servs., Inc.*** 188 AD2d at 248). Petitioner does not merely compile and consolidate the information it finds from the internet, databases and threats it finds when managing and monitoring devices and software for customers. Instead, petitioner reviews and processes the vulnerabilities, enriches them with knowledge from its researchers, and reports its findings to its customers. Bi-monthly, petitioner analyzes malware and threats and publishes a detailed breakdown of the same. Petitioner also

offers monthly webinar security briefings as part of the subscription. However, the primary purpose of this service is to inform petitioner's clients about current threats.

Petitioner also provides its customers with reports analyzing attack data in its add-on charge for the Attacker Database. These all result in petitioner generating reports including additional intelligence its customers did not otherwise have. Accordingly, petitioner's Threat Intelligence Service and its add-on Attacker Database service are taxable information services.

The second part of the inquiry is whether petitioner's information services are excluded from tax because they are personal or individual in nature and may not be substantially incorporated in reports furnished to other persons (***see*** Tax Law § 1105 [c] [1]). Where the information is gleaned from publicly available information, the information petitioner provides to its customers is not personal or individual in nature (***see Wegmans Food Markets***, 33 NY3d at 595). The information petitioner compiles and reports to its customers are derived from non-confidential and widely accessible sources, including the internet, a national vulnerability database, and common feeds that contain information about new vulnerabilities. While petitioner does obtain some of its information from the threats it sees in managing and monitoring its clients' security systems, such component does not make the information personal or individual.

Additionally, the reports generated as part of petitioner's Threat Intelligence Service are not unique to each Threat Intelligence Service customer. Anyone with the subscription receives the report. Some information may come from one client's network that petitioner serviced but that information is then shared among all Threat Intelligence subscribers. Accordingly, petitioner's Threat Intelligence Service is an information service subject to tax pursuant to Tax Law § 1105 (c) (1).

P. Petitioner's Enterprise Brand Surveillance is also an information service subject to tax. Much like the information contained in petitioner's Threat Intelligence Services, the information compiled in its Enterprise Brand Surveillance is from public sources (***see*** finding of fact 13). Petitioner simply searches key words or terms provided by its customer, collects the resulting information available on the web, and compiles it into reports which it furnishes to its clients. Customization of publicly available information into a report does not render it personal or individual in nature (***see Wegmans Food Markets, Inc.***, 33 NY3d at 594; ***Matter of RetailData, LLC***, Tax Appeals Tribunal, March 3, 2016). Accordingly, petitioner's Enterprise Brand Surveillance is a taxable information service pursuant to Tax Law § 1105 (c) (1).

Q. Petitioner's log retention service is not an enumerated service subject to tax. Petitioner provides a LogVault or supports different third-party log retention tools. This device collects and stores the events created by the different devices across a customer's network. Petitioner maintains the log retention device to ensure it is operating properly and reports the events created in its customer portal. Ensuring the proper operation of a device so that it retains all of the events created on a network is not a protective service subject to tax pursuant to Tax Law § 1105 (c) (8). Additionally, as petitioner merely reports the events in the customer portal without any additional intelligence, such service is also not an information service subject to tax pursuant to Tax Law § 1105 (c) (1).

R. The petitions are granted to the extent indicated in conclusion of law Q but otherwise denied, the Division is directed to revise the notices of determination in accordance conclusion of law Q, and the notices of determination, as recalculated, are sustained.

DATED: Albany, New York
January 14, 2021

__/s/ Jessica Difiore_____
ADMINISTRATIVE LAW JUDGE