المملكة العربية السعودية
وزارة التربية والتعليم
جامعة الملك فيصل

cloud security

Computer Skills - Group Project

NAME	*ID*
Mohammed abdullah	**222421869**
Mazen saleh alsallouk	**222425169**
Abdullah sami alnasser	**222428554**

- ❑ **Article number:** k6.

Spring Semester
2022\2023

Table Of Contact

TOPIC	Page Number
INTRODUCTION	**2**
What is cloud computing?	**3**
Why is cloud security important?	**5**
What are some cloud security challenges?	**7**
What types of cloud security solutions are available?	**9**
How should you approach cloud security?	**11**
concolution	**13**
references	**15**

INTRODUCTION

Cloud security is a set of practises and tools created to address both internal and external security threats to businesses. As they implement their digital transformation strategy and integrate cloud-based tools and services into their infrastructure, organisations need cloud security. The phrases "digital transformation" and "cloud migration" have become commonplace in business contexts in recent years. Although the meanings of the two expressions vary depending on the organisation, they are both motivated by the same need for change.

Businesses will face new difficulties balancing security and productivity as they adopt these ideas and work to improve their operational strategy. Although moving largely to cloud-based settings can have various ramifications if done insecurely, more contemporary technologies do enable organisations expand capabilities outside the boundaries of on-premise infrastructure.

Understanding how contemporary businesses can profit from the use of linked cloud technology while implementing the finest cloud security practises is necessary for striking the correct balance.

.

What is cloud computing?

The term "cloud" or, more precisely, "cloud computing" refers to the method of gaining access to materials, programmes, and databases via the Internet and outside the constraints of local hardware. Utilising this technology allows businesses to scale their operations with greater flexibility by transferring the majority or a portion of the management of their infrastructure to external hosting companies.

The most common and widely adopted cloud computing services are:

- **IaaS (Infrastructure-as-a-Service):** A hybrid approach, where organizations can manage some of their data and applications on-premise while relying on cloud providers to manage servers, hardware, networking, virtualization, and storage needs.
- **PaaS (Platform-as-a-Service):** Gives organizations the ability to streamline their application development and delivery by providing a custom application framework that automatically manages operating systems, software updates, storage, and supporting infrastructure in the cloud.
- **SaaS (Software-as-a-Service):** Cloud-based software hosted online and typically available on a subscription basis. Third-party providers manage all potential technical issues, such as data, middleware, servers, and storage, minimizing IT resource expenditures and streamlining maintenance and support functions.

Why is cloud security important?

The adoption of cloud-based environments and IaaS, PaaS, or SaaS computing models has increased in contemporary organisations. When organisations effectively resource their departments, the dynamic nature of infrastructure management, particularly in scaling applications and services, can present a number of issues. Organisations may outsource many of the time-consuming IT-related duties thanks to these as-a-service models.

Understanding the security standards for keeping data safe has become essential as businesses continue to shift to the cloud. Although third-party cloud computing service providers might take over the management of this infrastructure, the accountability and security of data assets may not necessarily move with it.

The majority of cloud service providers actively secure the integrity of their servers by default adhering to best security practises. When it comes to safeguarding data, applications, and workloads that are hosted in the cloud, organisations must take their unique factors into account.

With the continued development of the digital environment, security concerns have advanced. Due to an organization's general lack of visibility in data access and movement, these risks specifically target suppliers of cloud computing. Organisations may encounter serious governance and compliance concerns when handling client information, regardless of where it is housed, if they don't take proactive measures to increase their cloud security.

No of the size of your company, cloud security needs to be a major talking point. Almost every aspect of contemporary computing is supported by cloud infrastructure, which spans several verticals and all sectors.

However, successful cloud adoption is dependent on putting in place adequate countermeasures to defend against modern-day cyberattacks. Regardless of whether your organization operates in a public, private, or hybrid cloud environment, cloud security solutions and best practices are a necessity when ensuring business continuity.

What are some cloud security challenges?

Lack of visibility

It's easy to lose track of how your data is being accessed and by whom, since many cloud services are accessed outside of corporate networks and through third parties.

Multitenancy

Public cloud environments house multiple client infrastructures under the same umbrella, so it's possible your hosted services can get compromised by malicious attackers as collateral damage when targeting other businesses.

Access management and shadow IT

While enterprises may be able to successfully manage and restrict access points across on-premises systems, administering these same levels of restrictions can be challenging in cloud environments. This can be dangerous for organizations that don't deploy bring-your-own device (BYOD) policies and allow unfiltered access to cloud services from any device or geolocation.

Compliance

Regulatory compliance management is oftentimes a source of confusion for enterprises using public or hybrid cloud deployments. Overall accountability for data privacy and security still rests with the enterprise, and heavy reliance on third-party solutions to manage this component can lead to costly compliance issues.

Misconfigurations

Misconfigured assets accounted for 86% of breached records in 2019, making the inadvertent insider a key issue for cloud computing environments. Misconfigurations can include leaving default administrative passwords in place, or not creating appropriate privacy settings.

What types of cloud security solutions are available?

Identity and access management (IAM)
Identity and access management (IAM) tools and services allow enterprises to deploy policy-driven enforcement protocols for all users attempting to access both on-premises and cloud-based services. The core functionality of IAM is to create digital identities for all users so they can be actively monitored and restricted when necessary during all data interactions

Data loss prevention (DLP)
Data loss prevention (DLP) services offer a set of tools and services designed to ensure the security of regulated cloud data. DLP solutions use a combination of remediation alerts, data encryption, and other preventative measures to protect all stored data, whether at rest or in motion.

Security information and event management (SIEM)
Security information and event management (SIEM) provides a comprehensive security orchestration solution that automates threat monitoring, detection, and response in cloud-based environments. Using artificial intelligence (AI)-driven technologies to correlate log data across multiple platforms and digital assets, SIEM technology gives IT teams the ability to successfully apply their network security protocols while being able to quickly react to any potential threats.

Business continuity and disaster recovery
Regardless of the preventative measures organizations have in place for their on-premise and cloud-based infrastructures, data breaches and disruptive outages can still occur. Enterprises must be able to quickly react to newly discovered vulnerabilities or significant system outages as soon as possible. Disaster recovery

solutions are a staple in cloud security and provide organizations with the tools, services, and protocols necessary to expedite the recovery of lost data and resume normal business operations.

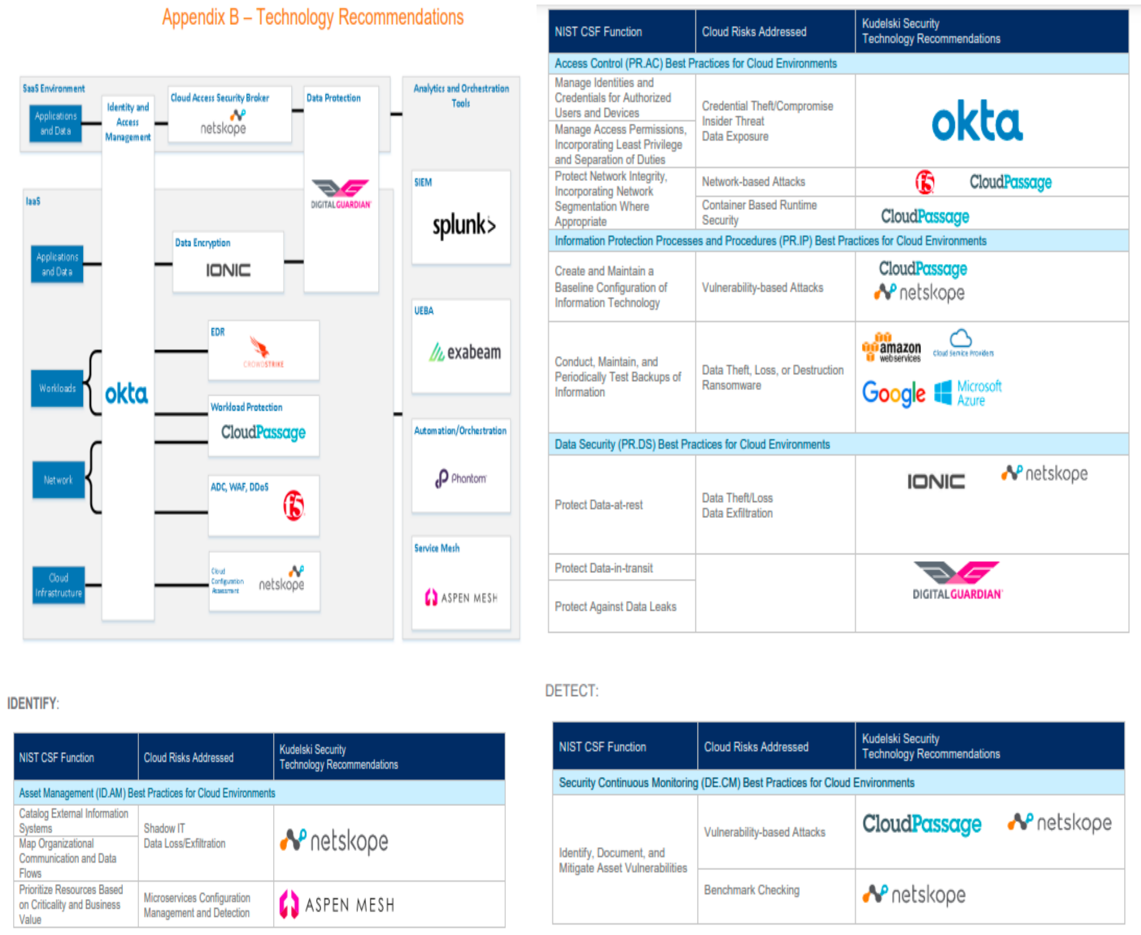
How should you approach cloud security?

The way to approach cloud security is different for every organization and can be dependent on several variables. However, the National Institute of Standards and Technology (NIST) has made a list of best practices that can be followed to establish a secure and sustainable cloud computing framework.

The NIST has created necessary steps for every organization to self-assess their security preparedness and apply adequate preventative and recovery security measures to their systems. These principles are built on the NIST's five pillars of a cybersecurity framework: Identify, Protect, Detect, Respond, and Recover.

Another emerging technology in cloud security that supports the execution of NIST's cybersecurity framework is cloud security posture management (CSPM). CSPM solutions are designed to address a common flaw in many cloud environments - misconfigurations.

Cloud infrastructures that remain misconfigured by enterprises or even cloud providers can lead to several vulnerabilities that significantly increase an organization's attack surface. CSPM addresses these issues by helping to organize and deploy the core components of cloud security. These include identity and access management (IAM), regulatory compliance management, traffic monitoring, threat response, risk mitigation, and digital asset management.



Appendix B – Technology Recommendations

SaaS Environment
Applications and Data
Identity and Access Management
Cloud Access Security Broker
netskope
Data Protection
DIGITALGUARDIAN
Analytics and Orchestration Tools
IaaS
Applications and Data
Data Encryption
IONIC
SIEM
splunk>
EDR
CROWDSTRIKE
UEBA
exabeam
Workloads
okta
Workload Protection
CloudPassage
Automation/Orchestration
Phantom
Network
ADC, WAF, DDoS
f5
Service Mesh
Cloud Infrastructure
Cloud Configuration Assessment
netskope
ASPEN MESH

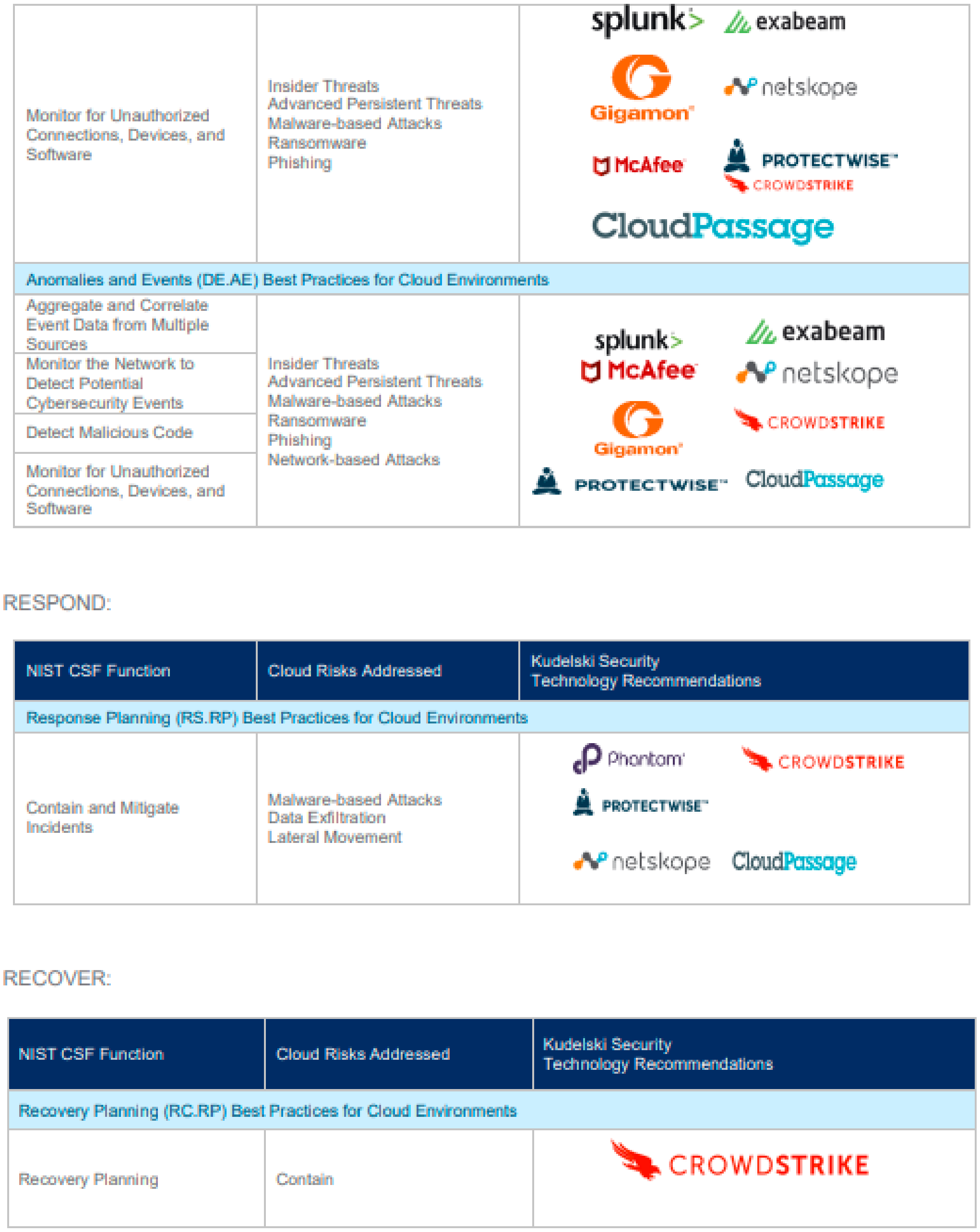
NIST CSF Function	Cloud Risks Addressed	Kudelski Security Technology Recommendations
Access Control (PR.AC) Best Practices for Cloud Environments		
Manage Identities and Credentials for Authorized Users and Devices	Credential Theft/Compromise Insider Threat Data Exposure	okta
Manage Access Permissions, Incorporating Least Privilege and Separation of Duties		
Protect Network Integrity, Incorporating Network Segmentation Where Appropriate	Network-based Attacks	f5 CloudPassage
	Container Based Runtime Security	CloudPassage
Information Protection Processes and Procedures (PR.IP) Best Practices for Cloud Environments		
Create and Maintain a Baseline Configuration of Information Technology	Vulnerability-based Attacks	CloudPassage netskope
Conduct, Maintain, and Periodically Test Backups of Information	Data Theft, Loss, or Destruction Ransomware	amazon webservices Cloud Service Providers Google Microsoft Azure
Data Security (PR.DS) Best Practices for Cloud Environments		
Protect Data-at-rest	Data Theft/Loss Data Exfiltration	IONIC netskope
Protect Data-in-transit		DIGITALGUARDIAN
Protect Against Data Leaks		

IDENTIFY:

NIST CSF Function	Cloud Risks Addressed	Kudelski Security Technology Recommendations
Asset Management (ID.AM) Best Practices for Cloud Environments		
Catalog External Information Systems	Shadow IT Data Loss/Exfiltration	netskope
Map Organizational Communication and Data Flows		
Prioritize Resources Based on Criticality and Business Value	Microservices Configuration Management and Detection	ASPEN MESH

DETECT:

NIST CSF Function	Cloud Risks Addressed	Kudelski Security Technology Recommendations
Security Continuous Monitoring (DE.CM) Best Practices for Cloud Environments		
Identify, Document, and Mitigate Asset Vulnerabilities	Vulnerability-based Attacks	CloudPassage netskope
	Benchmark Checking	netskope



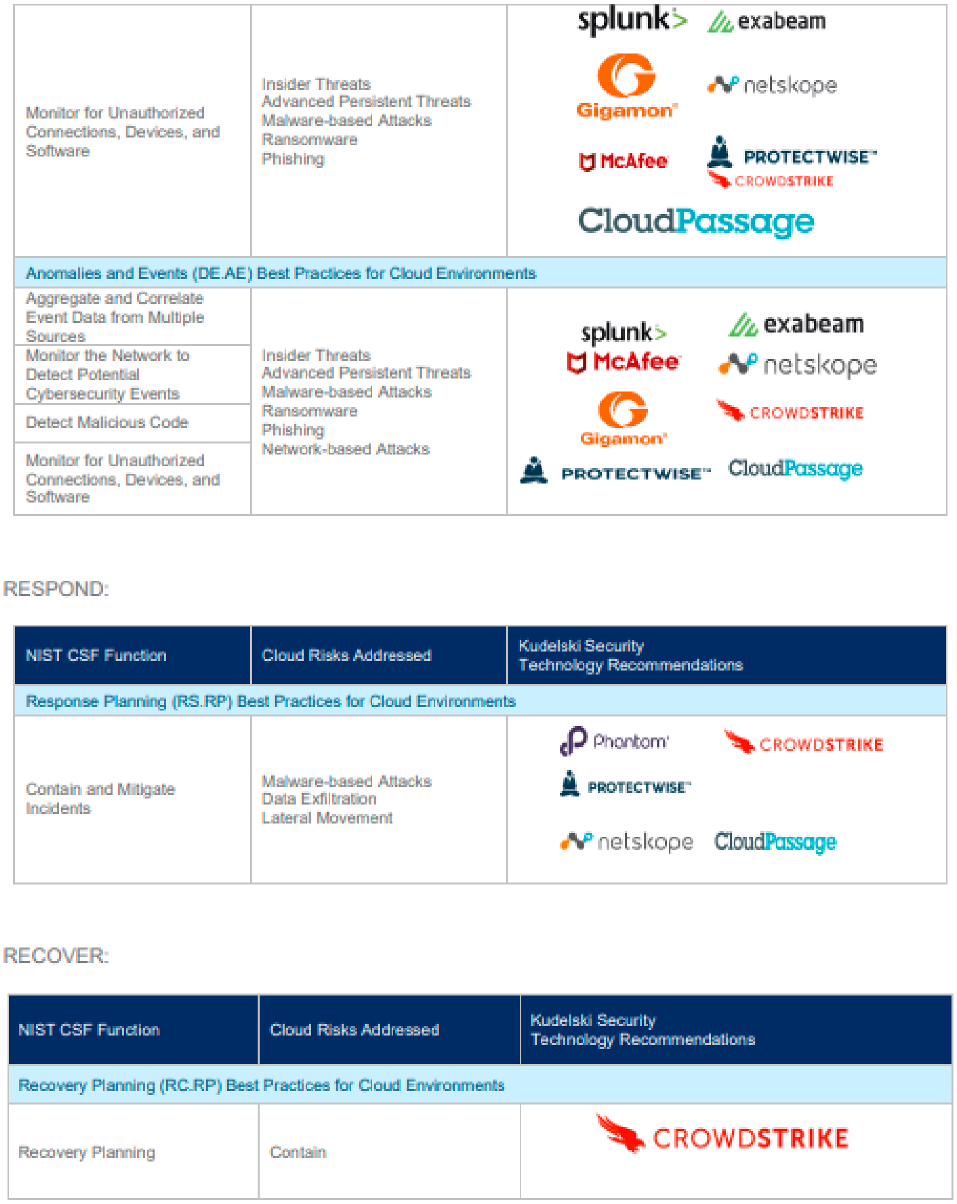
Monitor for Unauthorized Connections, Devices, and Software	Insider Threats Advanced Persistent Threats Malware-based Attacks Ransomware Phishing	splunk exabeam Gigamon netskope McAfee PROTECTWISE CROWDSTRIKE CloudPassage
Anomalies and Events (DE.AE) Best Practices for Cloud Environments		
Aggregate and Correlate Event Data from Multiple Sources	Insider Threats Advanced Persistent Threats Malware-based Attacks Ransomware Phishing Network-based Attacks	splunk exabeam McAfee netskope Gigamon CROWDSTRIKE PROTECTWISE CloudPassage
Monitor the Network to Detect Potential Cybersecurity Events		
Detect Malicious Code		
Monitor for Unauthorized Connections, Devices, and Software		

RESPOND:

NIST CSF Function	Cloud Risks Addressed	Kudelski Security Technology Recommendations
Response Planning (RS.RP) Best Practices for Cloud Environments		
Contain and Mitigate Incidents	Malware-based Attacks Data Exfiltration Lateral Movement	Phantom CROWDSTRIKE PROTECTWISE netskope CloudPassage

RECOVER:

NIST CSF Function	Cloud Risks Addressed	Kudelski Security Technology Recommendations
Recovery Planning (RC.RP) Best Practices for Cloud Environments		
Recovery Planning	Contain	CROWDSTRIKE



Monitor for Unauthorized Connections, Devices, and Software	Insider Threats Advanced Persistent Threats Malware-based Attacks Ransomware Phishing	splunk> exabeam Gigamon® netskope McAfee PROTECTWISE™ CROWDSTRIKE CloudPassage
Anomalies and Events (DE.AE) Best Practices for Cloud Environments		
Aggregate and Correlate Event Data from Multiple Sources	Insider Threats Advanced Persistent Threats Malware-based Attacks Ransomware Phishing Network-based Attacks	splunk> exabeam McAfee netskope Gigamon® CROWDSTRIKE PROTECTWISE™ CloudPassage
Monitor the Network to Detect Potential Cybersecurity Events		
Detect Malicious Code		
Monitor for Unauthorized Connections, Devices, and Software		

RESPOND:

NIST CSF Function	Cloud Risks Addressed	Kudelski Security Technology Recommendations
Response Planning (RS.RP) Best Practices for Cloud Environments		
Contain and Mitigate Incidents	Malware-based Attacks Data Exfiltration Lateral Movement	Phantom® CROWDSTRIKE PROTECTWISE™ netskope CloudPassage

RECOVER:

NIST CSF Function	Cloud Risks Addressed	Kudelski Security Technology Recommendations
Recovery Planning (RC.RP) Best Practices for Cloud Environments		
Recovery Planning	Contain	CROWDSTRIKE

CONCOLUTION

Cloud security involves the procedures and technology that secure cloud computing environments against both external and insider cybersecurity threats. Cloud computing, which is the delivery of information technology services over the internet, has become a must for businesses and governments seeking to accelerate innovation and collaboration. Cloud security and security management best practices designed to prevent unauthorized access are required to keep data and applications in the cloud secure from current and emerging cybersecurity threats.

REFERENCES

1. Cloud Computing PaaS Enterprise Design Pattern § (2010). https://www.ea.oit.va.gov/EAOIT/docs/April2017docs/041117 EDP Cloud-Computing-PaaS- EDP-v1.pdf.
2. Continuous Diagnostics and Mitigation Program § (2020). https://www.gsa.gov/cdnstatic/CDM%20Tech Cap Vol Two Req Catalog 2020 RFinal 10 2% 20. Pdf.
3. "Digital Services Playbook." The Digital Services Playbook - from the U.S. Digital Service. Accessed July 9, 2021. https: // playbook.cio.gov/.
4. Department of Defense Enterprise DevSecOps Reference Design § (2019). https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0 Public%20Release.pdf.
5. "Enterprise Architecture Quick Guide." Cloud Security Alliance, 2011. https://downloads.cloudsecurityalliance.org/initiatives/eawg/EAWG Whitepaper.pdf.
6. "Federal ICAM Architecture Introduction." GSA. Accessed November 18, 2021. https://playbooks.idmanagement.gov/arch/.
7. Gartner, Inc. "How to Protect Your Clouds With CSPM, CWPP, CNAPP and CASB." Gartner, May 6, 2021. https://www.gartner.com/en/documents/4001348/how-to-protect-your-clouds-with-cspm-
8. cwpp-cnapp-and-casb. Gartner, Inc. "Innovation Insight for Cloud Security Posture Management." Gartner, January 25, 2019. https://www.gartner.com/en/documents/3899373/innovation-insight-for-cloud-security-posture- management.
9. Gwosdz, Medi Madelen. "The Rise of the DevOps Mindset." Stack Overflow Blog, June 22, 2020. https://stackoverflow.blog/2020/06/10/the-rise-of-the-devops-mindset/.
10. Lui, Fang, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger, and Dawn Leaf, NIST Cloud
11. Computing Reference Architecture § (2011). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf.
12. Mell, Peter, and Timothy Grance, The NIST Definition of Cloud Computing § (2011).
13. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.
14. National Cybersecurity Protection System (NCPS) Cloud Interface Reference Architecture § (2020).