CompTIA®

For more information contact:

Marie Cronin

Senior Manager Skills Certification, Western Europe
https://www.linkedin.com/in/marie-cronin-comptia/

CompTIA

The Voice of the World's IT Industry and over 2 million IT Professionals

ASSOCIATION

7000+ IT Channel Providers & Partners

A non-profit trade association with more than 7,000 members and business partners. Our members drive our programs through their participation in CompTIA communities, research studies, events, sharing of best practices and more.

PHILANTHROPY

Creating IT Futures

A 501(c)(3) charitable organization that creates on-ramps for successful IT careers, serving individuals who are underrepresented in IT and lacking in opportunities to be successful in IT, including veterans, youth, and the unemployed.

CERTIFICATIONS

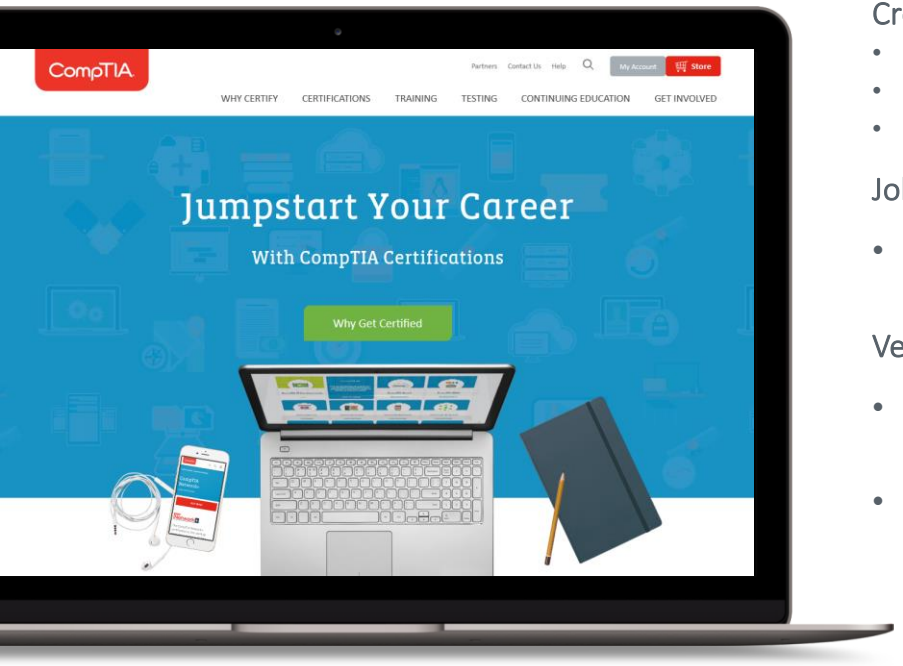
Largest Provider of Vendor-Neutral IT Certifications

- ✓ Higher Salaries
- ✓ Growing Demand
- ✓ Verified Strengths
- ✓ Universal Skills

"Three of the 'Top 10 Certifications That Help IT Workers Get Jobs' are CompTIA certifications."*

* Source: The Dice Report, February 2012

Worldwide Leading Provider of Vendor-Neutral IT Certifications



Created by Industry for Industry

- Relevant
- Regularly updated
- Internationally Recognised

Job Role Led

- Span entry level roles – to help entrants to the their first job – through to more advanced roles

Vendor Neutral / Inclusive

- Independent of any particular technology, product or platform
- Reflect the diverse technologies deployed in today's organisation

CompTIA A+ CompTIA Network+ CompTIA Security+

COGEnT

Overview:

A consortium of 4 leading universities (**Cambridge, Oxford, Glasgow and Edinburgh)** championing the T-Shaped worker among technical staff within their institutions. Collaboration has been consistent with all X4 Uni's and CompTIA

Result – gives each University particularly those linked to APUC SUPC easy access to training materials and Academic discounts – 80% COURSEWARE / 50% EXAMS

UNIVERSITY OF CAMBRIDGE

UNIVERSITY OF OXFORD

University of Glasgow

THE UNIVERSITY of EDINBURGH

CompTIA The IT Industry Trade Association

WHO WE ARE

CompTIA is a global, not-for-profit IT trade association and the voice of the industry

OUR MISSION

Advance the IT industry

Technology is infrastructure, just like roads and bridges. Our economic growth, national security and quality of life depend on it. When we help tech businesses grow and help build a skilled tech workforce, we make that infrastructure stronger.

WHO WE SERVE

Tech businesses, tech professionals, tech educators, and anyone interested in a tech career or a vibrant tech industry.

- Membership
- Education
- Certification
- Public Sector
- Philanthropy
- Media and industry partners

Working in the Cloud –
Perceptions from CompTIA

COGEnT

23 February, 2021

CompTIA

Your presenter

Twitter:
@jamesstanger

James Stanger, PhD

Chief Technology Evangelist - CompTIA
A+, Network+, Security+, MCSE, LPI LPIC 1, Symantec STA

Award-winning author and educator. Responsible for working with IT pros, hiring managers, and helping shape CompTIA educational standards to close the skills gap. I also help students worldwide. I have experience in:

- *Cloud security*
- *Security analytics and monitoring*
- *Pen testing, red teaming*
- *Emerging technology (e.g., blockchain, AI & ML)*
- *Linux and open source*
- *Threat hunting*
- *Network administration*
- *Web technologies*
- *Certification development*
- *Award-winning author and instructor*

LinkedIn:
https://www.linkedin.com/in/jamesstanger

CompTIA blog page:
https://tinyurl.com/y6pdw72g

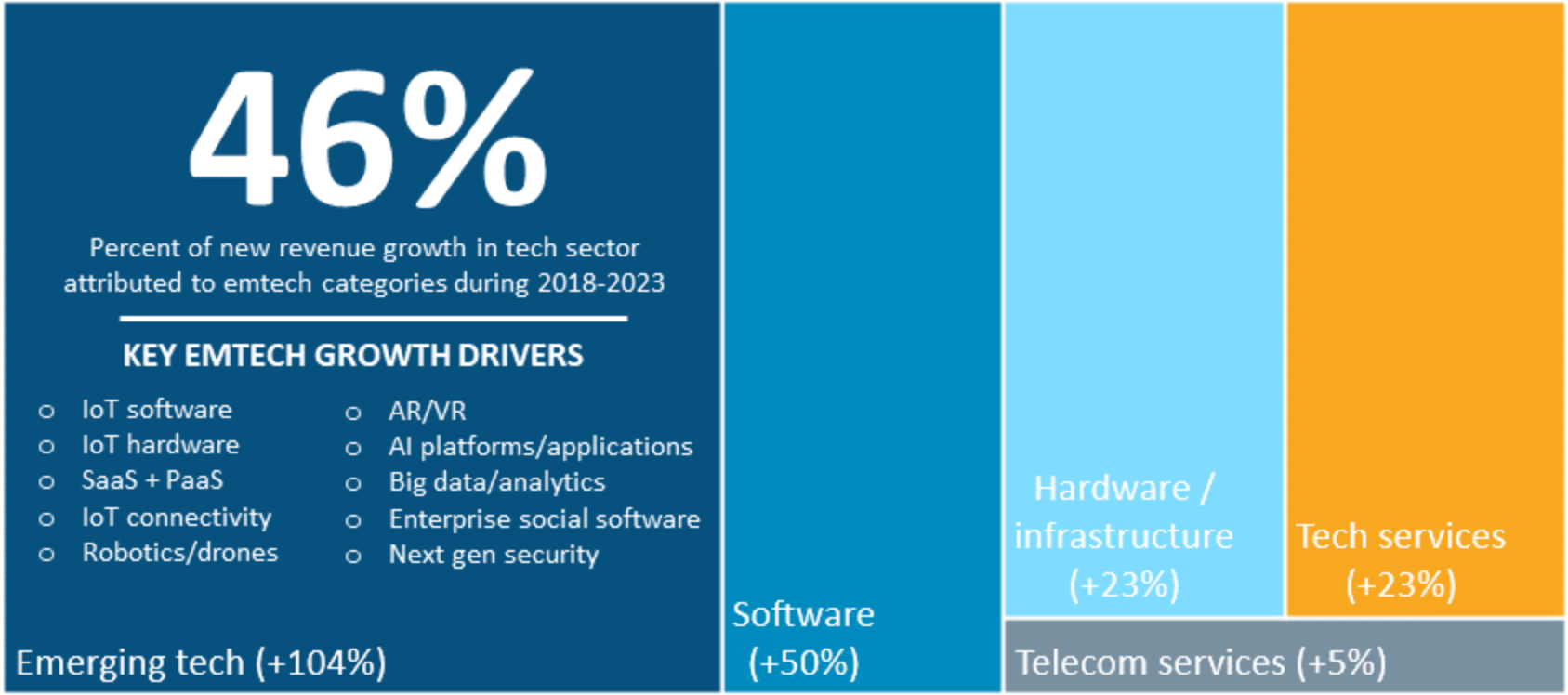
Agenda

- The “cloud landscape” – Trends in the cloud
- Overview of Cloud Essentials
- Cloud+ updates
- The CompTIA IT roadmap
- Q & A

Let’s discuss trends we’re finding in regards to the cloud, as well as CompTIA’s Cloud+ and Cloud Essentials training and certification programs.

The “cloud landscape” – Trends we’re seeing in the cloud

Emerging tech categories driving growth through 2023

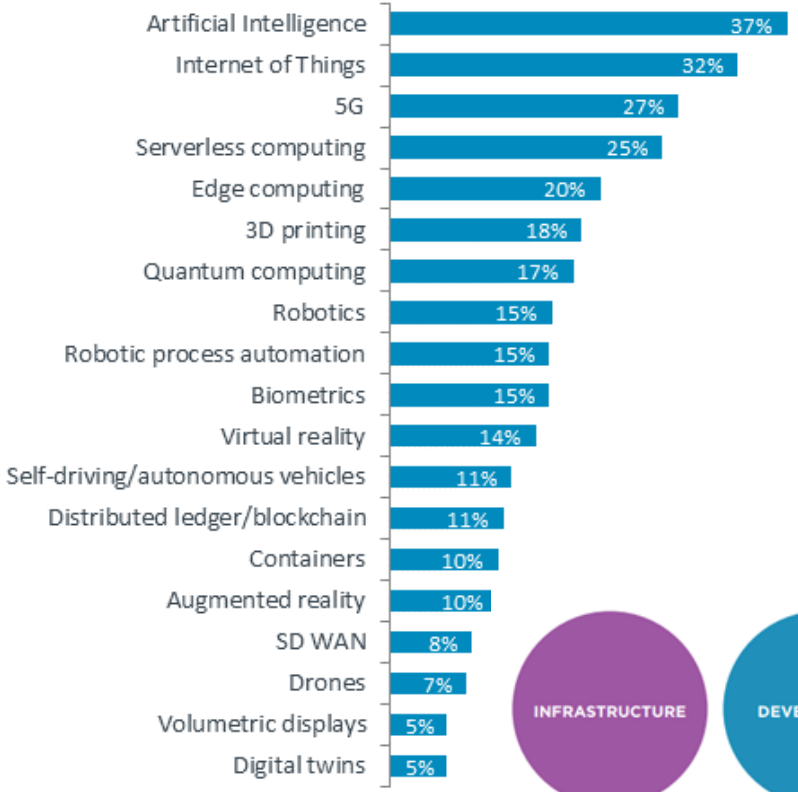


Source: IDC

The above revenue drivers are also the building blocks of modern IT

The technology that makes business move forward (business perspective)

- The IT pro sees that AI, IoT, and 5G are extremely important
- Why?
  - Improves our computing environment
  - Customer experience



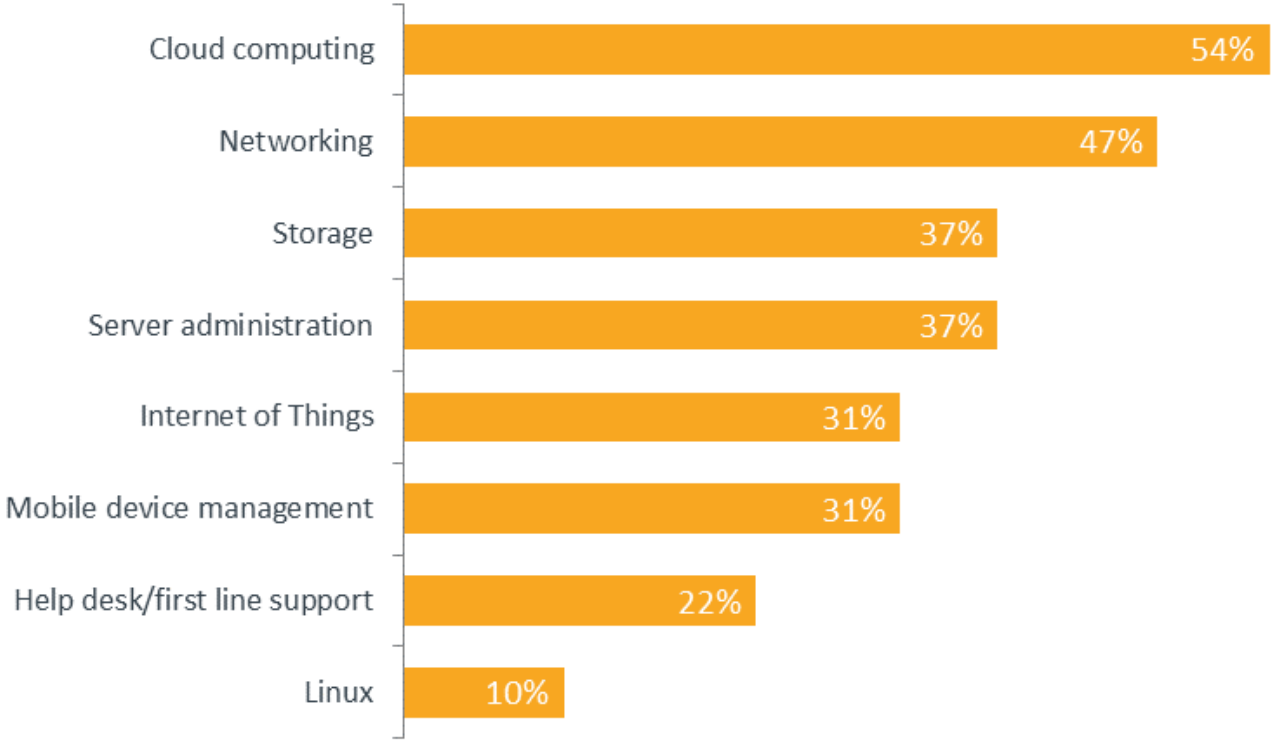
Respondents were asked to select the three technologies that they believed held the most potential for their business

https://www.comptia.org/blog/the-four-pillars-of-an-it-framework

The IT pro's perspective of the business

- These are the building blocks for our ambient computing world
- They support the 4th industrial revolution
- Reflects today's hybrid environment

Where do we get our AI and emerging tech? From the cloud . . .

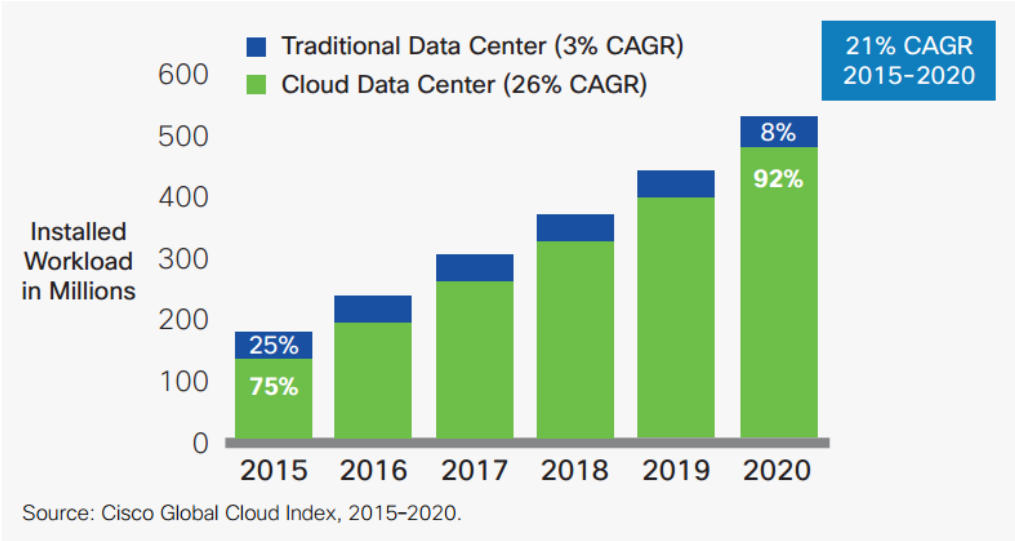


Cloud expertise is hard to find

Top 3 Cloud Challenges

- Lack of resources/expertise
- Security
- Managing cloud spend

Source: RightScale 2017 State of the Cloud Report



Source: Cisco Global Cloud Index, 2015-2020.

In January of 2021, Microsoft noted that the lack of cloud-specific skills has slowed adoption worldwide

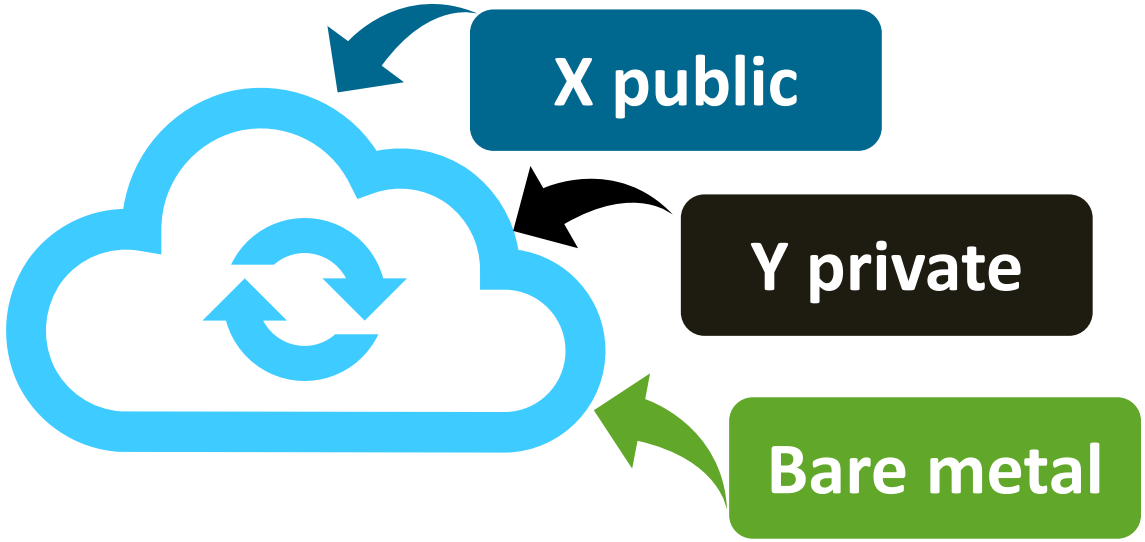
Multi-cloud environments

- Vendor lock-in – a real worry
- How do you choose the right tool for the right job?
- Making informed choices

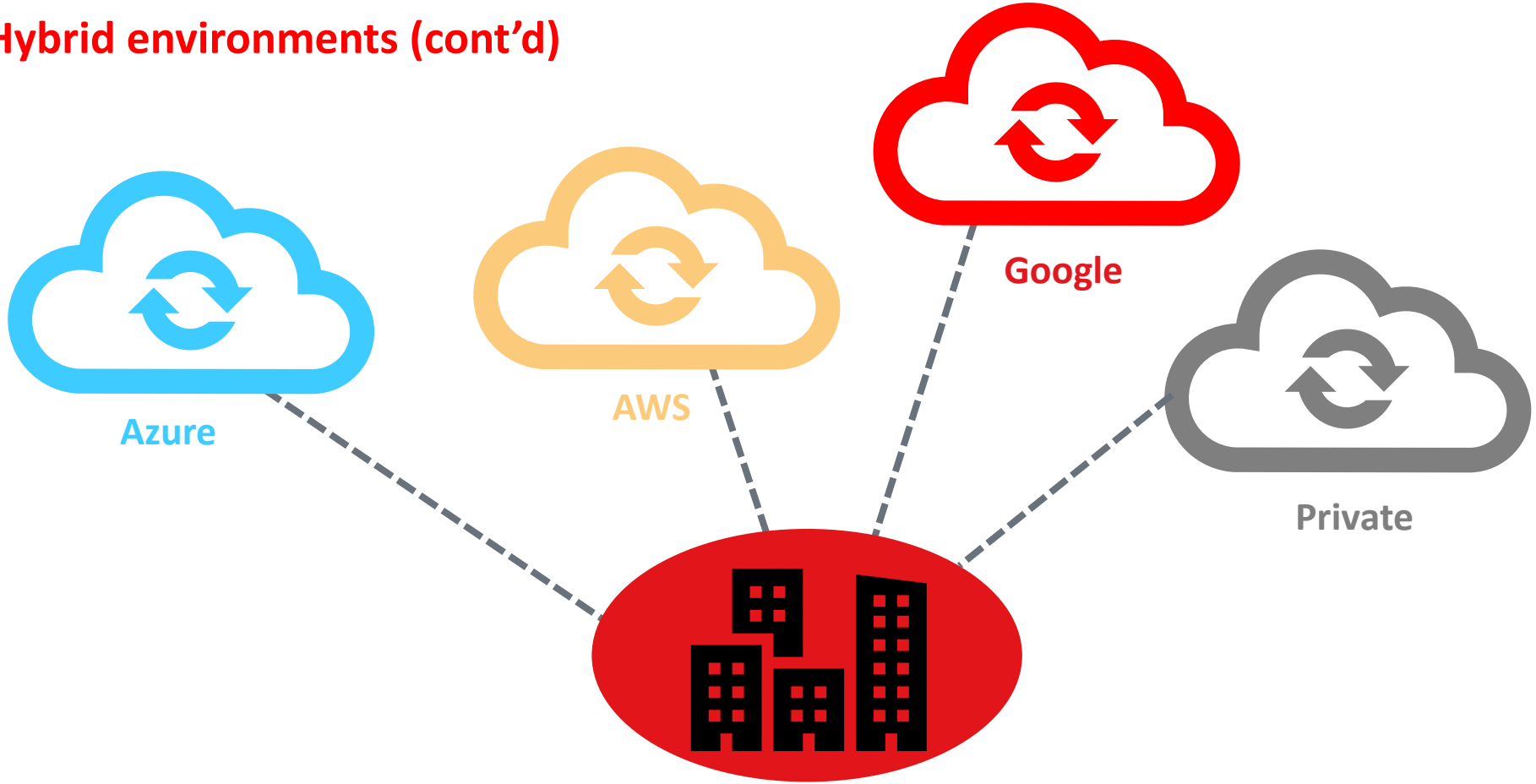
IBM Cloud

Hybrid environments

- Deploying across two or more environments
  - Portability
  - Orchestration
  - Management
- Choosing models
  - Public
  - Private



Hybrid environments (cont'd)



IT Industry Outlook 2021

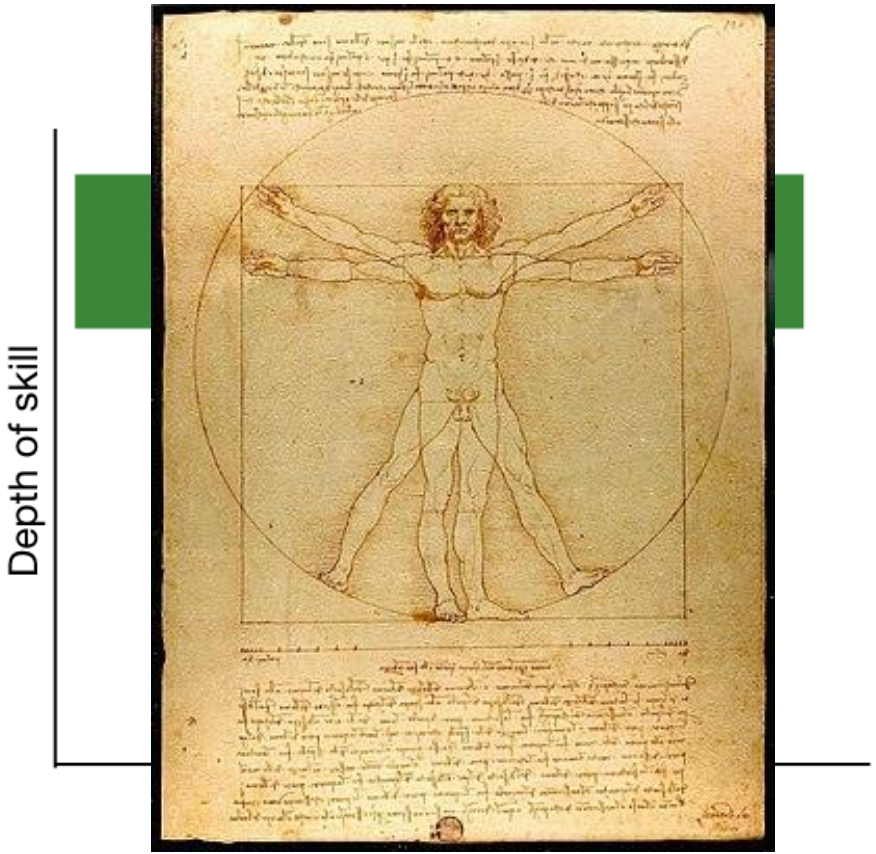
- No “normal”
- Cloud is king
- Tech pros now talk business
- Zero trust – an essential skill
- Governance / regulation – in all sectors
- Diversity

URL: https://www.comptia.org/content/research/it-industry-trends-analysis

the “T-shaped worker”

The T-shaped individual

- Individuals who understand
  - System diversity
  - Mapping business needs to tech
  - How information flows from one system to another
  - Complex, multi-vendor situations
- Teamwork is *essential*
  - Complex reasoning
  - Emotional intelligence
- Helps make strategic choices about the cloud



getting the most out of the cloud

Strategic IT – a major evolution

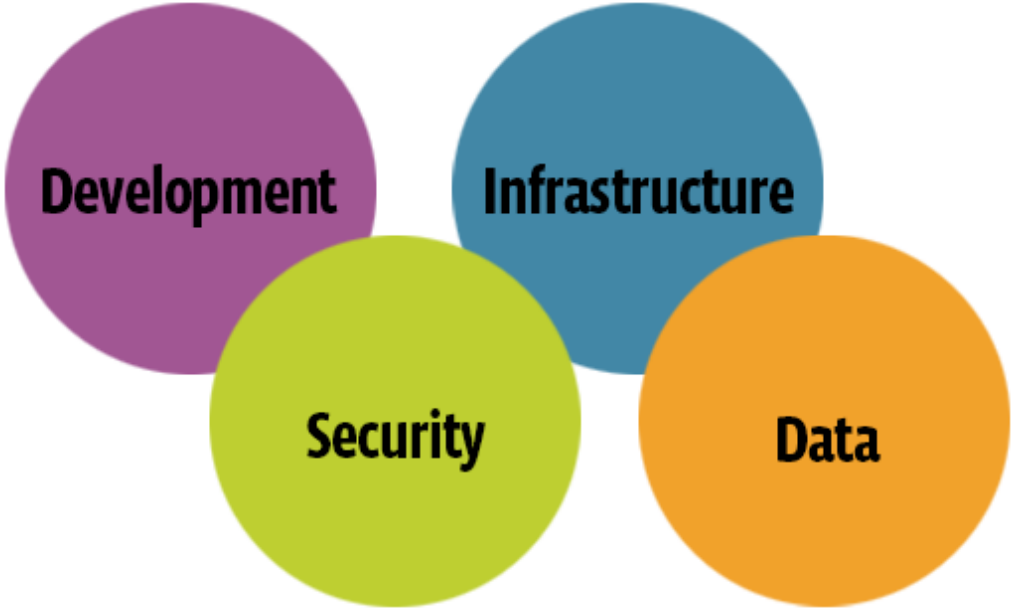
- Two perspectives
- Corporations need partners that know "the business of tech" and "the tech of business"

Traditional viewpoint:
Business objectives were driven by business units, which were supported by operational IT

Modern viewpoint:
Strategic IT works alongside business units to help drive objectives, with operational IT still acting as a foundation

The cloud and the pillars of IT

- Four pillars of IT
- Cloud is in all four
- Or, they are all in the cloud
- Depends upon your perspective

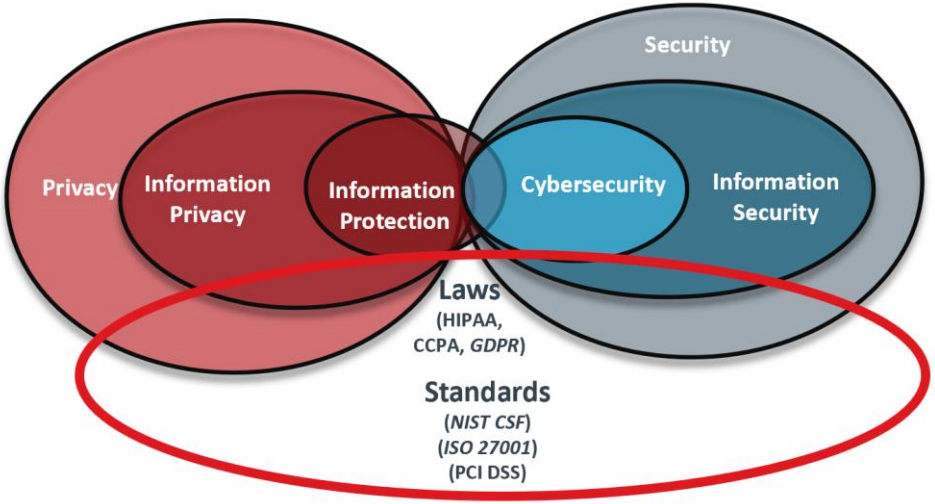


Source:
https://www.comptia.org/blog/the-four-pillars-of-an-it-framework

IT today

IT today:
Information custodians / curators

- If possession is 9/10^{ths} of the law, then . .
- IT workers possess the data
  - Intellectual Property (IP)
  - Personally Identifiable Information (PII)
- We need ***information curators***
- Partners must provide “knowledge workers”
- But it’s really more than that

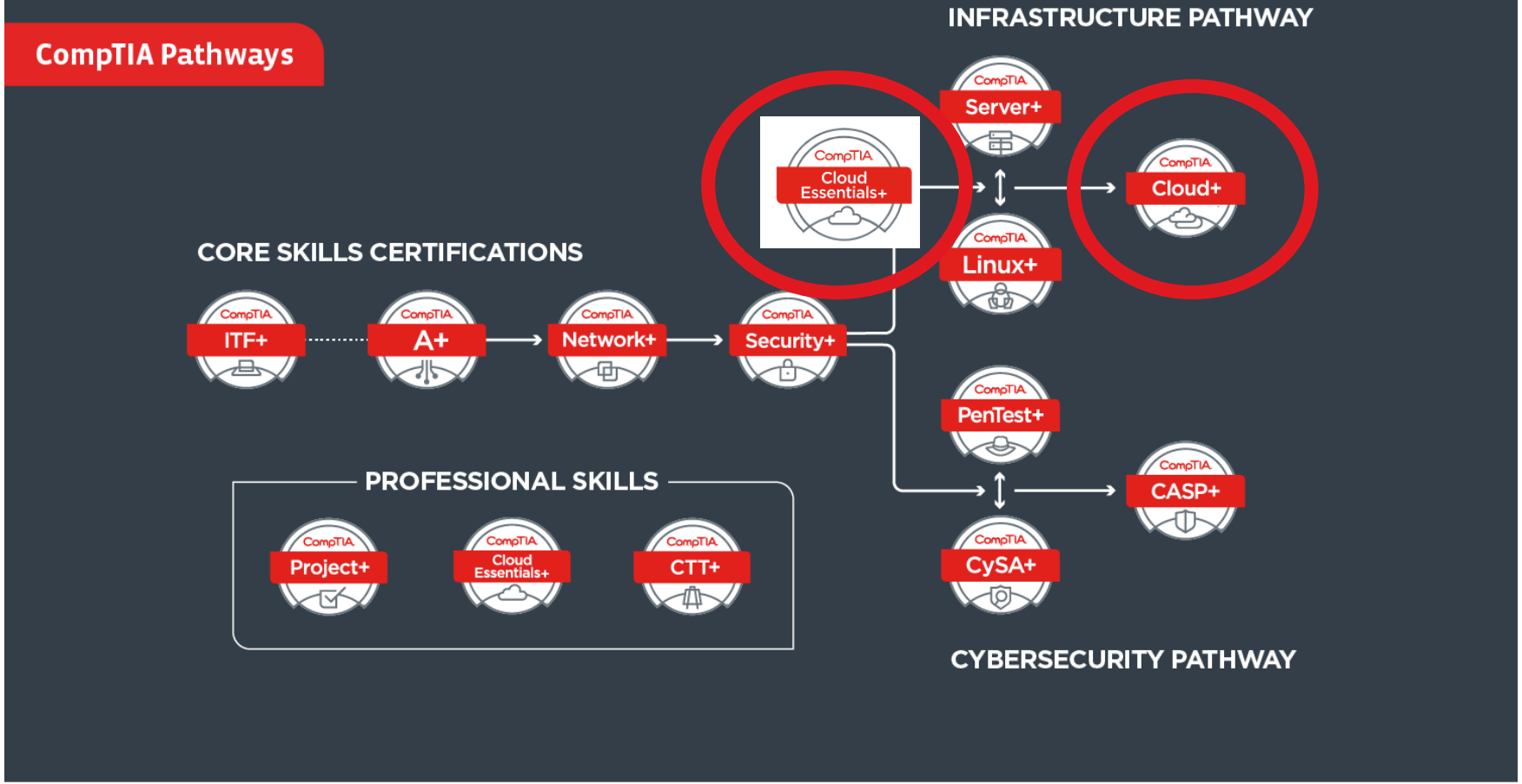


Guardians of identity

- More than:
  - Systems
  - Data
  - Information
- IT workers protect our ***modern identities***
- The cloud is where identities will reside, increasingly

CompTIA IT roadmap

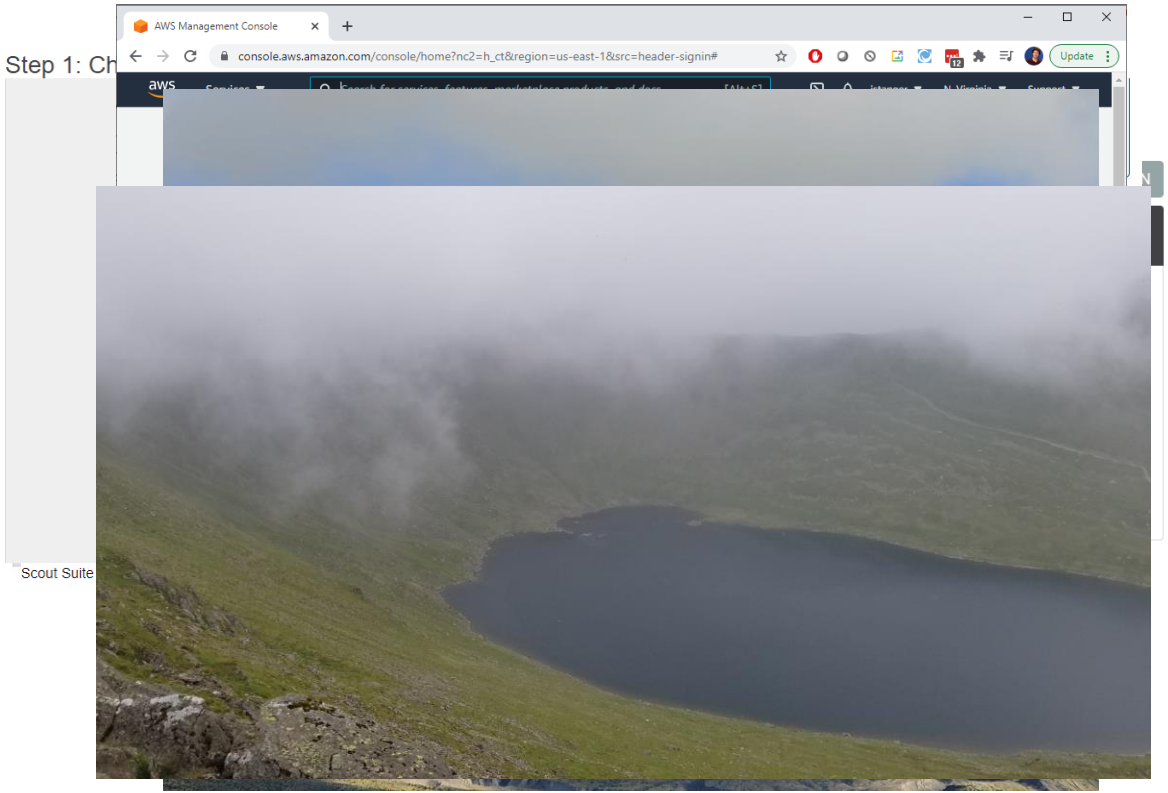
Enter where it makes sense for you . . .



skills we need in cloud workers

The primary attack surface: The cloud

- We currently source many solutions from the cloud – will will continue to do so!
- Are we acting securely?
- In most cases, current practices – what I call “cowboy IT,” just aren’t getting the job done



Organisations that use Cloud Essentials and Cloud+

System Administrator	Systems Engineer
Network Administrator	Network Engineer
Cloud Developer	Cloud Specialist
Project Manager, Cloud	Computing Services
Cloud Engineer	Manager, Data Center SANs
Business Analyst, Cloud Computing	

Overview of Cloud Essentials

- The business of the cloud
- The foundation for a successful implementation
- For “techies” and ***non-techies***

DOMAIN	PERCENTAGE OF EXAMINATION
1.0 Cloud Concepts	24%
2.0 Business Principles of Cloud Environments	28%
3.0 Management and Technical Operations	26%
4.0 Governance, Risk, Compliance, and Security for the Cloud	22%
Total	**100%**

Why Cloud Essentials?

- Primary issues encountered by today's IT managers
  - Workers have difficulty mapping technology to business
  - Lack of cross-departmental communication
  - Workers that don't know "foundations"
    - Technical
    - Non-technical

https://www.comptia.org/certifications/cloud-essentials#overview

Why Cloud Essentials? (cont'd)

- Domain 1.0 makes sure everyone has the same vocabulary

1.1 Explain cloud principles.

- **Service models**
  - SaaS
  - IaaS
  - PaaS
- **Deployment models**
  - Public
  - Private
  - Hybrid
- **Characteristics**
  - Elastic
  - Self-service
  - Scalability
  - Broad network access
  - Pay-as-you-go
  - Availability
- **Shared responsibility model**

1.2 Identify cloud networking concepts.

- **Connectivity types**
  - Direct connect
  - VPN
- **Common access types**
  - RDP
  - SSH
  - HTTPS
- **Software-defined networking (SDN)**
- **Load balancing**
- **DNS**
- **Firewall**

1.3 Identify cloud storage technologies.

- **Storage features**
  - Compression
  - Deduplication
  - Capacity on demand
- **Storage types**
  - Object storage
  - File storage
  - Block storage

Why Cloud Essentials?

- Domain 2.0
- Notice the emphasis on the "why" of the cloud

2.1 Given a scenario, use appropriate cloud assessments.

- **Current and future requirements**
- **Baseline**
- **Feasibility study**
- **Gap analysis**
  - Business
  - Technical
- **Reporting**
  - Compute
  - Network
  - Storage
- **Benchmarks**
- **Documentation and diagrams**
- **Key stakeholders**
- **Point of contact**

2.2 Summarize the financial aspects of engaging a cloud provider.

- **Capital expenditures**
- **Operating expenditures**
- **Variable vs. fixed cost**
- **Licensing models**
  - BYOL
  - Subscription
- **Contracts**
- **Billing**
- **Request for information**
- **Human capital**
  - Training
  - Professional development

2.3 Identify the important business aspects of vendor relations in cloud adoptions.

- **Professional services**
  - Time to market
- **Training**
- **Evaluations**

Why Cloud Essentials? (cont'd)

- Domain 3.0
  - An overview of operations
  - Some tech – just to make sure everyone is on the same page
  - Sets the stage for Cloud+, as well

3.1 Explain aspects of operating within the cloud.

- **Data management**
  - Replication
  - Locality
  - Backup
- **Availability**
  - Zones
  - Geo-redundancy
- **Disposable resources**
- **Monitoring and visibility**
  - Alerts
  - Logging
- **Optimization**
  - Auto-scaling
  - Right-sizing

3.2 Explain DevOps in cloud environments.

- **Provisioning**
  - Infrastructure as code
  - Templates
- **Continuous integration/ continuous delivery**
- **Testing in QA environments**
  - Sandboxing
  - Load testing
  - Regression testing
- **Configuration management**
  - Orchestration
  - Automation
  - Upgrades and patching
- **API integration**

3.3 Given a scenario, review and report on the financial expenditures related to cloud resources.

- **Storage**
- **Network**
- **Compute**
- **Chargebacks**
  - Resource tagging
- **Instances**
  - Reserved
  - Spot
- **Licensing type**
- **Licensing quantity**

Why Cloud Essentials? (cont'd)

- Domain 4.0 – the value of security and privacy

4.0 Governance, Risk, Compliance, and Security for the Cloud

4.1 Recognize risk management concepts related to cloud services.

- **Risk assessment**
  - Asset inventory
  - Classification
  - Ownership
- **Risk response**
  - Mitigation
  - Acceptance
  - Avoidance
  - Transfer
- **Documentation**
  - Findings
  - Risk register
- **Vendor lock-in**
- **Data portability**

4.2 Explain policies or procedures.

- **Standard operating procedures**
- **Change management**
- **Resource management**
- **Security policies**
  - Incident response
- **Access and control policies**
- **Department specific policies**
- **Communication policies**

4.3 Identify the importance and impacts of compliance in the cloud.

CompTIA Cloud+

Why Cloud+

- Technical emphasis
- Focus is on implementation

DOMAIN	PERCENTAGE OF EXAMINATION
1.0 Cloud Architecture and Design	13%
2.0 Security	20%
3.0 Deployment	23%
4.0 Operations and Support	22%
5.0 Troubleshooting	22%
Total	**100%**

Cloud+ 003
(live, May 2021)

https://www.comptia.org/certifications/cloud#examdetails

DOMAIN	PERCENTAGE OF EXAMINATION
1.0 Configuration and Deployment	24%
2.0 Security	16%
3.0 Maintenance	18%
4.0 Management	20%
5.0 Troubleshooting	22%
Total	**100%**

Cloud+ 002 (live now)

DOMAIN	PERCENTAGE OF EXAMINATION
1.0 Cloud Architecture and Design	13%
2.0 Security	20%
3.0 Deployment	23%
4.0 Operations and Support	22%
5.0 Troubleshooting	22%
Total	**100%**

Cloud+ 003 (live as of May 2021)

Cloud+ details

- Version 2.0 (CV0-002) has been live since February of 2019
- New version – CV0-003
  - May 2021
  - Max. of 90 questions
  - Performance-based and multiple choice
  - 90 minutes

https://www.comptia.org/certifications/cloud#examdetails

Cloud+ details

- Domain 1.0
- Focus on practical requirements
- Planning

- **Requirements**
  - Hardware
  - Software
  - Budgetary
  - Business need analysis
- **Standard templates**
- **Licensing**
  - Per-user
  - Socket-based
  - Volume-based
  - Core-based
  - Subscription
- **User density**
- **System load**
- **Trend analysis**
  - Baselines
  - Patterns
  - Anomalies
- **Performance capacity planning**

Cloud+ details (cont'd)

- Domain 2.0
- GRC

2.4 Given a scenario, apply data security and compliance controls in cloud environments.

- **Encryption**
- **Integrity**
  - Hashing algorithms
  - Digital signatures
  - File integrity monitoring (FIM)
- **Classification**
- **Segmentation**
- **Access control**
- **Impact of laws and regulations**
  - Legal hold
- **Records management**
  - Versioning
  - Retention
  - Destruction
  - Write once read many
- **Data loss prevention (DLP)**
- **Cloud access security broker (CASB)**

2.5 Given a scenario, implement measures to meet security requirements.

- **Tools**
  - Vulnerability scanners
  - Port scanners
- **Vulnerability assessment**
  - Default and common credential scans
  - Credentialed scans
  - Network-based scans
  - Agent-based scans
  - Service availabilities
- **Security patches**
  - Hot fixes
  - Scheduled updates
  - Virtual patches
  - Signature updates
  - Rollups
- **Risk register**
- **Prioritization of patch application**
- **Deactivate default accounts**
- **Impacts of security tools on systems and services**
- **Effects of cloud service models on security implementation**

Cloud+ details (cont'd)

- Domain 3.0
- Right-sizing
- Migrations

3.4 Given a scenario, configure the appropriate compute sizing for a deployment.

- **Virtualization**
  - Hypervisors
    - Type 1
    - Type 2
  - Simultaneous multi-threading (SMT)
  - Dynamic allocations
  - Oversubscription
- **Central processing unit (CPU)/ virtual CPU (vCPU)**
- **Graphics processing unit (GPU)**
  - Virtual
    - Shared
  - Pass-through
- **Clock speed/Instructions per cycle (IPC)**
- **Hyperconverged**
- **Memory**
  - Dynamic allocation
  - Ballooning

3.5 Given a scenario, perform cloud migrations.

- **Physical to virtual (P2V)**
- **Virtual to virtual (V2V)**
- **Cloud-to-cloud migrations**
  - Vendor lock-in
  - PaaS or SaaS migrations
    - Access control lists (ACLs)
- **Storage migrations**
  - Block
  - File
  - Object
- **Database migrations**
  - Cross-service migrations

Cloud+ details (cont'd)

- Domain 4.0
- Monitoring
- Data
- Also, continuity, including backup

4.4 Given a scenario, apply proper automation and orchestration techniques.

4.1 Given a scenario, configure logging, monitoring, and alerting to maintain operational status.

- **Logging**
  - Collectors
    - Simple network management protocol (SNMP)
    - Syslog
  - Analysis
  - Severity categorization
  - Audits
  - Types
    - Access/authentication
    - System
    - Application
  - Automation
  - Trending
    - Application-level backup
    - Filesystem backup
    - Database dumps
    - Configuration files
    - Location
    - SLAs
    - Recovery time objective (RTO)
    - Recovery point objective (RPO)
    - Alternate location
    - Restore files
    - Snapshot
- **Monitoring**
  - Baselines
  - Thresholds
  - Tagging
  - Log scrubbing
  - Performance monitoring
    - Application
    - Infrastructure components
  - Resource utilization
  - Availability
    - SLA-defined uptime requirements
  - Verification of continuous monitoring activities
  - Service management tool integration
- **Alerting**
  - Common messaging methods
  - Enable/disable alerts
    - Maintenance mode
  - Appropriate responses
  - Policies for categorizing and communicating alerts

Cloud+ details (cont'd)

- Domain 5.0
- Troubleshooting

5.2 Given a scenario, troubleshoot security issues.

- **Privilege**
  - Missing
  - Incomplete
  - Escalation
  - Keys
- **Authentication**
- **Authorization**
- **Security groups**
  - Network security groups
  - Directory security groups
- **Keys and certificates**
  - Expired
  - Revoked
  - Trust
  - Compromised
  - Misconfigured
- **Misconfigured or misapplied policies**
- **Data security issues**
  - Unencrypted data
  - Data breaches
  - Misclassification
  - Lack of encryption in protocols
  - Insecure ciphers
- **Exposed endpoints**
- **Misconfigured or failed security appliances**
  - IPS
  - IDS
  - NAC
  - WAF
- **Unsupported protocols**
- **External/internal attacks**

5.3 Given a scenario, troubleshoot deployment issues.

- **Connectivity issues**
  - Cloud service provider (CSP) or Internet service provider (ISP) outages
- **Performance degradation**
  - Latency
- **Configurations**
  - Scripts
- **Applications in containers**
- **Misconfigured templates**
- **Missing or incorrect tags**
- **Insufficient capacity**
  - Scaling configurations
  - Compute
  - Storage
  - Bandwidth issues
  - Oversubscription
- **Licensing issues**
- **Vendor-related issues**
  - Migrations of vendors or platforms
  - Integration of vendors or platforms
  - API request limits
  - Cost or billing issues

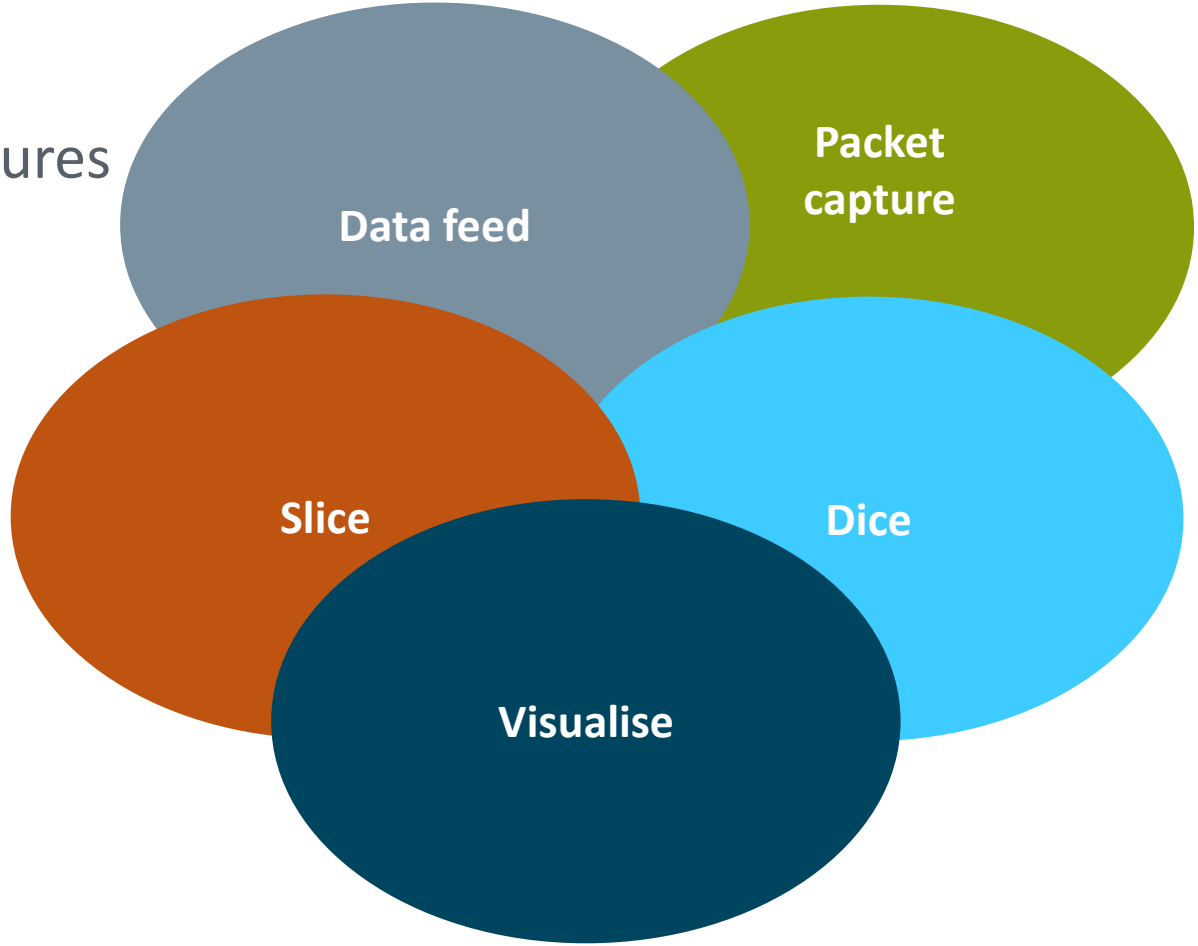
securing the cloud

Solutions that security professionals provide

- We surveyed IT hiring managers worldwide
- Here's what we found

Monitoring

- Data feeds + packet captures
- Direct feed from:
  - Cloud resources
  - Cloud AIM
  - Hosts themselves
  - “East / West” data
- Necessitated by:
  - Cloud
  - Data analytics



Visualisation – what do you see, here?

Visualisation – what pattern do you see, here?

summary

We need workers that can handle . . .

- Cloud Architecture
- Right sizing
- Governance
- Scoping
- Cloud service implementation
- Business continuity
- Cloud management
- Cybersecurity

Thank You!

James Stanger, PhD

Twitter: @jamesstanger

Skype: stangernet

Latest articles and blog entries:

The Internet of Things (IoT) and Technical Debt: Why It Matters (CompTIA)

How Technical Debt Can Damage Business Agility and Competitiveness (ITPro, UK)

Where the Wild Things Are: Investigating Browser-based Brute Force Attacks October, 2020, *Admin Magazine*

Threat Modeling and Cyber Threat Intelligence (CompTIA)

Old Guard "Cowboy IT" (SC Magazine)

Moving to the Cloud: IT Infrastructure and Cybersecurity skills required (CompTIA)

Rust Never Sleeps: Cyber and my Vintage Land Cruiser (CompTIA)

The Cybersecurity Hat Trick (CompTIA)

Threat Intelligence Platforms – needed? (CompTIA)

Putting AI and ML to work (CompTIA)

Visualizing with the Elastic Stack and Zeek (CompTIA)

The Skills needed to combat today's cybersecurity threats (RSA)

Automated Pen Testing (Admin Magazine)

Two sides of the same coin: Pen testing and security analytics

What's hot in network certifications (NetworkWorld)

Escaping the Cybersecurity Metrics Matrix (CompTIA)

Private Eye: Open source tools for automated pen testing *Admin Magazine*

Thoughts about the help desk (YouTube)

The Hunt for the Meaning of the Red team (CompTIA)

The IT security disconnect (HP Enterprise)

A blockchain manifesto? A report from the RSA 2018 Blockchain Focus Group Cloud Orchestration with Chef *Admin Magazine*

No more close shaves: Talking end user security

How CIOs can optimize ITSM software (SearchCIO)

Vulnerability management: How to target bug bounty programs (*TechTarget*)

My career change journey: The importance of networking

The role of the service desk in the cybersecurity kill chain (HDI)

How to prevent insiders from breaching your data (*Forbes*)

10 critical security skills every IT team needs (interview, *CIO Magazine*)

How AI can help you stay ahead of cybersecurity threats (CSO Magazine)

Don't hack me, bro! (*Admin Magazine*)

At the hop: Security testing with hping3 (*Linux Magazine*)

No sleep 'til SITS: The birth of time itself (CompTIA)

Cross-Layered Detection and Response (XDR): A Welcome New Entry in the Cybersecurity Alphabet Soup (CompTIA)

We're All in this Together: Community and Collaboration Are Key to Cyber Success (CompTIA)

What is the difference between IT security and cybersecurity? (CompTIA)

Do Fuzzing Applications Really Work? (CompTIA)

Observations at RSA San Francisco 2020 (CompTIA)

My CompTIA hub:

https://www.comptia.org/blog/listing/author/james%20stanger