Practical Cloud Security

Principles and Concepts

Principles and Concepts

Least Privilege

- Can only access what they need to do their jobs.
- Deny by default.
- Tightly control access to and privileges on both cloud console and on-premise data center access.

Defense in Depth

- Any security control can fail.
- Create multiple layers of overlapping security controls (if one fails, the one behind it can, hopefully, help.
- Keeping asking yourself “What if this fails?”

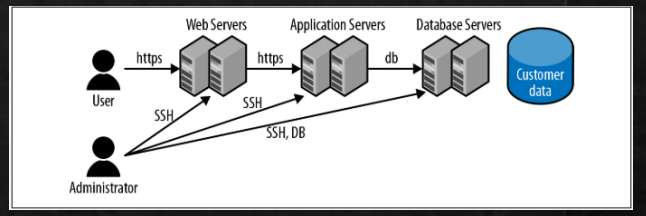
Principles and Concepts

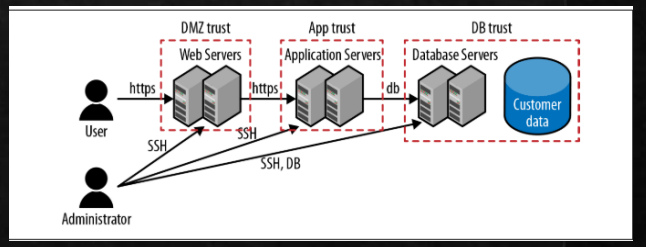
Threat Actors

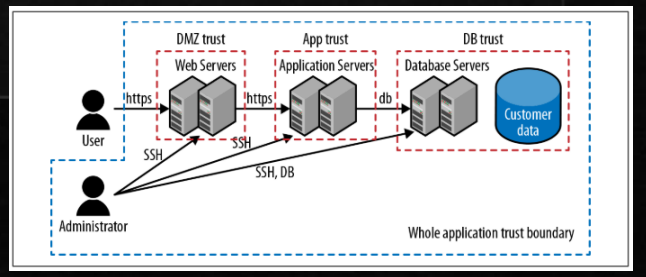
- Organized crime or independent criminals, interested in making money.
- Hacktivists, interested in discrediting you or disrupting your business.
- Inside attackers, discrediting you or making money.
- State actors, stealing secrets or disrupting business.

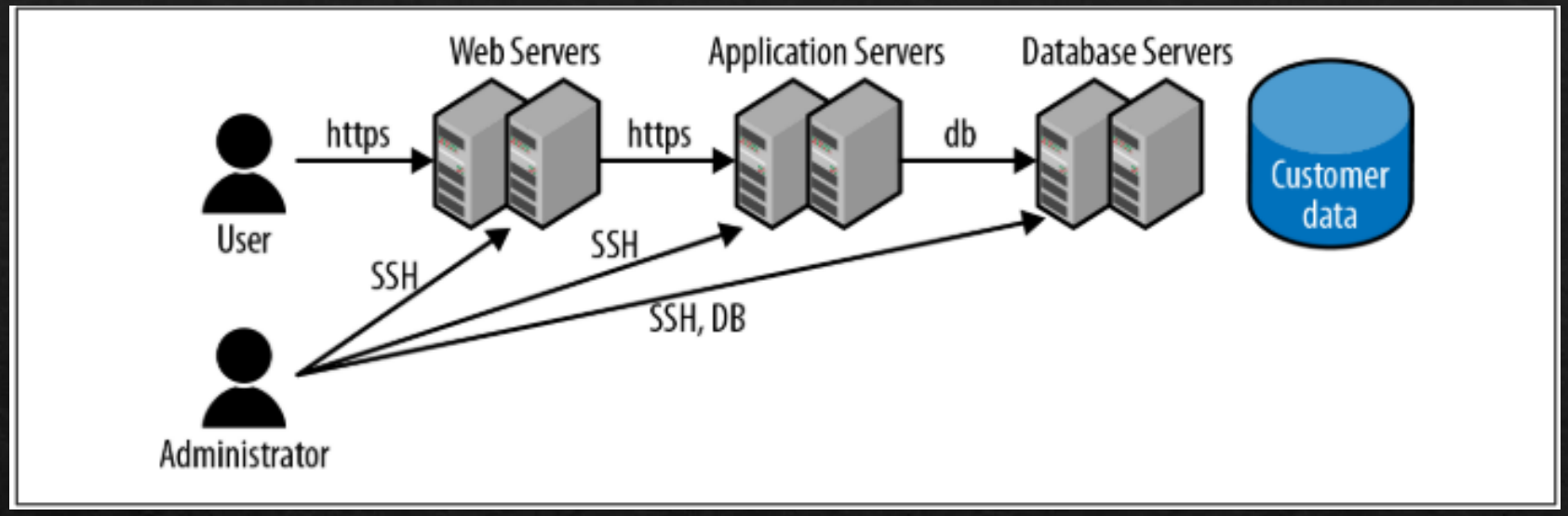
Trust Boundaries

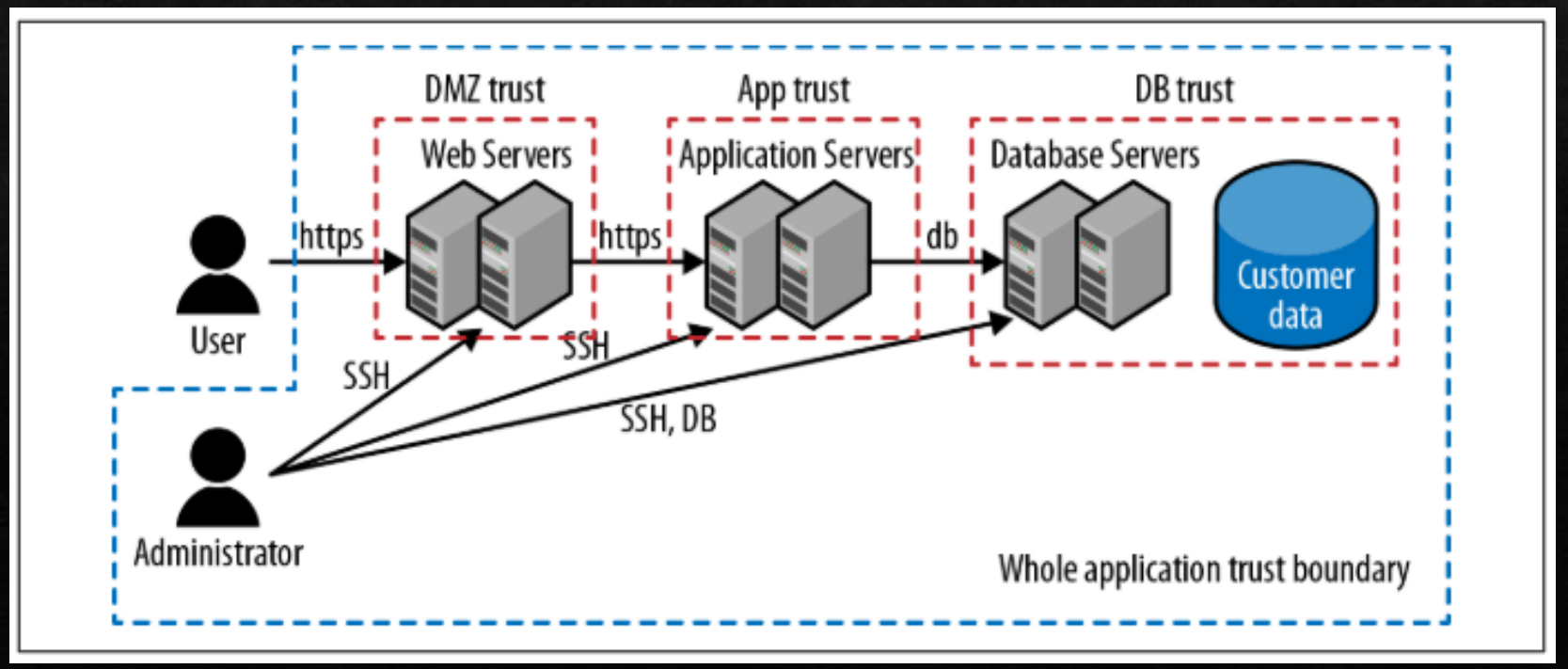
- Create trust boundaries.
- Levels of trust








Web Servers
Application Servers
Database Servers
https
https
db
User
SSH
SSH
SSH, DB
Customer data
Administrator


DMZ trust
App trust
DB trust
Web Servers
Application Servers
Database Servers
https
https
db
User
SSH
SSH
SSH, DB
Customer data
Administrator
Whole application trust boundary

Principles and Concepts

Shared Responsible Model

- What aspects of security am I responsible for? E.g.,
- Dev is responsible for code errors.
- IT is responsible for everything else (network, security, etc.)
- Responsibility is inside the company and is blurred these days.

- Things are different if services are moved to cloud.
- Need to know where cloud provider's responsibility ends and where yours starts
- Keeping asking yourself "What if this fails?"

Principles and Concepts

Risk Management

- Likelihood (how probable it is that the bad thing will happen).
- Impact (what are bad results if it happens).
- One of four things can be done risks are known:

Once risks are known

- Avoid the risk – turn it off, no more risk (but for what?)
- Mitigate the risk – do additional things to lower the likelihood or impact.
- Transfer the risk – pay someone else to manage things.
- Accept the risk – know that some risks exist and move on.

Assets Management and Protection

Data Asset and Cloud Asset

Data Asset Management and Protection

Data Identification and Classification

- Data Classification Levels (example)
  - Low – server's public IP, application log without personal data, secrets or value to attack
  - Moderate – Not to be disclosed outside of the organization, e.g., detailed system design, personnel information (address, phone, etc. which may lead to phishing attack), or routine financial information.
  - High – vital to the organization and disclosure can cause significant harm, e.g., future plan and strategy, trade secrets, credentials to access cloud, customer's financial data, etc.

Compliance

- Relevant Industry or Regulatory Requirements
  - GDPR, PCI (Payment Card Industry), PHI (Protected Health Information), Thailand Computer Act, PDPA, etc.
- Transfer the risk – pay someone else to manage things.
- Accept the risk – know that some risks exist and move on.

Data Asset Management and Protection

Data Asset Management in the Cloud

- Apart from sensitive information or customer data in the database, where else do we have important assets?
  - Web servers have log that may be used to identify your customers.
  - Web servers have a private key for a TLS certificate.
  - Application server needs a password or API key to access the database.
- Tagging helps to do categorization and inventory.
- Tag = name + value

Protecting Data in the Cloud

- Tokenization – substitute sensitive data with a token (randomly generated number).
- Encryption
  - In motion
  - In use (being processed in a CPU or stored in RAM)
  - At rest
- In-memory encryption such as Intel SGX, AMD SME, IBM Z Pervasive Encryption.

Data Asset Management and Protection

Protecting Data in the Cloud

- Key management system.
- Cryptographic erasure – typically it takes to destroy/delete large amount of data. One possible solution is to store encrypted data and revoke key when we want to make data undiscoverable.

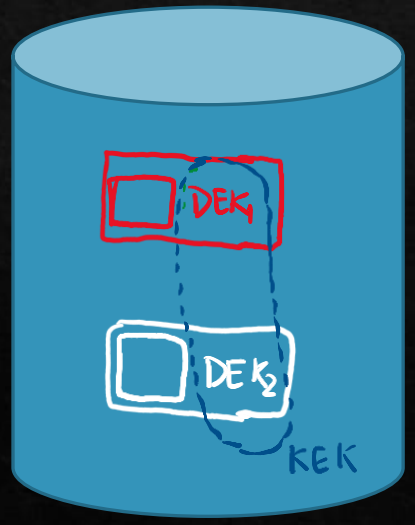
- What if attacker gained unauthorized access to
  - Physical media.
  - Platform or storage system.
  - Hypervisor.
  - Operating system.
  - Application.
- Although encryption may reduce performance, due to extra processing required. This should not be a major concern in the future as some forms of hardware acceleration is being utilized. (e.g., T1 Chip)

- In on-premise environment, one may purchase a hardware security module (HSM) to held encryption keys, usually in the form of an expansion card or a module accessed over a network. HSM has sensors to wipe out data if it is tampered. Note that HSMs are expensive.

Two levels of key - Data Encryption Key (DEK)

KEY ENCRYPTION KEY (KEK)

Cryptographic Erasure



Metadata – creator, creation time, permissions

Objects are immutable (cannot be changed after creation)

Cloud Asset Management and Protection

Types of Cloud Assets

- Compute Assets
  - VMs attacks (hypervisor breakout and side-channel attacks)
    - Fortunately, these attacks are not easy to achieve.
    - Items to track for VMs – OS name and version, platform/middleware name and version, IP addresses, users allowed to access OS/platform.
  - Containers – larger attack surface due to shared kernel.
    - Containers should hold minimum OS components/kernels.
    - Containers are immutable.
    - Containers don't update their own code. Old one is destroyed and new one is created with updated codes.
  - Serverless – code run only when needed (when service is requested) e.g., AWS Lambda, Azure Functions
- Storage Assets
  - Block storage – attackers may bypass OS control to get access to assets (HDD).
  - File storage – attacks with access to the file storage can read all files (filesystem).
  - Object storage – controlled by policies. If set for open access, data breaches may arise (flat file – stream of bytes with metadata).
  - Others – images, cloud databases, message queues, configuration storage, encryption key storage, certificate storage, source code repositories.
- They all require strict access control.

Cloud Asset Management and Protection

Types of Cloud Assets

- Network Assets
  - Virtual private clouds and subnets
    - High-level boundaries to allow what can talk to what.
    - Good inventory of them deems necessary.
  - Content Delivery Networks (CDNs).
    - Distribute content globally for low-latency access, typically non-sensitive data.
    - Attackers with access to CDN can poison the content with malware, bitcoin miners, DDoS.

- Network Assets
  - TLS certificates – entire class of certificates needs to be reissues, such as when cryptographic algorithm is found to be weak.
    - Access to private keys must be properly tracked.
  - Load balancers, reverse proxy, web application firewall

Asset Management Pipeline

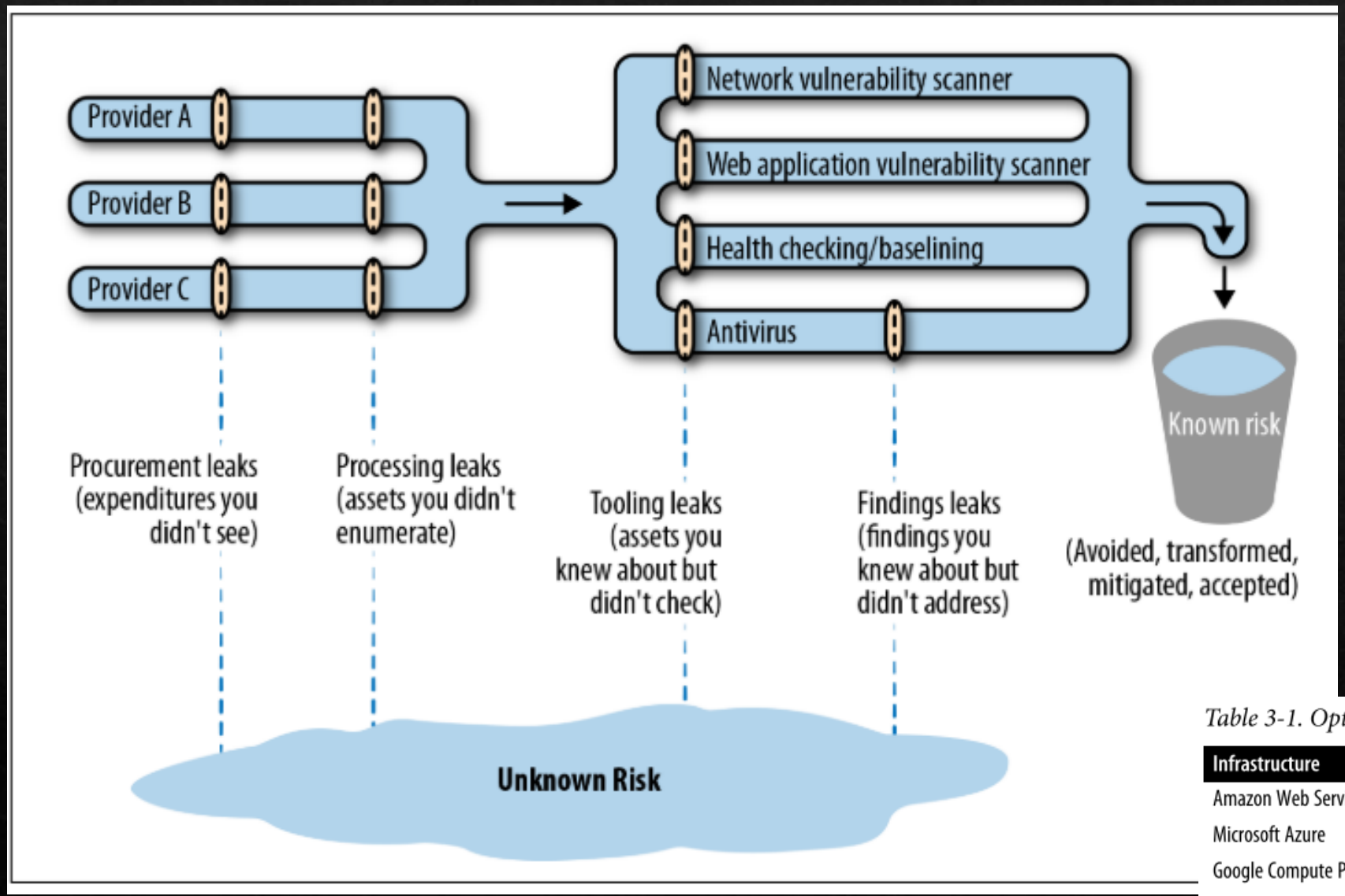


Table 3-1. Options for auditing cloud activity

Infrastructure	Ways to audit usage
Amazon Web Services	API, portal, command line, AWS Systems Manager Inventory
Microsoft Azure	API, portal, command line, Azure Automation Inventory
Google Compute Platform	API, portal, command line, Cloud Security Command Center Asset Inventory
IBM Cloud	API, portal, command line, IBM Cloud Security Advisor
Kubernetes	API, dashboard

Asset Management Pipeline

- Procurement leaks
  - You may have multiple cloud providers with different models (Iaas, PaaS, SaaS)
  - Pull inventory information
  - Leaks here means you've missed an entire cloud provider, because you didn't see the expenses or it is free.

- Processing leaks
  - Check for what cloud providers do for you – use their portal, API or inventory systems to pull a list of assets.
  - Leaks here mean you queries the cloud provider for assets but didn't inventory some assets. For example, you have a list of all VMs but forget about object storage

Asset Management Pipeline

- Tooling leaks
  - Use tools to check the security of your assets.
  - Leaks here mean that you know about some assets but don’t have tools or processes check those assets for security issues.

- Finding leaks
  - This step is to address any findings (vulnerabilities or weaknesses – these are risks) from your tooling systems.
  - In practice these findings may be ignored due to high false positives.
  - Perfectly acceptable to a risk without fixing it.

Detecting, Responding to, and Recovering from Security Incidents

What to Watch

- So many different logs and metrics to watch. Pick the right one is very important.
  - Log/event – a record of a specific thing that happens, e.g., authentication attempted by someone, some makes a web request, admin changes firewall policies.
  - Metrics – a set of numbers that give information about something, usually a time-based, e.g., number of authentication success/failure, CPU usage/time, etc.
  - Watch these – privileged user access, logs from defensive tools such as anti-DDoS, WAF, firewall, IPS/IDS, antivirus, endpoint detection and response, file integrity monitoring.

What to Watch - Cloud Service Logs and Metrics

- CPU usage metrics – spikes CPU usage, if not from increased usage, might indicate active ransomware encryption or cryptomining.
- Network logs and metrics – spikes in network traffic might indicate DDoS or an attacker is actively stealing data.
- Storage input/output metrics - spikes in I/O usage might indicate DDoS or an attacker is actively stealing data.
- Metrics on requests to platform components, such as databases or message queues – spikes may indicate an attacker is stealing data or is attempting to send messages to other components.
- End-user logins and activity on SaaS offerings – if a user starts pulling large amounts of data, this could be an indication that the account is compromised.

What Else to Watch

- OS logs and metrics – check CIS Benchmarks list for a base set of events to log.
  - Different OSs have different base, e.g., for Windows – a specific event IDs must be monitored to detect pass-the-hash attack.
  - Metrics such as memory usage, CPU usage, and I/O can be very useful to security teams as well as operation teams.
- Middleware logs
  - If you are running your own databases, queue manager, application server or other middleware, don’t forget to turn on logging and metric collection.
- Secrets Server – all access/activity to secrets server must be logged.

- “Database traffic is up 200% from the monthly average. Maybe the application is just really popular right now, but is someone systematically stealing our data?”
- “We just saw an outbound connection to an IP address that has been used by a known threat actor recently, according to this threat intelligence feed. Is that a compromised system talking to a command-and-control server?”
- “There were 150 failed login attempts on an account, followed by a success. Is that a successful brute-force attack?”
- “We saw a single failed login attempt on 300 different accounts, followed by a success on account #301. Is that a successful password spraying attack?”

- “A new administrative account was just created outside of normal business hours. Maybe someone’s working late, but maybe there’s an issue?”
- “Someone was just added to the administrator group. That’s a rare event, so shouldn’t we check on it?”
- “Why are there firewall denies with an internal system as the source? Either something is misconfigured or there’s an unauthorized user trying to move around the network.”

- "A port scan was followed by a lot of traffic from a port that hasn't been used in months. Port scans happen all the time, but perhaps a vulnerable service was found and compromised?"
- "John doesn't normally log in at 3:00 AM ET, or from that country. Maybe that's not really John?"
- "Three different accounts logged in from the same system over the course of 30 minutes. It seems unlikely all of those people are actually using that system, so maybe the system and those accounts are compromised?"

Preparing and Responding to an Incident

- You need a team; CTO, IT manager, security specialist, legal department, communications department, HR.
- You need a plan when incidents happen. For example,
  - A plan to disable all cloud portal and API access other than the minimum required during the incident.
  - A plan to disable all network access to your cloud environment, or some subset of it.
  - A plan to shutdown the entire environment, lock the secrets server, and recreate a new environment.
  - A plan to recover data from backup when data storage is compromised.
- You need tools.

- Cloud-aware forensic analysis tools, which can help you understand what happened on a particular system.
- Up-to-date diagrams showing network configuration, data locations, and event logging locations.
- Tested communications systems. Will you be able to respond to a threat if your instant message platform, email, or telephone systems are down? In an emergency, perhaps you will permit people to use personal email and cell phones for work activities, even if that's normally disallowed. It's better to think about those decisions ahead of time.
- Contact lists, for both people internal to the organization and external contacts such as cloud providers, incident response firms, or other suppliers that may be involved in incident response.

- A war room. In cloud environments, you won't be physically touching the equipment in most cases, but you still need a physical or virtual war room where the team can meet, exchange information, and make decisions. If you may have remote attendees, make sure you have meaningful ways for them to participate, such as screen sharing and a reasonable audio system.
- Checklists. I'm not a fan of "checklist security" at all, where you tick off that you have a firewall, antivirus software, and similar items without actually verifying that they're being used effectively. However, incident response is often performed by panicky, tired people. For these situations, checklists that help you implement plans are essential to ensure you haven't forgotten something really important. For example, one online checklist suggests a useful set of logs to review during an incident.
- Forms for documenting incident response activities. For example, the SANS institute offers some forms that can be customized for your organization.
- Incident response software, which has components that can track incidents and built-in playbooks for incident response.