IR in the Cloud – ‘72 hours and Ticking’

Robert Floodeen (New Anderton, UK)
Rebecca Taylor (Secureworks, UK)
‘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

Prepare → Detect & Investigate → Remediate → Follow-up
Background - Outcomes
‘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

<table>
<thead>
<tr>
<th>Infrastructure-as-a-Service (IaaS)</th>
<th>Platforms-as-a-Service (PaaS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides users with <strong>compute</strong>, <strong>networking</strong>, and <strong>storage</strong> resources.</td>
<td>Provides users with a platform on which applications can run, as well as all the <strong>IT infrastructure</strong> required for it to run.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Software-as-a-Service (SaaS)</th>
<th>Function-as-a-Service (FaaS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides users with—essentially—a <strong>cloud application</strong>, the platform on which it runs, and the platform’s <strong>underlying infrastructure</strong>.</td>
<td>An event-driven execution model, lets developers build, run, and <strong>manage app packages as functions</strong> without maintaining the infrastructure.</td>
</tr>
</tbody>
</table>
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.
<table>
<thead>
<tr>
<th>Local Hardware (on-prem)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Immediate</td>
</tr>
</tbody>
</table>

#FirstCon23

35th ANNUAL FIRST CONFERENCE | EMPOWERING COMMUNITIES
<table>
<thead>
<tr>
<th>Immediate</th>
<th>First 24 Hours</th>
<th>48 Hours</th>
<th>72 Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Get IR and BCDR Plan and assign a resource to start reviewing content</td>
<td>• Setup Collaboration and Communication systems</td>
<td>• Build Communication plan, as required</td>
<td>• First draft of Common Operational Picture (COP) available in command room</td>
</tr>
<tr>
<td>• Assign task of documenting known knowns</td>
<td>• Command room / Space is established</td>
<td>• Key Contact list completed</td>
<td>• All workstreams fully up and running</td>
</tr>
<tr>
<td>• Assign task of understanding business impact</td>
<td>• Activate the full IR Team</td>
<td>• Operational Cycle is defined</td>
<td>• Containment / Eviction plan developed</td>
</tr>
<tr>
<td>• Assign task of checking sensitive data (CIA)</td>
<td>• Drive creation and update of Core Response Objectives</td>
<td>• Known Knowns are more developed (i.e., incident timeline, business impacts, objectives)</td>
<td>• Recovery plan, where feasible, started</td>
</tr>
<tr>
<td>• Appoint an Incident Commander</td>
<td>• Workstreams update</td>
<td>• Materials for analysis are available (e.g., images, interview)</td>
<td>• Initial Communications, as required, completed</td>
</tr>
<tr>
<td>• Consult Legal Counsel</td>
<td>• Analysis Workstream briefs the known knowns and initial containment recommendations</td>
<td>• Recovery Workstream has a working plan developed</td>
<td></td>
</tr>
<tr>
<td>• Consider Core Response Objectives</td>
<td>• Determine if Communications Workstream is required</td>
<td>• Second status meeting held</td>
<td></td>
</tr>
<tr>
<td>• Activate Core IR Team</td>
<td>• Complete first status meeting</td>
<td>• Second update published</td>
<td></td>
</tr>
<tr>
<td>• Start primary workstream</td>
<td></td>
<td>• Rolling Action Item Log (RAIL) in place</td>
<td></td>
</tr>
<tr>
<td>• Schedule first status meeting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Publish CIRT Command Structure and Key Points of Contact</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Local Hardware (on-prem)

<table>
<thead>
<tr>
<th>Immediate</th>
<th>First 24 Hours</th>
<th>48 Hours</th>
<th>72 Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Get IR and BC/DR Plan and assign a resource to start reviewing content</td>
<td>• Setup Collaboration and Communication systems</td>
<td>• Build Communication plan, as required</td>
<td>• First draft of Common Operational Picture (COP) available in command room</td>
</tr>
<tr>
<td>• Assign task of documenting known knowns</td>
<td>• Command room / space is established</td>
<td>• Key Contact list completed</td>
<td>• All workstreams fully up and running</td>
</tr>
<tr>
<td>• Assign task of understanding business impact</td>
<td>• Activate the full IR Team</td>
<td>• Operational Cycle is defined</td>
<td>• Containment / Ejection plan developed</td>
</tr>
<tr>
<td>• Assign task of checking sensitive data (CIA)</td>
<td>• Drive creation and update of Core Response Objectives</td>
<td>• Known Knowns are more developed (i.e. incident timeline, business impacts, objectives)</td>
<td>• Recovery plan, where feasible, started</td>
</tr>
<tr>
<td>• Appoint an Incident Commander</td>
<td>Workstream update</td>
<td>• Materials for analysis are available (e.g., images, interviews)</td>
<td>• Initial Communications, as required, completed</td>
</tr>
<tr>
<td>• Consult Legal Counsel</td>
<td>• Analyze Workstream briefs known knowns and initial containment recommendations</td>
<td>• Recovery Workstream has a working plan developed</td>
<td></td>
</tr>
<tr>
<td>• Consider Core Response Objectives</td>
<td>• Recovery Workstream briefs business impact(s) and recovery objectives</td>
<td>• Second status meeting held</td>
<td></td>
</tr>
<tr>
<td>• Activate Core IR Team</td>
<td>• Determine if Communications Workstream is required</td>
<td>• Second update published</td>
<td></td>
</tr>
<tr>
<td>• Start primary workstreams</td>
<td>• Complete first status meeting</td>
<td>• Rolling Action Item Log (RAIL) in place</td>
<td></td>
</tr>
<tr>
<td>• Schedule first status meeting</td>
<td>Publish CIRT Command Structure and Key Points of Contact</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

# Cloud Service (cloud)

<table>
<thead>
<tr>
<th>Immediate</th>
<th>First 24 Hours</th>
<th>48 Hours</th>
<th>72 Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Get IR and BC/DR Plan and assign a resource to start reviewing content</td>
<td>• Setup Collaboration and Communication systems</td>
<td>• Build Communication plan, as required</td>
<td>• First draft of Common Operational Picture (COP) available in command room</td>
</tr>
<tr>
<td>• Assign task of documenting known knowns</td>
<td>Command room / space is established</td>
<td>• Key Contact list completed</td>
<td>• All workstreams fully up and running</td>
</tr>
<tr>
<td>• Assign task of understanding business impact</td>
<td>• Activate the full IR Team</td>
<td>• Operational Cycle is defined</td>
<td>• Containment / Ejection plan developed</td>
</tr>
<tr>
<td>• Assign task of checking sensitive data (CIA)</td>
<td>• Create / Validate secure space for response activities</td>
<td>• Known Knowns are more developed (i.e. incident timeline, business impacts, objectives)</td>
<td>• Recovery plan, where feasible, started</td>
</tr>
<tr>
<td>• Appoint an Incident Commander</td>
<td>• New account or a clean separate account</td>
<td>• Materials for analysis are available (e.g., images, interviews)</td>
<td>• Initial Communications, as required, completed</td>
</tr>
<tr>
<td>• Consult Legal Counsel</td>
<td>• Assign task to validate logging needs</td>
<td>• Recovery Workstream has a working plan developed</td>
<td>• Account, user, policies, and other credentials validated</td>
</tr>
<tr>
<td>• Contact CSP/SaaS and review/create ticket/case early in order to start a dialogue (this can be critical so do it early/late)</td>
<td>• Determine roles / policies for response team</td>
<td>• Second status meeting held</td>
<td></td>
</tr>
<tr>
<td>• Consider Core Response Objectives</td>
<td>• Ensure assessment of ephemeral systems and systems with ‘console only’ access</td>
<td>• Second update published</td>
<td></td>
</tr>
<tr>
<td>• Activate Core IR Team</td>
<td>• Assign task to validate logging/analysis assumptions</td>
<td>• Rolling Action Item Log (RAIL) in place</td>
<td></td>
</tr>
<tr>
<td>• Start primary workstreams</td>
<td>• Include API analysis account to account</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Review and understand Chain of Custody for the CSP(s)</td>
<td>• Drive creation and update of Core Response Objectives</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Schedule first status meeting</td>
<td>Workstream update</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Publish CIRT Command Structure and Key Points of Contact</td>
<td>Workstream update</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Analyze Workstream briefs known knowns and initial containment recommendations</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Recovery Workstream briefs business impact(s) and recovery objectives</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Determine if Communications Workstream is required</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Assign POC to work with CSP/SaaS to generate rough costing model for response, to include possible license upgrades</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Complete first status meeting</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Local Hardware (on-prem)

<table>
<thead>
<tr>
<th>Immediate</th>
<th>First 24 Hours</th>
<th>48 Hours</th>
<th>72 Hours</th>
</tr>
</thead>
</table>
| - 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 | - Setup Collaboration and Communication systems  
- Build Communication plan, as required  | - First draft of Common Operational Picture (COP) |
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.
"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)

<table>
<thead>
<tr>
<th>Immediate</th>
<th>First 24 Hours</th>
<th>48 Hours</th>
<th>72 Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get IR and BC/DR Plan and assign a resource to start</td>
<td>Setup Collaboration and Communication systems</td>
<td>Build Communication plan, as required</td>
<td>First draft of Common Operational Picture (COP)</td>
</tr>
</tbody>
</table>

### 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 assessment 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
  - 4 IPs (2 x NAT Gateway, 2 x actual src/dst)
  - Not all underlying traffic is logged by CSP
    - 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
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.
<table>
<thead>
<tr>
<th></th>
<th>Immediate</th>
<th>First 24 Hours</th>
<th>48 Hours</th>
<th>72 Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Get IR and BC/DR Plan and assign a resource to start</td>
<td>Setup Collaboration and Communication systems</td>
<td>Build Communication plan, as required</td>
<td>First draft of Common Operational Picture (COP)</td>
</tr>
</tbody>
</table>

**48 Hours**

- 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
Communication

- Tempo/SLAs
- Communication Plans
- Critical Findings
- Boundaries
# Local Hardware (on-prem)

<table>
<thead>
<tr>
<th>Immediate</th>
<th>First 24 Hours</th>
<th>48 Hours</th>
<th>72 Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get IR and BCDR Plan and assign a resource to start</td>
<td>Setup Collaboration and Communication systems</td>
<td>Build Communication plan, as required</td>
<td>First draft of Common Operational Picture (COP) available in command room</td>
</tr>
</tbody>
</table>

## 72 Hours

- 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
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

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

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

So these are also what we should be logging!
KM Guidance

Influence your ticket and logging processes and procedures.
Conclusion, thank you, and questions

Rob Floodeen - robert.floodeen@newanderton.com

Rebecca Taylor - rtaylor@secureworks.com
Thank you!

Rob Floodeen - robert.floodeen@newanderton.com
Rebecca Taylor – rtaylor@secureworks.com