Roles and Responsibilities of Third-Party Security Services

cloud security alliance®

The permanent and official location for the Cloud Security Services Management (CSSM) Cloud Security Working Group research is:
https://cloudsecurityalliance.org/research/working-groups/cloud-security-services-management/

Acknowledgments

Initiative Leads:

Dr. Chen Kai
Dr. Liu Wenmao

Key Contributors:

Du Cheng
Nirjhar Roy
Michael Roza
Jiangyong Shi
Zhiyuan Wu

Reviewers:

Adalberto Valle

CSA Staff:

Hing-Yan Lee
Claire Lehnert (Design)
Ekta Mishra
AnnMarie Ulskey (Cover)

Table of Contents

1 Introduction

1.1 Background

Defining roles and responsibilities to secure cloud services has always been pertinent and necessary. In 2018, the Cloud Security Services Management (CSSM) Working Group (WG) released a white paper entitled 'Guideline on Effectively Managing Security Service in the Cloud' that defined the shared security responsibilities between CSPs and cloud customers. Utilizing this publication, the CSSM WG developed guidelines for designing, deploying, and operating secure cloud services for different cloud service models.

As cloud services are adopted more broadly, it is no surprise that third-party outsourced service availability is also on the rise. The security responsibilities are typically split between the CSPs and cloud service customers (CSCs). However, in reality, third-party security service providers increasingly play essential roles, such as providing consultancy or managing security services for CSCs. In addition, these parties participate in securing the cloud platform as well. For example, some SMEs (small and medium enterprises) without security professionals may be unsure how to safeguard their services and thus engage a third-party security service provider (TPSSP) for consultancy. The TPSSP's role can be pivotal for SME security.

While the 2018 CSSM WG guidelines briefly described the security roles and responsibilities of the TPSSPs, this framework cannot reflect the exact roles and responsibilities of TPSSPs in practice.

1.2 Scope

This document expands on the key ideas covered in 'Guideline on Effectively Managing Security Service in the Cloud' (Chapter 2.6, "Roles of Third-Party Security Service Providers"). Roles and responsibilities are presented in detail below for each service offering.

1.3 Goal

This document aims to educate CSCs on possible services they can engage in based on their requirements.

1.4 Audience

The document's audience includes CSCs, CSPs, and TPSSPs.

2 Definitions and Characteristics

2.1 Definitions

TPSSP/MSSP: A common, alternative term for TPSSP is managed security service provider (MSSP). Gartner states that an MSSP provides outsourced monitoring and management of security devices and systems to cloud customers. Typical services include managed firewalls, intrusion detection, virtual private networks, vulnerability scanning, and antivirus services. The MSSPs use high-availability security operation centers (either from their facilities or other data center providers) to provide 24/7 services that reduce the number of operational security personnel an enterprise needs to hire, train and retain to maintain an appropriate security maturity.[1, 2]

Roles: Description of the types of jobs a third-party security service should perform.

Responsibilities: Definition of processes the service should perform and data types the service should access or manipulate to fulfill a job.

2.2 TPSSP/MSSP Characteristics

Common TPSSP characteristics and services include:

1. TPSSPs provide a menu of options containing various quality security services and products.
2. TPSSPs offer compatibility with various CSP ecosystems.
3. 24/7 online operations and customer support.
4. An ability to leverage multi-tenant solutions to obtain operational efficiencies to reduce costs.
5. A clear development roadmap for security products and services.
6. A well-defined service level agreement (SLA) with measurable and actionable key performance indicators (KPIs).
7. Qualified, skilled professionals and experts, and a structured process to manage personnel changes to minimize service quality impacts.

[1] https://www.gartner.com/en/information-technology/glossary/mssp-managed-security-service-provider

[2] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf, page 14, Incident related

3 Roles and Responsibilities of TPSSPs

3.1 Identity and Access Management (IAM)

Roles: Identity and access management assists in granting appropriate permissions to users and authenticating access to several resources.

Responsibilities: Identity and access management service authenticates and authorizes users and applications using appropriate credentials and monitors user behaviors.

3.1.1 Privileged Access Management (PAM)

Roles: Privileged access management provides secure access to critical assets by managing administrative credentials and privileges for users safely and helps meet compliance requirements.

Responsibilities: Privileged access management manages privileged access between applications, services, and systems.

3.1.2 Access Management and Authentication (AMA)

Roles: Access management enables federation, single-sign-on (SSO), runtime authentication, and authorization for all entities interacting with cloud, web, and legacy applications. Authentication establishes confidence in who is interacting with whom or what.

Responsibilities: Access management and authentication enable authentication that includes multi-factor authentication (MFA), SSO, federation, and runtime authorization for all entities. Furthermore, it establishes trust in the identities of people, devices, and services throughout their interactions. Access management and authentication require that users and applications provide appropriate credentials, including passwords, tokens, and biometric information.

3.1.3 Identity Governance and Administration (IGA)

Roles: Identity governance and administration help enterprises control access risks.

Responsibilities: Identity governance and administration tools manage the identity lifecycle for people, applications, services, and internet of things (IoT) devices. The IGA tools also manage relationships and interactions among entities and ensure they have the correct attributes and entitlements.

3.1.4 Fraud Detection

Roles: Fraud detection improves operational efficiency, enables new and competitive customer eXperience (CX), and reduces fraud.

Responsibilities: Fraud detection solutions should establish the identity of new customers (identity proofing), detect fraudulent identity claims, corroborate identities in subsequent interactions, and deliver robust transaction monitoring.

3.1.5 Identity Threat Protection

Roles: Identity threat protection enables enterprises to detect and protect identities from common threats—thus preventing identity theft attacks such as brute force, password spray, and privilege escalation.

Responsibilities: Identity threat protection solutions manage authentication and authorization with a zero-trust strategy, monitor user identities, behavior, and context for adaptive risk assessments, and detect/prevent identity theft attacks in real-time.

3.2 Cloud Workload Protection Platform (CWPP)

Roles: Cloud workload protection platforms have broad capabilities that span on-premises, physical and virtual machines (VMs), and multiple public cloud infrastructure-as-a-service (IaaS) environments. Ideally, they also support container-based application architectures. This workload includes (but is not limited to) the ability to decrease the attack surface, execute protection capabilities, and conduct runtime detection capabilities.

Responsibilities: Cloud workload protection platforms address the unique requirements of server workload protection in modern hybrid data center architectures. The CWPPs provide workload configuration and vulnerability management, network segmentation, firewalls, traffic visibility, and workload behavior monitoring. Undertaking these tasks essentially furnishes environments with endpoint detection and response (EDR) for servers, anti-malware scanning, system integrity measurement, attestation, monitoring, application control, and log management. In these capacities, CWPPs usually collect a combination of the following data types:

- File hashes and process behavioral data
- Virtual machine processes
- Network access logs
- File access logs
- User access logs
- Container static image data
- Container runtime data
- Container orchestration tools data
- Serverless-related code
- Authentication and configuration data
- Memory and process-related, real-time data
- Basic network access strategic data
- Container access control strategies
- Application programming interface (API) access strategies
- Software information
- Other configuration information

3.2.1 Malware Analysis (Anti-Virus)

Roles: Malware analysis in CWPP helps customers understand the behavior and purpose of a suspicious file or uniform resource locator (URL). This analysis aims to help customers safely upload files to their servers and comply with regulations and policies.

Responsibilities: Malware analysis in CWPP pragmatically triage incidents by severity level, uncovers hidden indicators of compromise (IOCs) that should be blocked, improve the efficacy of IOC alerts and notifications, and enrich context when threat hunting. Malware analysis in CWPP collects file hash values and processes behavior-related data. This analysis is usually performed by traditional anti-virus software.

3.2.2 Server Endpoint Detection and Response (Server EDR)

Roles: Server EDR focuses on runtime detection, continuous real-time monitoring, and data collection with rule-based automated response and analysis capabilities.

Responsibilities: Server EDR monitors and collects activity data from servers assisting in identifying threats, automatically responds to identified hazards to remove or contain them, notifies security personnel of these threats, researches identified threats and searches for suspicious activities. Server EDR can be used to collect virtual machine processes, network access logs, file access logs, user login info, etc.

3.2.3 Container Security

Roles: Container security focuses on protecting container hosts, container applications, and container networks and securing image building, deployment pipelines, and container management planes.

Responsibilities: Container security mainly involves securing container workloads and applications and providing vulnerability assessment, high-fidelity posture management, and workload protection of containers—from development through runtime—across cloud environments. Container security usually collects static image data, runtime data, and logs orchestration tools (e.g., Kubernetes) data from the containers.

3.2.4 Serverless Security

Roles: Serverless security focuses on authentication, preventing application-level attacks, and abuse of serverless applications.

Responsibilities: Serverless security scans and continuously monitors functions for vulnerabilities of serverless applications, starting with integrated continuous integration (CI) tooling and serverless repositories and continuing through runtime for a full lifecycle view into serverless risk.

Serverless security usually collects serverless-related codes, verifies configuration data and application credentials, and scans exposed services.

3.2.5 Memory and Process, Integrity/Protection (MPIP)

Roles: Memory and process integrity/protection focuses on application control and memory protection. The critical point to MPIP is its focus on processes and memory.

Responsibilities: Memory and process integrity/protection helps keep root-level malware from taking over certain parts of an operating system. Memory and process integrity/protection usually needs to collect real-time memory and process-related data, check the integrity of memory and stop suspicious processes from starting.

3.2.6 Micro-segmentation

Roles: Micro-segmentation focuses on the traffic and access control within the internal network while overseeing server-level strategy management and generating alerts on abnormal access activities.

Responsibilities: Micro-segmentation creates secure zones across cloud and data center environments to isolate application workloads from one another and secure them individually. It limits traffic between workloads based on a zero-trust security approach to reduce attack surfaces.

Micro-segmentation usually collects data related to basic network access policies, container access control policies, and API access control policies.

3.2.7 Vulnerability, Hardening, and Configuration Compliance

Roles: Vulnerability, hardening, and configuration compliance focus on vulnerability scanning and compliance monitoring. It is an essential component of CWPP and helps decrease attack surfaces during daily security operations.

Responsibilities: Vulnerability, hardening, and configuration compliance help reduce the chance of introducing new vulnerabilities while minimizing organizational threats. Also, it provides the capacity to manage privileged access and address threat protection for workloads and sensitive data (regardless of where they reside).

Vulnerability, hardening, and configuration compliance usually collect software data and system configuration information.

3.3 Network Security

Roles: Network security focuses on securing inbound and outbound network access, traffic, and behaviors.

Responsibilities: Some network security services are deployed inside tenant networks, coordinating with virtual east/west (internal) or north/south(external) traffic. Additionally, some network security services (e.g., WAFaaS, DDoS mitigation services) are deployed outside CSPs, providing standalone security services.

Network security services must inspect network traffic (usually statistics), payload, or application data for detection purposes. The services must drop, allow, bypass, or redirect the packets for access control and attack mitigation purposes.

3.3.1 Virtual Private Network (VPN)-as-a-Service (VPNaaS)

Roles: Virtual private network services provide remote access to enterprise internal networks (or virtual private clouds) to build an overlay network in a multi-cloud environment.

Responsibilities: A VPN service must solicit a username and password/token from the user for authentication. Moreover, the service requires network access policies (accessible hosts or networks) for network access enforcement.

3.3.2 Network Security Audit

Roles: Network security audit service can be integrated with the CSP to provide content audit, behavior audit, database audit, network traffic audit, etc.

Responsibilities: Network security audit service must monitor all tenant network traffic to capture and extract packets, analyze, and audit corresponding behaviors.

3.3.3 Web Application Firewall (WAF)-as-a-Service (WAFaaS)

Roles: Web application firewalls are deployable in front of a cloud user's website and protect against various web-based attacks while mitigating some DDoS attacks.

Responsibilities: A WAF must control all web traffic to and from websites requiring protection.

- If the WAF is deployed in the reverse proxy mode in the CSP network or deployed in the TPSSP's cloud, the website administrator should modify its domain name system (DNS) record. The WAF must also know the host internet protocol (IP) address and web server hosting port. If the website runs hypertext transfer protocol secure (HTTPS) protocol, the WAF also requires the website's certificates (including private key files) to decrypt encrypted traffic.
- If the WAF is deployed in the inline mode in the CSP network, it must capture all the traffic in the tenant network to and from the website.

3.3.4 Distributed Denial-of-Service (DDoS) Mitigation Service

Roles: Distributed denial-of-service mitigation service usually works with DDoS detection services to mitigate DDoS attacks. Usually, DDoS mitigation services have two deployment types.

- First, TPSSPs deploy DDoS mitigation services in their data center or cloud to provide standalone mitigation services.
- Second, TPSSPs integrate DDoS mitigation (primarily physical) appliances with CSP services to CSP tenants.

Responsibilities: A DDoS mitigation service must control a tenant website's network- or application-level traffic and collect the application types (i.e., web, DNS…), volume, open ports, and IP range of tenant traffic to learn normal patterns in advance.

3.3.5 Network Intrusion Detection/Prevention (NIDPS) Service

Roles: Network intrusion detection/prevention is deployed inside the virtual tenant network. Once malicious packets are captured, the service triggers alerts. Moreover, the network intrusion prevention service terminates network connections or drops malicious packets to prevent an attack's success.

Responsibilities: Network intrusion detection/prevention must monitor and inspect all the traffic through it, report malicious payloads or behaviors, and prevent these payloads and behaviors if necessary.

3.3.6 Secure Web Gateway (SWG) Service

Roles: A SWG provides a secure proxy for employees to visit software-as-a-service (SaaS). Some SWG services offer functionalities such as zero-trust network access or routing optimization.

Responsibilities: The SWG is deployed at the perimeter of an enterprise's on-premise network or cloud network and must capture and inspect all application-level traffic through it.

3.3.7 Network Traffic Analysis (NTA) Service

Roles: An NTA service analyzes tenant network bandwidth and flows to detect abnormal traffic or perform network troubleshooting.

Responsibilities: An NTA service detects and reports malicious traffic, such as scanning and denial of service. Therefore, the NTA service must monitor network flows or all network traffic.

3.4 Data and Storage Security

Roles: Data and storage security service is deployed in the cloud or at third-party data centers to provide services such as data backup, data recovery, digital risk protection, database auditing, data masking, and data encryption.

Responsibilities: Data and storage security services require access to data or operation logs.

3.4.1 Digital Risk Protection

Roles: Digital risk protection service is deployed at the cloud side to protect a tenant's digital assets, including social media channels, website domains, etc.

Responsibilities: Digital risk protection services must access publicly available data needing protection.

3.4.2 Data Backup and Recovery

Roles: Data backup and recovery service is responsible for implementing cloud-based data protection and disaster recovery. It can be divided into three categories: block-level, file-level, and object-level data backup and recovery. In addition, data backup and recovery may provide global data deduplication, compression, and encryption services.

Responsibilities: Data backup and recovery services must access data needing protection.

3.4.3 Database Forensic

Roles: Database forensic services check user operations and cloud databases to find abnormal behaviors or attacks.

Responsibilities: Database forensic services must access all requests from the client application to the database or database operation logs.

3.4.4 Data Masking

Roles: Data masking seeks to prevent sensitive data abuse by giving users masked data generated by actual, sensitive data.

Responsibilities: Data masking can be classified into two technologies based on data usage: static data masking (SDM) prevents the misuse of data at rest (typically in non-production databases). In contrast, dynamic data masking (DDM) deters the abuse of data in transit (typically in production databases). Both technologies must visit or capture the real, sensitive data and determine how it should be masked.

3.4.5 Data Encryption

Roles: Data encryption service encrypts data requiring protection, including static data (i.e., files) and dynamic data (i.e., network traffic).

Responsibilities: Data encryption service must access data to be encrypted.

3.5 Assessment

Roles: Assessment service aims to find vulnerabilities, misconfigurations of exposed or internal assets, and misconfigurations of in-line security products.

Responsibilities: Before assessing, the service needs a starting point (such as an asset's IP address). While evaluating, the service executor must enumerate asset attributes (e.g., open ports, service versions, etc.). Some services may need to perform potentially harmful actions for higher vulnerability verification accuracy or acquire privilege for further assessment.

3.5.1 Vulnerability Scan Services

Roles: Vulnerability scan service identifies and classifies the weakness of an asset or group of assets that one or more threats can exploit.

Responsibilities: Vulnerability scan services analyze systems searching for known vulnerabilities, such as open/insecure ports, software miss configurations, and malware infection susceptibilities.

3.5.2 Cloud Security Posture Management (CSPM)

Roles: Cloud security posture management aims to identify access, check for policy compliance, and detect and mitigate risks.

Responsibilities: Cloud security posture management is responsible for tracking and protecting sensitive data against cloud misconfigurations. It can detect issues such as a lack of encryption, improper encryption key management, extra account permissions, and other matters. Cloud security posture management can also integrate security procedures with DevOps processes.

3.5.3 Penetration Testing Services

Roles: Penetration testing (pentest) service is used to exploit cloud service and/or application vulnerabilities and weaknesses of internal assets (i.e., virtual machines, applications, etc.) in the virtual private cloud (VPC).

Responsibilities: During a pentest, testers must perform some operations (e.g., phishing, injection, denial of service, etc.) with the potential to harm system confidentiality, integrity, or availability. Therefore, every step of the pentest process should be carefully designed, examined, and executed. Note that all pentests must be authorized by asset owners or operators in advance.

3.6 Security Analytics-as-a-Service

Roles: Security analytics-as-a-service provides insight into the significant volume of logs and events generated by all security-related services.

Responsibilities: Security analytics-as-a-service must collect all logs, events, IOCs, and other forms of data to a datastore utility and leverage advanced analytics technology. This technology includes big data, artificial intelligence (AI)/machine learning, and knowledge graphs designed to triage and prioritize events that require attention.

3.6.1 Security Information and Event Management (SIEM)

Roles: Traditional SIEM provides real-time analysis of security alerts generated by servers, endpoints, networks, applications, databases, websites, and other technology systems. Also, SIEM can integrate with the information technology service management (ITSM) system to dispatch security cases.

Responsibilities: Security information and event management collect security data from across the enterprise, identifying events that have security relevance and bringing them to the attention of the security operations center (SOC) team. Security information and event management highlight all relevant information for security specialists to help them identify and mitigate incidents. For example, this includes network information (such as URLs), hashes, connection details, endpoint monitoring, vulnerability information revealed by vulnerability scanners, security intelligence feeds, intrusion prevention (IPS), and detection (IDS) systems.

3.6.2 Security Orchestration, Automation, and Response (SOAR)

Roles: Security orchestration, automation, and response provide organizational capabilities to automate responses to common security alerts or incidents generated by SIEM. Security orchestration, automation, and response help security analysts automate manual workflows and focus on more complex analytics and response processes, rather than spending time managing trivial, time-consuming tasks.

Responsibilities: Security orchestration, automation, and response have built-in or customer-defined processes for managing alerts or events. Each approach has well-defined input and output. Therefore, a SOAR engine can orchestrate these processes into a single pipeline or a more complicated workflow (as defined in a playbook). Playbooks are written by the user security team, security vendor, or managed service provider. Typically, a SOAR engine incorporates alerts and events from SIEM, invokes activities, opens tickets in SOC, and/or provides commands to third-party appliances/services. Therefore, SOAR must access SIEM/SOC and associated privileges to control third-party devices/services.

3.6.3 Audit Log-as-a-Service

Roles: Audit log-as-a-service provides a detailed audit trail of all activities within an enterprise account. An audit log service can be used to identify suspicious activity when it starts (if actively monitored) or to playback account activity during an incident review.

Responsibilities: Audit log service registers the relevant activity into an immutable system, time synced and accessible to account administrators. Audit log examples include application-specific user activities, errors, information security events (successful and rejected), use of privileges, log-on failed attempts and successes, log-offs, accessed data, data attempted to be accessed, administrative configuration changes, and the use of advanced privileges. Additionally, audit logs can be user-friendly, searchable, fully exportable, and available from APIs so events can be easily identified.

3.6.4 Threat Intelligence Services

Roles: Threat intelligence services research and report on emerging threats against the enterprise. Information technology (IT) enables organizations to anticipate, respond to, and remediate threats.

Responsibilities: Threat intelligence services provide evidence-based information, including context, mechanisms, compromise indicators, implications, and actionable advice about existing or emerging hazards to assets. These services allow IT professionals to make decisions and take action accordingly.

3.7 Application Security

Roles: Application security service provides application-level protection for cloud tenants or enterprise users.

Responsibilities: Application security service must identify application vulnerabilities and prevent attacks on different applications types, web applications, email gateways, SaaS applications, etc.

3.7.1 Email Security Service

Roles: Email security service is deployed at the tenant's cloud server and provides functions that include spam filtering, virus scanning, and outbound data auditing.

Responsibilities: Email security service examines the sender, title, and content fields of incoming emails and detects spam, ransomware, and phishing emails using technologies such as threat intelligence, content filtering, and AI.

3.7.2 Cloud Access Security Broker (CASB)

Roles: The CASB is deployed at the tenant's virtual network or virtual server to provide services such as acting as a cloud access agent, identity authentication and access control, data leakage prevention, malicious code detection, configuration, and compliance verification.

Responsibilities: The CASB usually requires access to the application API, application log, application request, or network layer data if deployed at a virtual server.

3.7.3 Key Management-as-a-Service (KMaaS)

Roles: Key management-as-a-service provides distributed/centralized key lifecycle management, data encryption, and/or signature and key usage auditing. Key management-as-a-service supports cloud-native key management for online clients rather than running a key manager on physical servers.

Responsibilities: Key management-as-a-service stores user keys or parts of user keys in the cloud, replaces new keys with old or compromised keys, and restores backup key data when required.

3.8 Security Support Services

Roles: Security support services include managed security services (MSSs) and managed detection and response (MDR) services. The outsourced service providers reduce dedicated enterprise security personnel costs while improving overall protection. An MDR service provider implements threat protection, monitoring, detection, and response capabilities.

Responsibilities: Managed security service providers (MSSPs) enable outsourced monitoring and management of various security devices and tools. They require access to the management plane of managed security devices or tools to view device runtime information and security logs. An MDR service provider furnishes security posture evaluations, threat protections, monitoring, detection, and response assistance. The MSSPs must monitor and analyze all related security logs and events. If some threat is identified, possible response action must be executed (e.g., apply isolation policies, mitigate malicious network traffic, etc.). Note that MSS and MDR services, roles, and responsibilities converge.

3.8.1 Security Configuration Management

Roles: Security configuration management services create baselines to assess cloud asset configurations via scanning, aggregating, and making event correlations. By checking cloud configuration compliances, non-compliant configurations must be remediated.

Responsibilities: Security configuration management services test configurations using scanning applications and then collect and aggregate configuration test results. When some configurations do not meet the initial baseline projections, they must be reported and corrected.

3.8.2 Security Incident Response

Roles: The MDR service plays the role of security incident responder, covering real-time detections, quick responses, and post-incident investigations.

Responsibilities: The detection application must collect as many logs and events as possible to find abnormal behavior and malicious attacks. These logs and events might be useful as input to AI models for training or be examined by human experts. During the response phase, affected resources or endpoints might be contained to avoid further attack. First, however, malicious static resources and runtime entities must be eradicated, and affected systems and businesses must be recovered. During the investigation phase, attack paths should be discovered, and related login credentials and system investigation privileges provided. Moreover, to establish a more credible report, it is possible to reproduce the attack scenario by simulating an attacker’s exploits without a malicious payload.

3.8.3 Security Policy Development

Roles: Security policy development services create and provide cloud security policies that align with cloud users’ risk management and compliance requirements and business objectives.

Responsibilities: Security policy development services cultivate policies and procedures and standards of configuration and maintenance, data protection, logging/audit, user/tenant management, vendor risk assessment, governance risk and compliance (GRC), etc.

3.8.4 Security Updates

Roles: Security update services or patch management services help detect missing patches and remediate cloud asset vulnerabilities.

Responsibilities: Security update services require a patching agent installed in any endpoint which needs security updates. The service collects software information and compares it with known vulnerabilities and security patches using the agent. If security updates are available, the service distributes patches to endpoints and applies these patches.

3.8.5 Security Reporting

Roles: Security reporting services deliver actionable security posture ratings, cyber risk metrics, and security benchmarks by continuously monitoring multi-source objects and data.

Responsibilities: To gain security posture, risk management visibility, and calculate security metrics, the service needs access to various data sources—including real-time and historical monitoring indexes and security alerts. Additionally, the service must associate security events with timelines, user behaviors, and/or knowledge attributes to build context for executives to understand the environment entirely.

3.8.6 Security Training and Education

Roles: Security training and education services deliver online or onsite training courses for enterprise staff and security teams. Enterprise staff learns to avoid threats—such as ransomware or phishing emails—via security awareness education. In contrast, security team members learn red team technologies to hack into systems and corresponding mitigation mechanisms.

Responsibilities: In a well-designed service, the course instructor must understand the enterprise organization, workflows, and asset information and then customize the course tutorials and case scenarios so that a simulated attack is more convincing.

4 Conclusion

Security services are highly segmented, and dramatic innovations must meet the rapid, unrelenting perils that cyber threats pose. It isn't easy (and also unnecessary) to examine all of the available security services in this document. Instead, this analysis defined the market's roles and responsibilities more broadly, focusing on well-recognized security services within eight general categories. These categories include:

> - IAMs
> - Cloud workload protection platforms
> - Network security, data, and storage security
> - Assessment
> - Security analytics-as-a-service
> - Application security
> - Security support services
> - Forty security services

The CSSM working group hopes the roles and responsibilities defined in this document will help CSCs as they sign contracts and SLAs with TPSSPs.

References

BeyondTrust. (2017, November 30). *What is an MSSP (Managed Security Services Provider)?* BeyondTrust. Accessed July 2021. https://www.beyondtrust.com/blog/entry/mssp-managed-security-services-provider

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology* (NIST SP 800-61r2; p. NIST SP 800-61r2) (Page 14). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Gartner. (n.d.). *Gartner Glossary, Information Technology, Glossary Managed Security Service Provider (MSSP)*. Gartner. Accessed July 2021. https://www.gartner.com/en/information-technology/glossary/mssp-managed-security-service-provider

MacDonald, N. & Croll, T. (2020, April 14). *Market Guide for Cloud Workload Protection Platforms. Gartner.* https://www.gartner.com/doc/3983483

SecureStrux. (n.d.). *Managed Security Service Provider (MSSP).* SecureStrux. Accessed July 2021. https://securestrux.com/capabilities/mssp/

Sepior. (n.d.). *Key Management as a Service (KMaaS).* Sepior. Accessed July 2021. https://sepior.com/solutions/kmaas-key-management-as-a-service

StorMagic. (n.d.). *Key Management as a Service (KMaaS).* StorMagic. Accessed July 2021. https://stormagic.com/cloud/kmaas

Vadakkanmarveettil, J. (2021, April 8). *What is MSSP? An Important Overview (2021).* Jigsaw Academy. Accessed July 2021. https://www.jigsawacademy.com/blogs/cyber-security/mssp

Ayal Tirosh, Marc-Antoine Meunier, Magic Quadrant for Data Masking Technology, Worldwide, December 2015. https://www.gartner.com/en/documents/3180344/magic-quadrant-for-data-masking-technology-worldwide