

IR in the Cloud – '72 hours and Ticking'

Robert Floodeen (New Anderton, UK)

Rebecca Taylor (Secureworks, UK)

#FIRSTCON23



35TH
ANNUAL
FIRST
CONFERENCE

MONTREAL

JUNE 4-9, 2023



'There are key aspects of cloud incident response, which differentiate it from non-cloud incident response. Notably **governance, shared responsibility, and visibility.**'

Cloud Incident Response Framework, Cloud Security Alliance

Agenda

- Background
- Considerations for Incident Command in the Cloud
- Common practices and Knowledge Management techniques

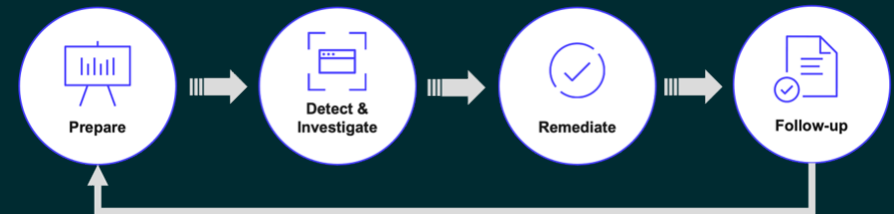


9

Secureworks®



COUNTER THREAT UNIT
The Secureworks Global Research Team





Background - Outcomes

#FIRSTCON23



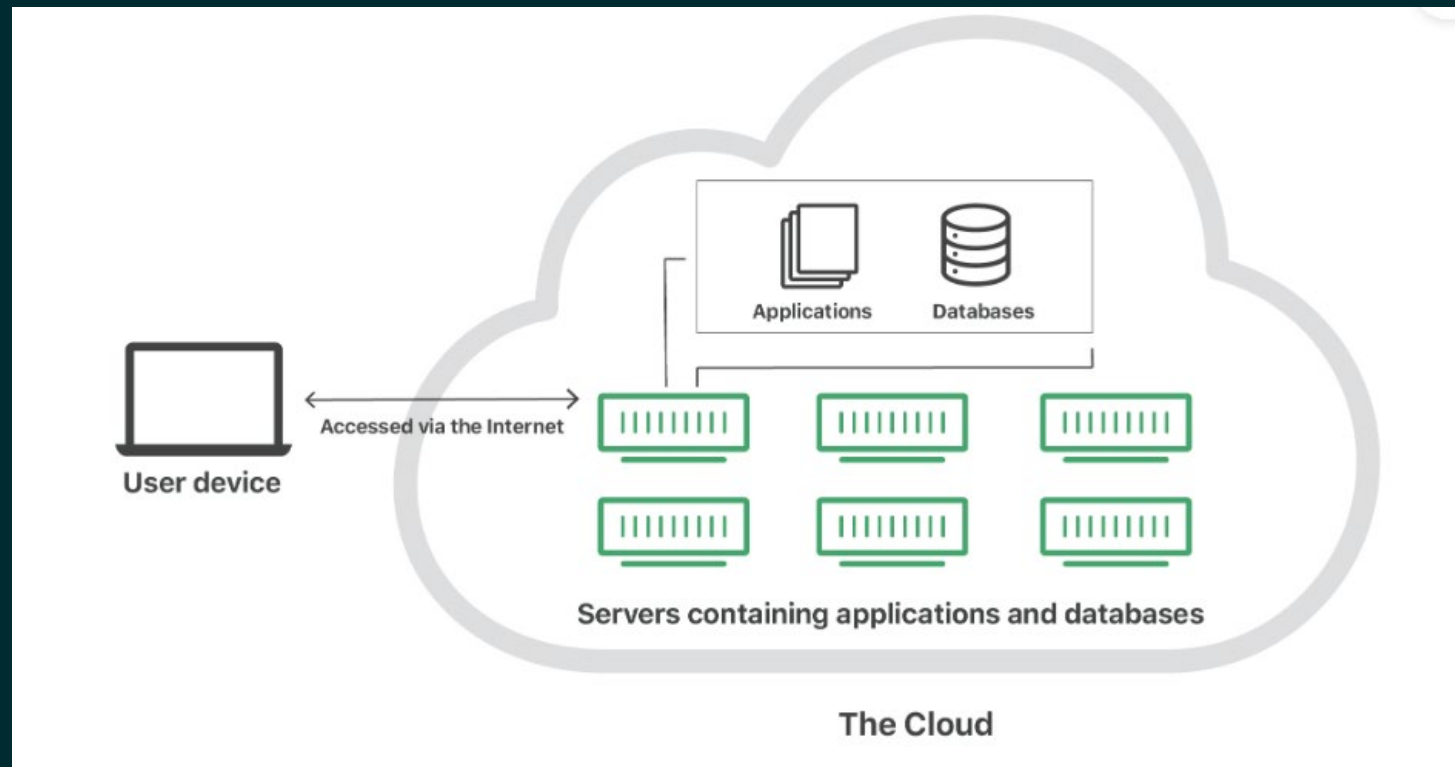
35TH
ANNUAL
FIRST
CONFERENCE

MONTREAL

JUNE 4-9, 2023



'Cloud services are infrastructure, platforms, or software that are hosted by third-party providers and made available to users through the internet.'



Quote Reference: [RedHat](#)

Image Reference: [Cloudflare](#)

As-a-Service Solutions

Infrastructure-as-a-Service (IaaS)

Provides users with **compute**, **networking**, and **storage** resources.

Platforms-as-a-Service (PaaS)

Provides users with a platform on which applications can run, as well as all the **IT infrastructure** required for it to run.

Software-as-a-Service (SaaS)

Provides users with—essentially—a **cloud application**, the platform on which it runs, and the platform's **underlying infrastructure**.

Function-as-a-Service (FaaS)

An event-driven execution model, lets developers build, run, and **manage app packages as functions** without maintaining the infrastructure.

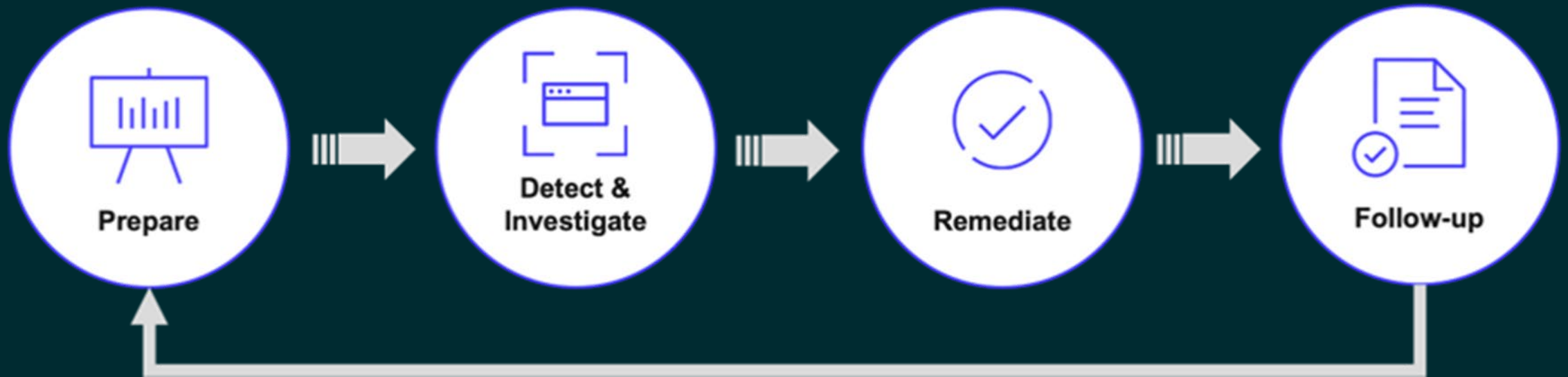
Terminology

- **Account:** Highest level of ownership and access controls, which are setup on creation using a unique email, and contain **resources, services and configurations** tied to an organization.
- **User:** Represents a person/application, with their own name and credentials, managed through IAM. **Permissions are granted** to a user for their access and management needs.
- **Role:** Defines **permissions and policies** that govern access to resources.

Terminology

- **Principal:** A human user or workload that can make a request for an action or operation on a resource. After authentication, the principal can be granted either permanent or temporary credentials to make requests, depending on the principal type.
- **Entity:** An individual, system or application that interacts with the Cloud. Represents the entity that requires access or permissions.





Reference: Secureworks

Local Hardware (on-prem)

Immediate

First 24 Hours

48 Hours

72 Hours

Local Hardware (on-prem)

Immediate	First 24 Hours	48 Hours	72 Hours
<ul style="list-style-type: none"> • Get IR and BC/DR Plan and assign a resource to start reviewing content • Assign task of documenting known knowns • Assign task of understanding business impact • Assign task of checking sensitive data (CIA) • Appoint an Incident Commander • Consult Legal Counsel • Consider Core Response Objectives • Activate Core IR Team • Start primary workstreams • Schedule first status meeting • Publish CIRT Command Structure and Key Points of Contact 	<ul style="list-style-type: none"> • Setup Collaboration and Communication systems • Command room / space is established • Activate the full IR Team • Drive creation and update of Core Response Objectives • Workstreams update <ul style="list-style-type: none"> • Analysis Workstream briefs the known knowns and initial containment recommendations • Recovery Workstream briefs business impact(s) and recovery objectives • Determine if Communications Workstream is required • Complete first status meeting 	<ul style="list-style-type: none"> • Build Communication plan, as required • Key Contact list completed • Operational Cycle is defined • Known Knowns are more developed (i.e. incident timeline, business impacts, objectives) • Materials for analysis are available (logs, images, interviews) • Recovery Workstream has a working plan developed • Second status meeting held • Second update published • Rolling Action Item Log (RAIL) in place 	<ul style="list-style-type: none"> • First draft of Common Operational Picture (COP) available in command room • All workstreams fully up and running • Containment / Eviction plan developed • Recovery plan, where feasible, started • Initial Communications, as required, completed

Local Hardware (on-prem)

Immediate	First 24 Hours	48 Hours	72 Hours
<ul style="list-style-type: none"> • Get IR and BC/DR Plan and assign a resource to start reviewing content • Assign task of documenting known knowns • Assign task of understanding business impact • Assign task of checking sensitive data (CIA) • Appoint an Incident Commander • Consult Legal Counsel • Consider Core Response Objectives • Activate Core IR Team • Start primary workstreams • Schedule first status meeting • Publish CIRT Command Structure and Key Points of Contact 	<ul style="list-style-type: none"> • Setup Collaboration and Communication systems • Command room / space is established • Activate the full IR Team • Drive creation and update of Core Response Objectives • Workstreams update <ul style="list-style-type: none"> • Analysis Workstream briefs the known knowns and initial containment recommendations • Recovery Workstream briefs business impact(s) and recovery objectives • Determine if Communications Workstream is required • Complete first status meeting 	<ul style="list-style-type: none"> • Build Communication plan, as required • Key Contact list completed • Operational Cycle is defined • Known Knowns are more developed (i.e. incident timeline, business impacts, objectives) • Materials for analysis are available (logs, images, interviews) • Recovery Workstream has a working plan developed • Second status meeting held • Second update published • Rolling Action Item Log (RAIL) in place 	<ul style="list-style-type: none"> • First draft of Common Operational Picture (COP) available in command room • All workstreams fully up and running • Containment / Eviction plan developed • Recovery plan, where feasible, started • Initial Communications, as required, completed

Cloud Service (cloud)

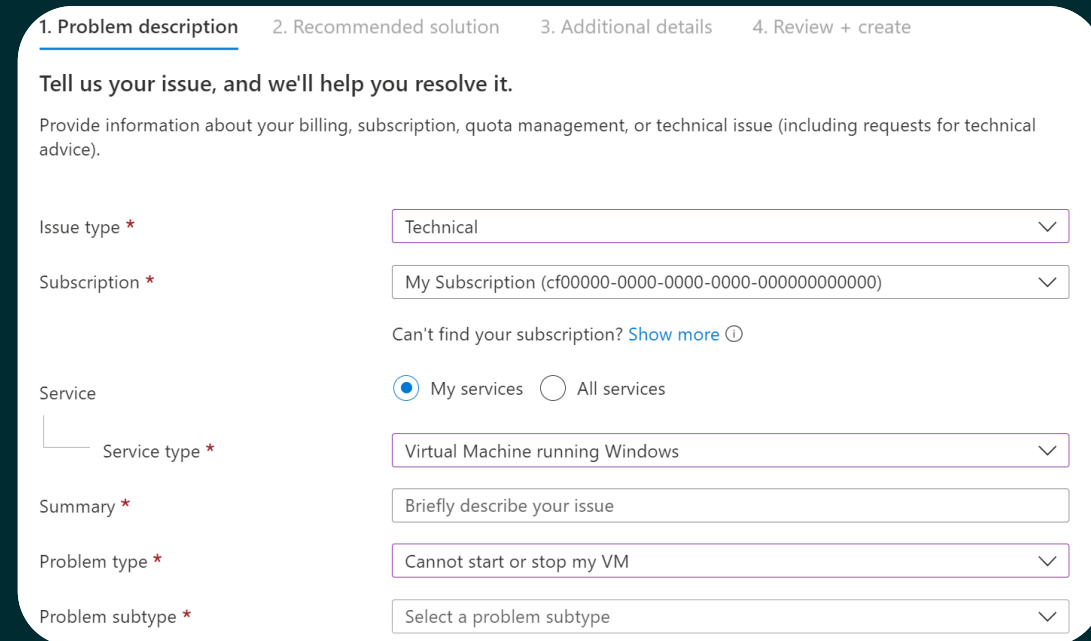
Immediate	First 24 Hours	48 Hours	72 Hours
<ul style="list-style-type: none"> • Get IR and BC/DR Plan and assign a resource to start reviewing content • Assign task of documenting known knowns • Assign task of understanding business impact • Assign task of checking sensitive data (CIA) • Appoint an Incident Commander • Consult Legal Counsel • Contact CSP(s) / SaaS and review/create ticket/case early in order to start a dialogue (this can be critical so do it early/fast) • Consider Core Response Objectives • Activate Core IR Team • Start primary workstreams • Review and understand Chain of Custody for the CSP(s) • Schedule first status meeting • Publish CIRT Command Structure and Key Points of Contact 	<ul style="list-style-type: none"> • Setup Collaboration and Communication systems • Command room / space is established • Activate the full IR Team • Create / Validate secure space for response activities <ul style="list-style-type: none"> • new account or a clean separate account • Assign task to validate logging needs <ul style="list-style-type: none"> • determine roles / policies for response team • ensure assesment of ephemeral systems and systems with 'console only' access • Assign task to validate logging/analysis assumptions <ul style="list-style-type: none"> • include API analysis (account to account) • Drive creation and update of Core Response Objectives • Workstreams update <ul style="list-style-type: none"> • Analysis Workstream briefs the known knowns and initial containment recommendations • Recovery Workstream briefs business impact(s) and recovery objectives • Determine if Communications Workstream is required • Assign POC to work with CSP/SaaS to generate rough costing model for response, to include possible license upgrades • Complete first status meeting 	<ul style="list-style-type: none"> • Build Communication plan, as required • Key Contact list completed • Operational Cycle is defined • Known Knowns are more developed (i.e. incident timeline, business impacts, objectives) • Monitoring includes APIs, keys, applications, roles, policies, new systems, hijacked IPs (endpointID vs source IP), and new or modified VPCs across the environment • Materials for analysis are available (logs, images, interviews) • Review/update ticket/case with CSP/SaaS. Check for new abuse notification(s) • Recovery Workstream has a working plan developed • Second status meeting held • Second update published • Rolling Action Item Log (RAIL) in place 	<ul style="list-style-type: none"> • First draft of Common Operational Picture (COP) available in command room • All workstreams fully up and running • Containment / Eviction plan developed • Recovery plan, where feasible, started • Initial Communications, as required, completed • Account, user, policies, and other credentials validated

Local Hardware (on-prem)

Immediate	First 24 Hours	48 Hours	72 Hours
<ul style="list-style-type: none"> Get IR and BC/DR Plan and assign a resource to start 	<ul style="list-style-type: none"> Setup Collaboration and Communication systems 	<ul style="list-style-type: none"> Build Communication plan, as required 	<ul style="list-style-type: none"> First draft of Common Operational Picture (COP)
<ul style="list-style-type: none"> re As As As As C C As St Sc Pl C 	<div style="border: 1px solid black; padding: 10px;"> <h3 style="text-align: center;">Immediate</h3> <ul style="list-style-type: none"> Get IR and BC/DR Plan and assign a resource to start reviewing content Assign task of documenting known knowns Assign task of understanding business impact Assign task of checking sensitive data (CIA) Appoint an Incident Commander Consult Legal Counsel Contact CSP(s) / SaaS and review/create ticket/case early in order to start a dialogue (this can be critical so do it early/fast) Consider Core Response Objectives Activate Core IR Team Start primary workstreams Review and understand Chain of Custody for the CSP(s) Schedule first status meeting Publish CIRT Command Structure and Key Points of Contact </div>	<ul style="list-style-type: none"> ed 	<ul style="list-style-type: none"> OP) ed validated

Talk to the CSPs

- Contact CSP (ticket and TAM).
 - Review new/open tickets/abuse notifications.
 - Create a new ticket.
 - Alert the team and request possible logs.
 - Example: the CSP IR Team may have access to older logs or even start logging for their own use



The screenshot shows a multi-step form for creating a ticket. The first step, '1. Problem description', is active. The form includes a title 'Tell us your issue, and we'll help you resolve it.' and a sub-instruction 'Provide information about your billing, subscription, quota management, or technical issue (including requests for technical advice)'. The form fields are: 'Issue type *' (dropdown menu with 'Technical' selected), 'Subscription *' (dropdown menu with 'My Subscription (cf00000-0000-0000-0000-000000000000)' selected), 'Service' (radio buttons for 'My services' and 'All services', with 'My services' selected), 'Service type *' (dropdown menu with 'Virtual Machine running Windows' selected), 'Summary *' (text input field with placeholder 'Briefly describe your issue'), 'Problem type *' (dropdown menu with 'Cannot start or stop my VM' selected), and 'Problem subtype *' (dropdown menu with 'Select a problem subtype' selected). Navigation tabs at the top are '1. Problem description', '2. Recommended solution', '3. Additional details', and '4. Review + create'.

"Daisy" Chain of Custody

- Isolate, Preserve, *and Monitor* Evidence.

- Example:

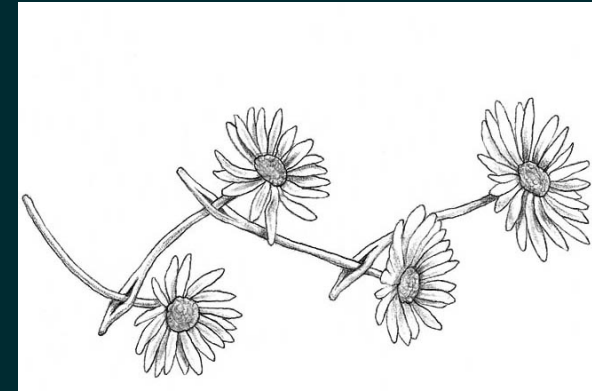
- AWS EC2 instance

- attach a new security group to the target instance
 - remove access for users, admins, and developers

- Azure

- maintain disks in an immutable Blob storage

- And Daisy Chain... Example: SHA-256 hash values should still be maintained, but in a different environment/account



Local Hardware (on-prem)

Immediate	First 24 Hours	48 Hours	72 Hours
<ul style="list-style-type: none"> Get IR and BC/DR Plan and assign a resource to start 	<ul style="list-style-type: none"> Setup Collaboration and Communication systems 	<ul style="list-style-type: none"> Build Communication plan, as required 	<ul style="list-style-type: none"> First draft of Common Operational Picture (COP)

First 24 Hours

- Setup Collaboration and Communication systems
- Command room / space is established
- Activate the full IR Team
- Create / Validate secure space for response activities
 - new account or a clean separate account
- Assign task to validate logging needs
 - determine roles / policies for response team
 - ensure assesment of ephemeral systems and systems with 'console only' access
- Assign task to validate logging/analysis assumptions
 - include API analysis (account to account)
- Drive creation and update of Core Response Objectives
- Workstreams update
 - Analysis Workstream briefs the known knowns and initial containment recommendations
 - Recovery Workstream briefs business impact(s) and recovery objectives
 - Determine if Communications Workstream is required
- Assign POC to work with CSP/SaaS to generate rough costing model for response, to include possible license upgrades
- Complete first status meeting

Systems can impact logging

- **Easy:** They can be ephemeral (we all know this right...)
 - Example: You should set up logging in containers, before deployment, if you want consistent logging out of containers.
- **Medium:** Data is a system/warehouse
 - Example: BigQuery, Redshift, Synapse Analytics, and deployed systems like MondoDB
- **Different:** Serverless compute and containers, there might not be access to the backend... so how do you interrogate?
 - Example: AWS Fargate you would use `/proc`

Logging Assumptions

- Networking = anywhere
 - Systems created/appear within VPC by TA
 - endpointID > sourceIP
 - Inter-CSP-trust could allow ANY authenticated
 - Examples in the CTF this year
 - Peered accounts != inside same account



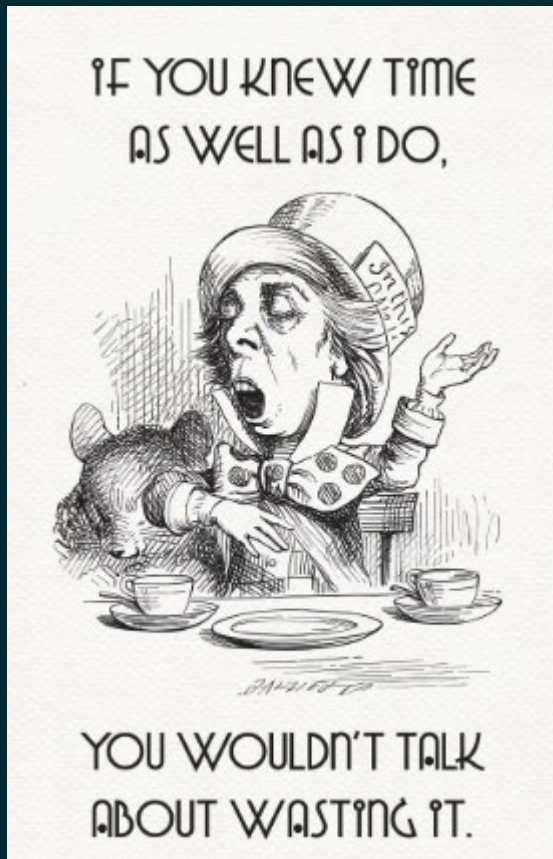
Logging Assumptions

- Src/Dst addresses != Pkt-Src/Pkt-Dst addresses
 - ⑩ 4 IPs (2 x NAT Gateway, 2 x actual src/dst)
 - ⑩ Not all underlying traffic is logged by CSP
 - ⑩ e.g. DNS Server traffic , DHCP
- CSPs have unique services with their own logging and levels of logging
 - Cross referencing between service logs is key

```
10.20.33.164 10.40.2.236 39812 80 6 3 IPv4 10.20.33.164 10.40.2.236 ACCEPT OK
```

```
10.40.2.236 10.20.33.164 80 39812 6 19 IPv4 10.40.2.236 10.20.33.164 ACCEPT OK
```

Logging Assumptions



- Timing = Aggregation + Processing + Publishing
 - 15 mins for VPC
 - Hours for S3 Bucket level activity
 - or minutes via CloudTrail
 - 48 hours of Guard Duty for AWS Detective
 - Secondary reuse – Recording time of event(s) or time when logs were received, date boundaries could result in missing logs

Licensing

- Understanding your licenses is important because it can affect several capabilities and timing to respond.
- Example: Detailed logging tends to **increase with license cost**
- Example: Might need to go through **your partner** to modify existing licenses



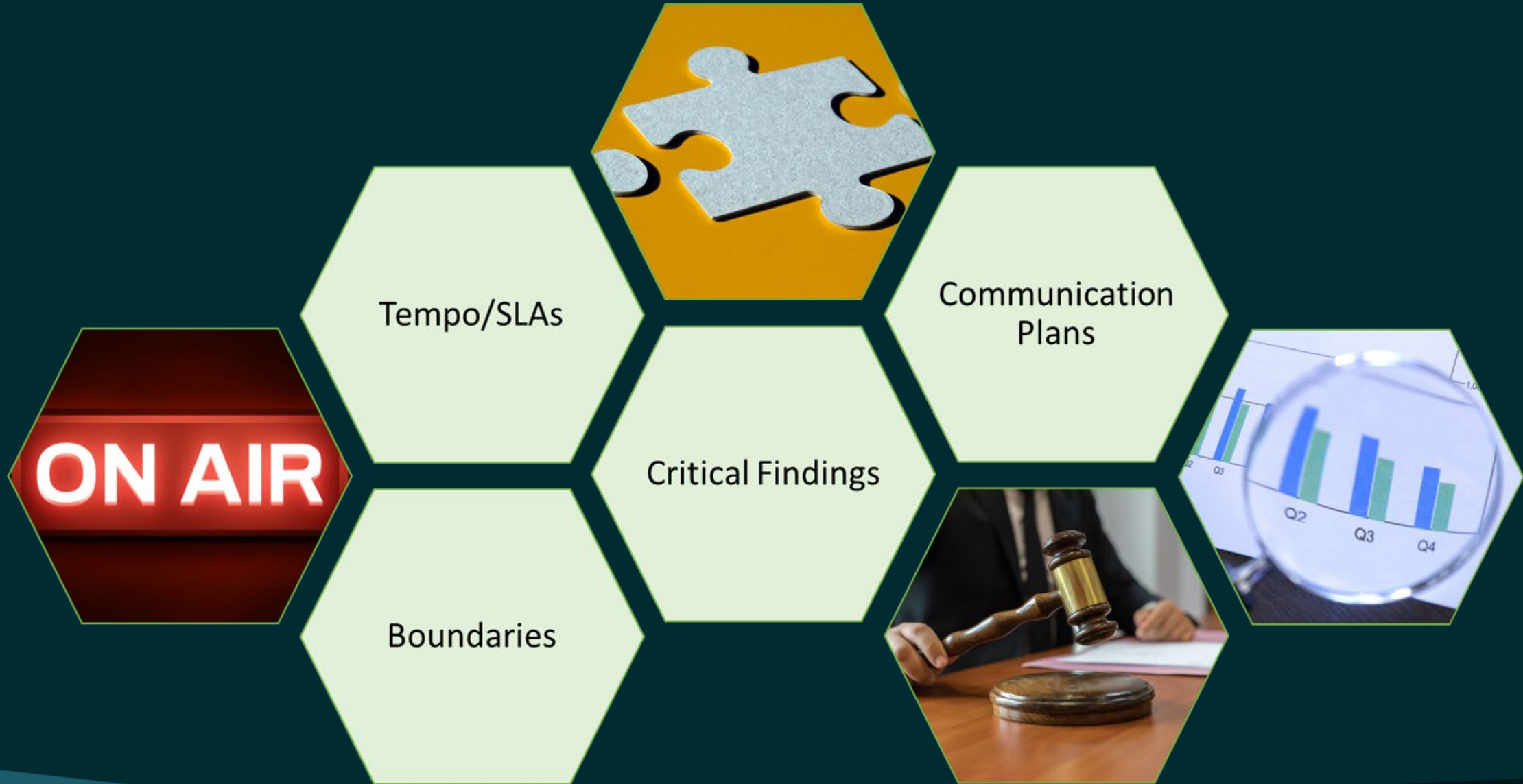
Costs

- Different costs associated with forensic analysis and work effort on Cloud environments.
- Example: [cost breakdown](#) to run **Automated Forensics Orchestrator in AWS**:
 - AWS Region is approximately \$235 a month, assuming an average of one forensic instance is 50% utilized for performing forensic analysis.

Local Hardware (on-prem)

Immediate	First 24 Hours	48 Hours	72 Hours
<ul style="list-style-type: none"> Get IR and BC/DR Plan and assign a resource to start 	<ul style="list-style-type: none"> Setup Collaboration and Communication systems 	<ul style="list-style-type: none"> Build Communication plan, as required 	<ul style="list-style-type: none"> First draft of Common Operational Picture (COP)
<ul style="list-style-type: none"> re As As As As C C As St Sc P C 	<div style="border: 1px solid black; padding: 10px; background-color: #f9f9f9;"> <h3 style="text-align: center;">48 Hours</h3> <ul style="list-style-type: none"> Build Communication plan, as required Key Contact list completed Operational Cycle is defined Known Knowns are more developed (i.e. incident timeline, business impacts, objectives) Monitoring includes APIs, keys, applications, roles, policies, new systems, hijacked IPs (endpointID vs source IP), and new or modified VPCs across the environment Materials for analysis are available (logs, images, interviews) Review/update ticket/case with CSP/SaaS. Check for new abuse notification(s) Recovery Workstream has a working plan developed Second status meeting held Second update published Rolling Action Item Log (RAIL) in place </div>	<ul style="list-style-type: none"> ed 	
<ul style="list-style-type: none"> G re As As As As C es d C As St R Sc P C 		<ul style="list-style-type: none"> OP) ed validated 	

Communication



Local Hardware (on-prem)

Immediate	First 24 Hours	48 Hours	72 Hours
<ul style="list-style-type: none"> Get IR and BC/DR Plan and assign a resource to start 	<ul style="list-style-type: none"> Setup Collaboration and Communication systems 	<ul style="list-style-type: none"> Build Communication plan, as required 	<ul style="list-style-type: none"> First draft of Common Operational Picture (COP)
			<div data-bbox="1031 297 1773 1313" data-label="Complex-Block"> <p style="text-align: center;">72 Hours</p> <ul style="list-style-type: none"> First draft of Common Operational Picture (COP) available in command room All workstreams fully up and running Containment / Eviction plan developed Recovery plan, where feasible, started Initial Communications, as required, completed Account, user, policies, and other credentials validated </div>



Cloud Incident Command

- Access, Licensing, Costs
 - Systems
 - Networks
 - KM Guidance
 - Ticketing Considerations
- There are different questions to ask.
 - There are different ways to get answers.
 - Knowledge management is throughout.

KM Guidance



Strong and tested communication mechanisms.



Understand your policies, processes and ticket structures.



Know your costs.

KM Guidance



Cloud mapping and
assets.



Understand your
templates and displays.

Ticket Best Practice

Date ↓

2023-05-08T22:41:39+... ⋮

2023-05-05T15:06:20+01:00

5263883

- Timestamp in UTC of first alert/indicator
- Cloud tenant ID/account
- Region/Availability Zone
- VPC/Security Group
- Subnet and or affected IP address(es).

5263883

5263883

- Affected user accounts/access key(s)Volume ID
- Snapshot ID
- Operating System
- S3/Blob ID
- IAM role
- Available logging/platforms

5263883

So these are also what we should be logging!

KM Guidance



Conclusion, thank you, and questions

The screenshot shows a Miro board with the following content:

- Local Hardware (on-prem)** and **Cloud Service (Cloud)** tables with columns for Location, First 20 hours, All hours, and 12 hours.
- FRST 72 hours** table with columns for On-Prem and Cloud, and rows for Incident Date, FRST 24 hours, First 48 hours, and First 72 hours.
- Objective Tracking** table with columns: Objective, Description, Critical Condition, Status, Time Estimate, Progress, Assessment, Assigned To/Status, and Notes.
- Frame 1** section containing a grid of 12 colored boxes, each representing a phase of an incident response cycle with associated tasks and milestones.
- Operational Cycle** table at the bottom.



Rob Floodeen -
robert.floodeen@newanderton.com

Rebecca Taylor -
rtaylor@secureworks.com

#FIRSTCON23



Thank you!

Rob Floodeen - robert.floodeen@newanderton.com

Rebecca Taylor – rtaylor@secureworks.com