2020 SANS Enterprise Cloud Incident Response (IR) Survey Results

Today's Speaker

- Chris Dale, Certified Instructor, SANS, and Principal Consultant, River Security

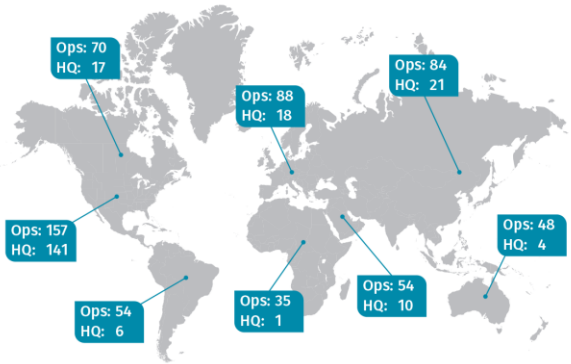
Survey Respondents

Top 4 Industries Represented

- Technology
- Cybersecurity
- Government
- Banking and finance

Each gear represents 10 respondents.

Operations and Headquarters



Organizational Size

- **Small** (Up to 1,000)
- **Small/Medium** (1,001–5,000)
- **Medium** (5,001–15,000)
- **Medium/Large** (15,001–50,000)
- **Large** (More than 50,000)

Each building represents 10 respondents.

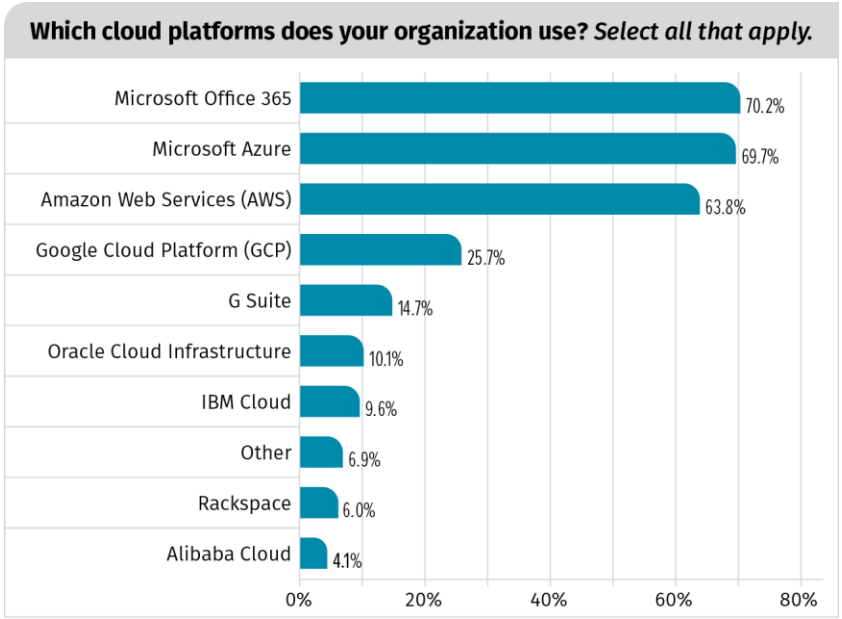
Top 4 Roles Represented

- Security administrator/ Security analyst
- IR team leader
- Security manager or director
- Security architect

Each person represents 10 respondents.

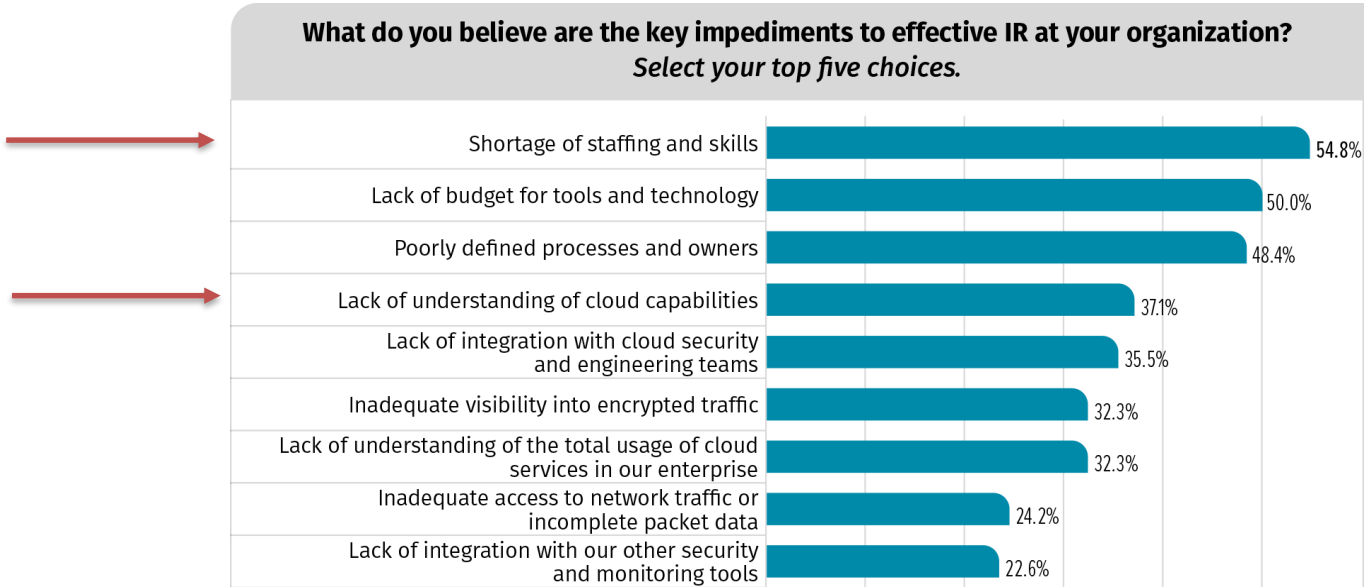
Cloud Platforms

- Difference in what they're solving:
  - Some support business processes.
  - Others are for provisioning of services.
- Many are using multiple cloud platforms.



A Potential Concern

- We might be biting off more than we can chew.



Traditional Approach to Cloud

Are we seeking to solve before seeking to understand?

- Infrastructure-as-a-service (IaaS) instead of serverless
- IaaS instead of platform-as-a-service (PaaS)
- IaaS instead of software-as-a-service (SaaS)

In response to “shortage of staffing and skills”—we need to do more with less.

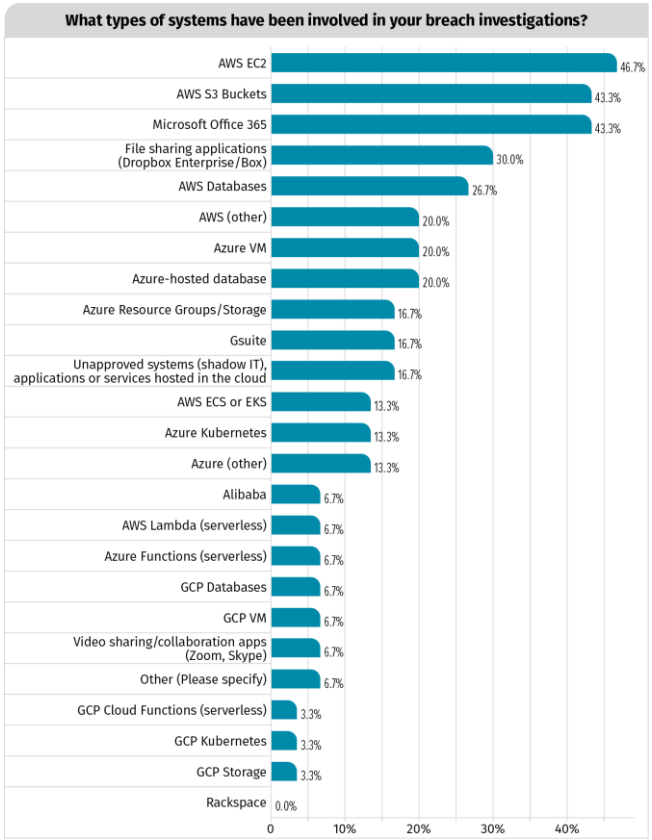
Doing More With Less

- Headcount does not necessarily grow proportionally with the number of services provisioned.
- Luckily, we live in the Age of Information:
  - A proof-of-concept is normally just hours away.
  - Information is quite reliable, and authors often reply to inquiries about their content.
- Cloud providers should continue their efforts in making their services “POC-able.”

Traditional Components Are the Most Breached

Analyst Program

Traditional components—such as file storage and IaaS—are typically involved in breaches.



Traditional Cloud vs. Tailored Approach

Analyst Program

- Traditional:
  - Large attack surface
  - Open by default
  - Example: IaaS
- Tailored Approach:
  - Least amount of privileges
  - Very limited attack surface
  - Example: Functions as a service

Example: You breach code deployed as a function vs. a breach of IaaS.

A tailored approach is more daunting and requires investing more in understanding and skills before solving the problem.

Breakout Times

Time it takes from compromise to lateral movement:

- Often within hours

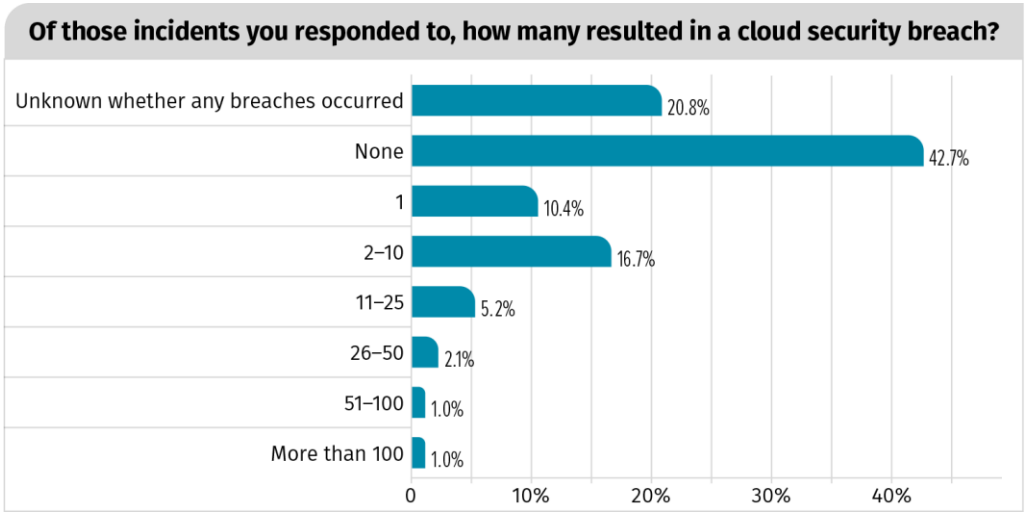
Harder within cloud environments:

- Cloud environments have built-in resilience, in many cases, due to default segmentation.
- They are hardened by default, with the least amount of privileges—especially for tailored services.

Cloud-Attacker and Cloud-Defender Maturity

Analyst Program

Attacks on cloud environments do not appear to compromise the rest of the cloud infrastructure.



Why Not Cloud Security Breach?

Analyst Program

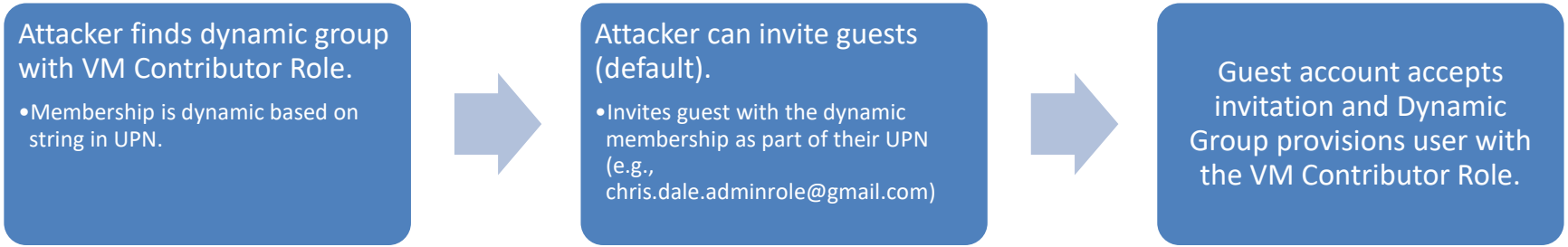
- Attackers' TTPs are not focused on cloud security breach.
- Attackers have not yet matured to this point, and they are incapable of performing such attacks.
- Defenders fail to detect that attackers are already compromising the rest of their cloud infrastructure.
- Cloud services are more resilient, with built-in segregation and least amount of privileges

Future of Attacker TTPs?

- A full cloud infrastructure compromise is extremely fruitful for attackers.
- Without a doubt, attackers will focus on this more.
- Attack paths to accomplish this are possible:
  - Not necessarily by compromising the cloud itself, but perhaps through leveraging chained attacks to try to compromise developers and administrators.

Dynamic Groups Abuse

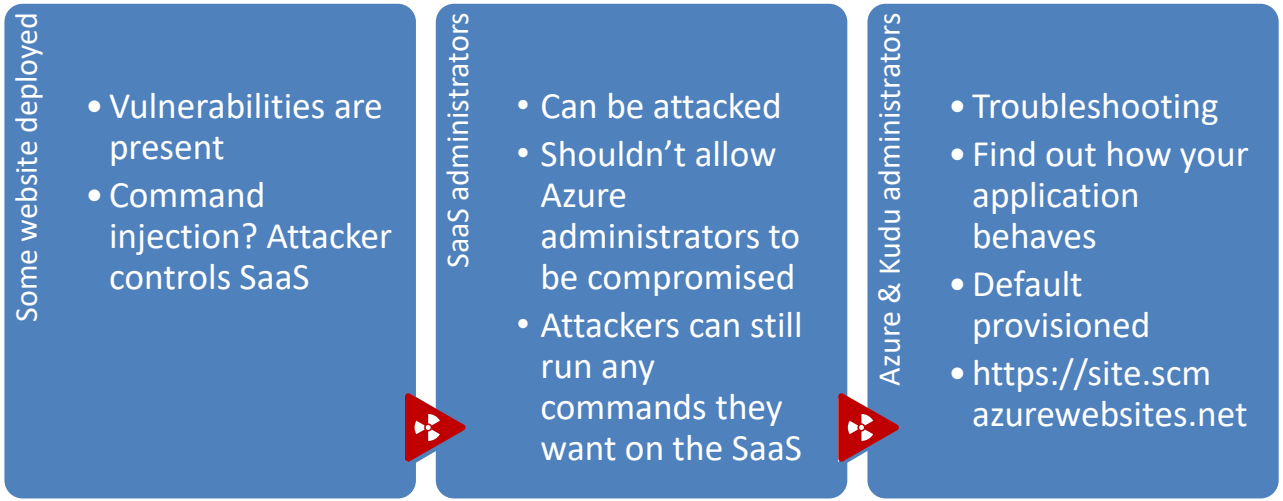
Azure Dynamic Groups could lead to privilege escalation



Source: https://www.mnemonic.no/blog/abusing-dynamic-groups-in-azure/

Cloud Escapes Are Real

- But not something that we expect to see on a regular basis with the more mature providers.

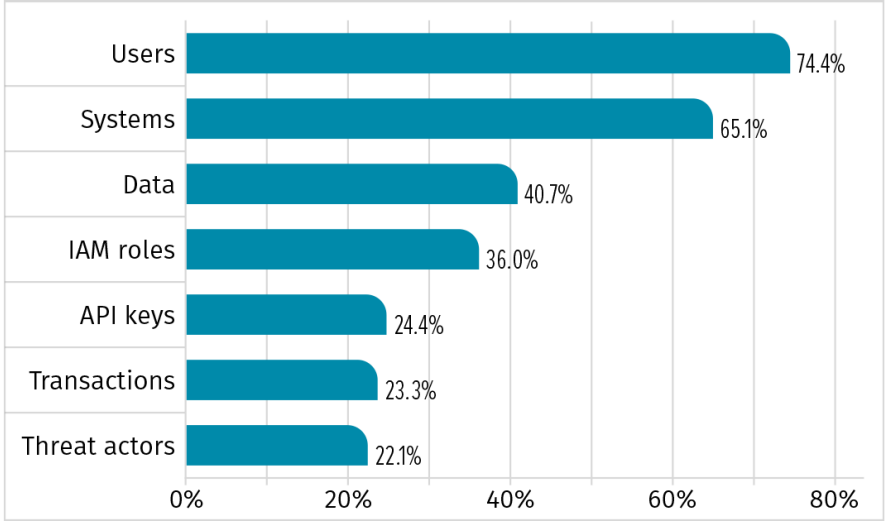


https://www.sans.org/blog/azure-0day-cross-site-scripting-with-sandbox-escape/

Ability to Discover Impact

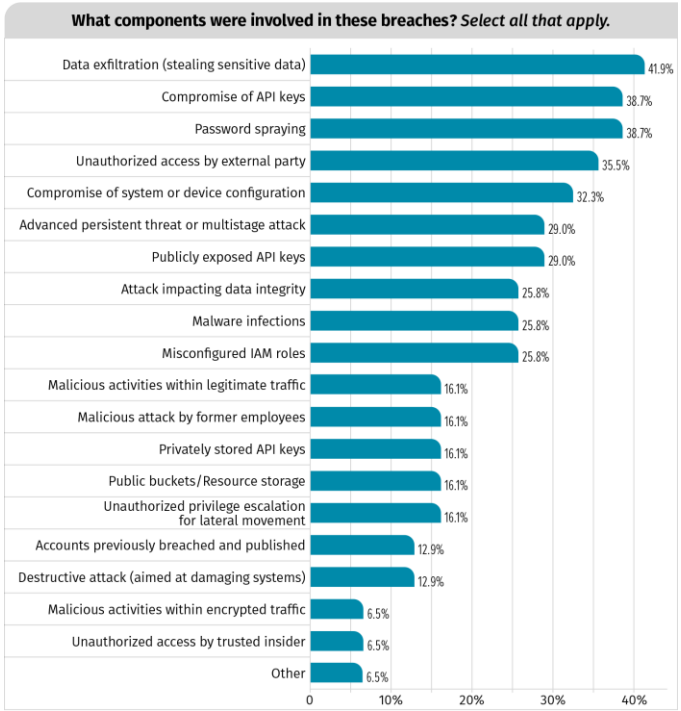
Analyst Program

When investigating these incidents and breaches, were you able to consistently and accurately discover the impacted API keys, IAM roles, users, systems, data, transactions and threat actors involved? ***Select all that apply.***



Breached Components and Impacted Systems

Analyst Program



- Data is the new currency.
- Hard to conclude consequences:
  - Scoping changes quickly.
  - Data can have value short-term and long-term.
- Regulatory and legal requirements:
  - PII
  - Health care

Timing: An Important Attribute

- Breakout is already at a record low.
- What about detection, containment and remediation in cloud environments?

Table 1. Compromise to Detection to Containment to Remediation

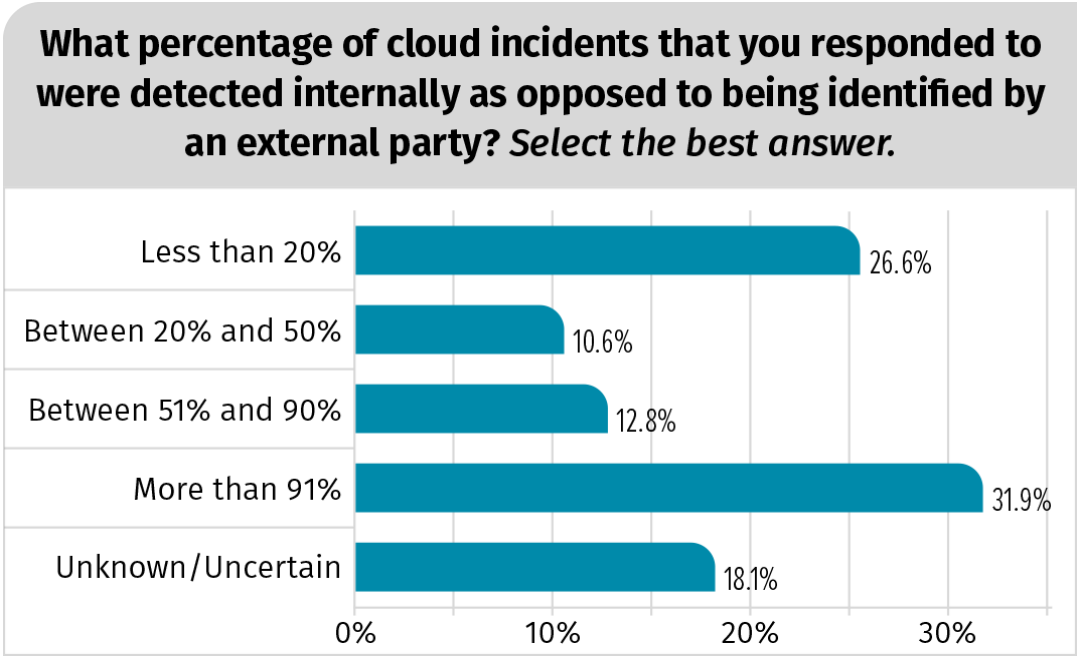
Duration	Time from Compromise to Detection	Time from Detection to Containment	Time from Containment to Remediation
Unknown	19.2%	7.7%	11.5%
Less than 1 hour	3.8%	19.2%	15.4%
1–5 hours	0.0%	30.8%	15.4%
6–24 hours	19.2%	15.4%	7.7%
2–7 days	30.8%	23.1%	23.1%
8–30 days	11.5%	3.8%	15.4%
1–3 months	15.4%	0.0%	3.8%
4–6 months	0.0%	0.0%	3.8%
>1 year	0.0%	0.0%	3.8%

Speed and Agility

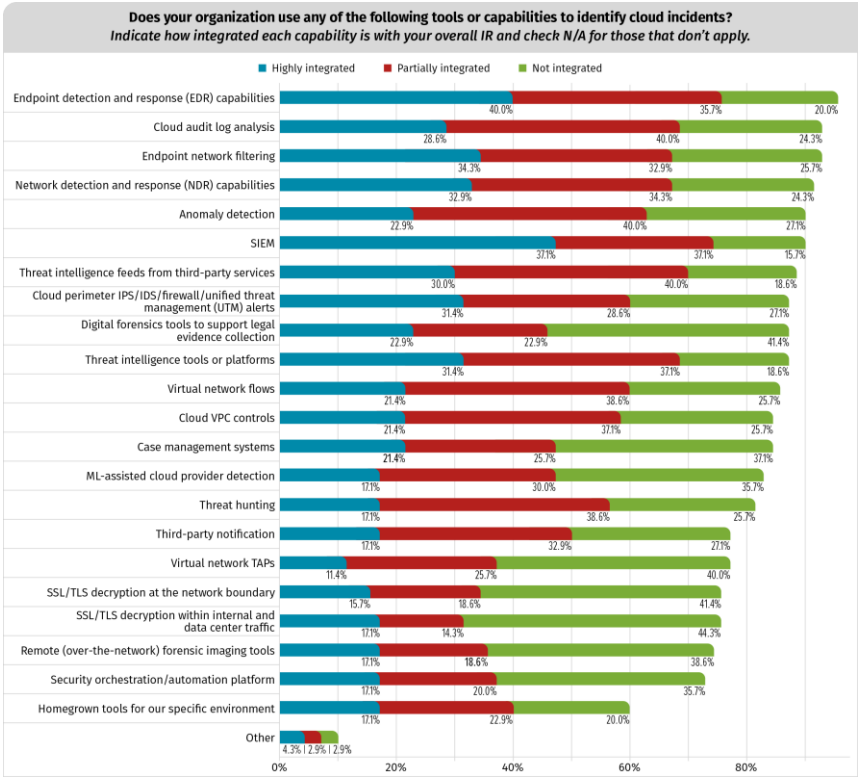
- Cloud as an enabler for both speed and agility: Dwell time is still too high.
- Cloud environments often enable:
  - Infrastructure as code
  - Elastic scaling
  - Third-party notifications
  - Visibility into provisioned services and assets
  - Management tools and logging

Third-Party Notifications: Symbiosis with Cloud Provider

Analyst Program



Tools and Capabilities: The Status Quo



Preferred Cloud-Generated Data

Table 2. Cloud-Generated Data by Preference

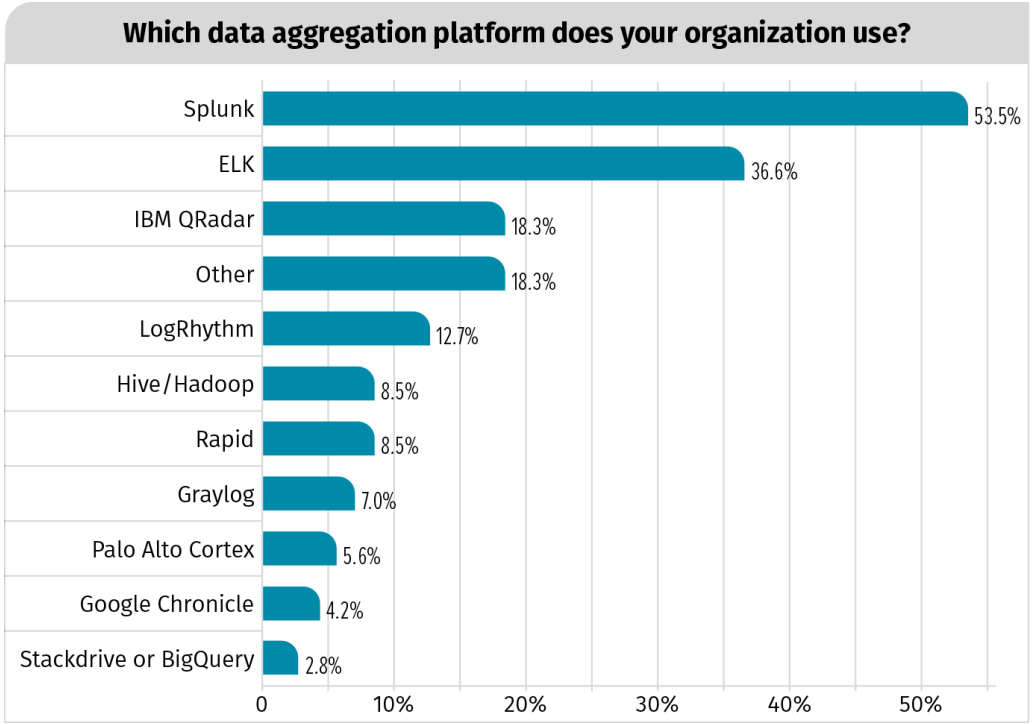
Data Types	Need But Can't Acquire
Data from endpoints (virtual machines/containers)	8.5%
Host, domain and URL reputation data	5.6%
Indicator of compromise (IoC) threat intelligence data	9.9%
Short-term historical event data and logs (as much as seven days old) from SIEM	5.6%
Long-term historical event data and logs (older than seven days) from SIEM	12.7%
Virtual network TAPs	23.9%
Virtual network flows	18.3%
Transaction data from encrypted network traffic	38.0%
Cloud audit logs (Microsoft Azure Audit Logs, AWS CloudTrail, Microsoft Office 365 audit logs, etc.)	2.8%
ML/AI-assisted cloud provider detections (Amazon GuardDuty, Microsoft Azure Sentinel, Google Cloud Security Command Center)	11.3%
Related alarms from IPS, antivirus, network detection and SIEM	8.5%
Threat campaign data	21.1%
Vulnerability data	5.6%
Other	2.8%

A Crypto Paradox: The Desire for Network Traffic

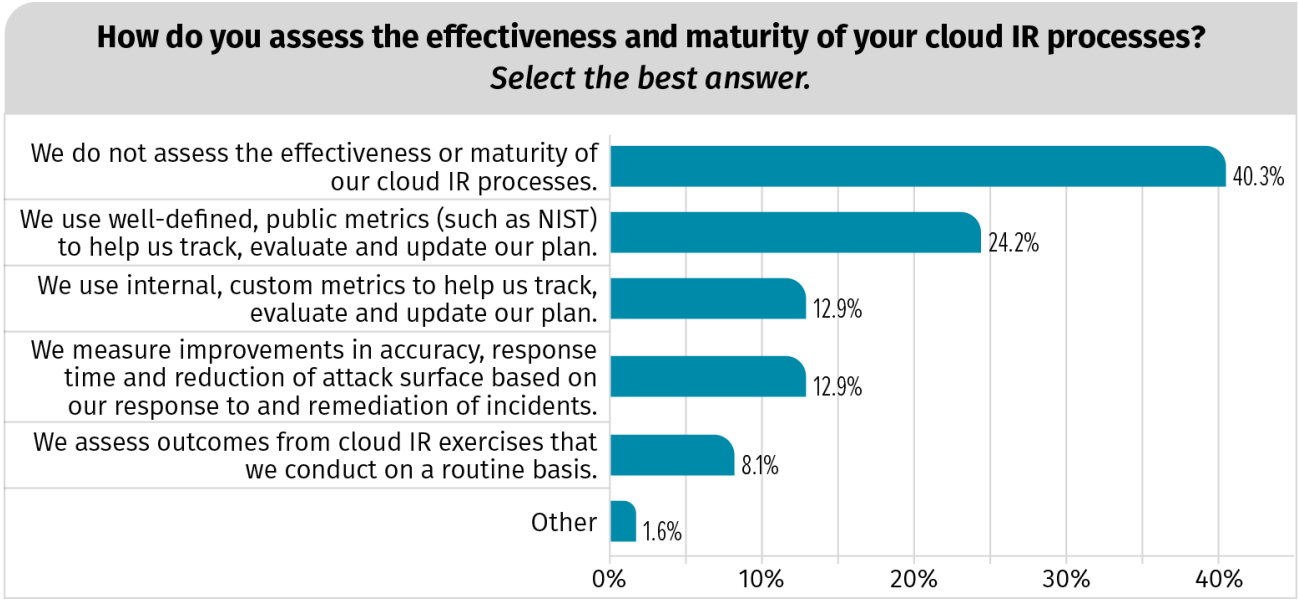
- Traffic is often hard to support, as the cloud provider must facilitate network stack—shared with other tenants.
- Decryption is not always desired, as we long for end-to-end encryption, especially not allowing third party access.
- TLS 1.3 supports encryption of SNI, making it harder to gain visibility.
- Out-of-band decryption is a possible and likely a solution.

Current Data Aggregation

Analyst Program



Maturity


How do you assess the effectiveness and maturity of your cloud IR processes?
Select the best answer.
We do not assess the effectiveness or maturity of our cloud IR processes.
40.3%
We use well-defined, public metrics (such as NIST) to help us track, evaluate and update our plan.
24.2%
We use internal, custom metrics to help us track, evaluate and update our plan.
12.9%
We measure improvements in accuracy, response time and reduction of attack surface based on our response to and remediation of incidents.
12.9%
We assess outcomes from cloud IR exercises that we conduct on a routine basis.
8.1%
Other
1.6%
0%
10%
20%
30%
40%

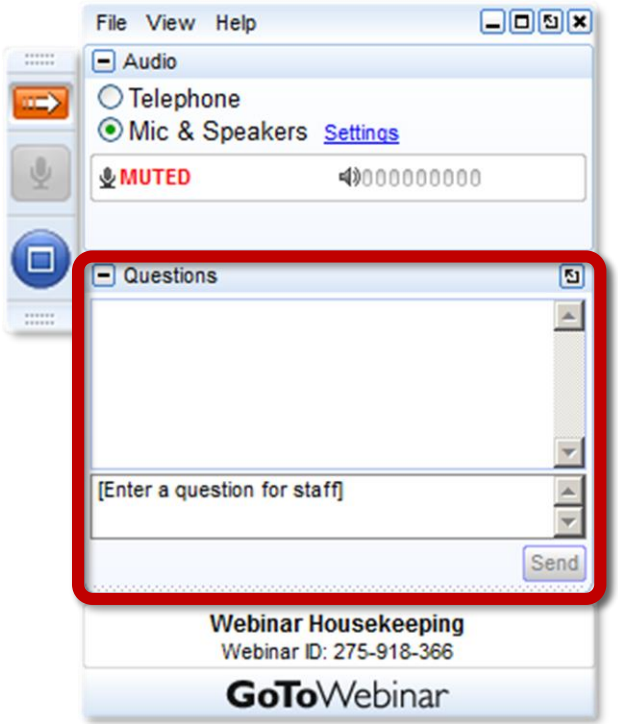
Stifling Innovation: Not an Option

- Cloud provides opportunities to be seized:
  - Is the security organization the one to say, “No,” or should we instead seek to be agile and control the risk?
- We might not be trained for the latest opportunities that the cloud offers:
  - But the fruits to be picked might be ripe.
  - When do we declare ourselves ready for new technology vs. the “traditional-and-safe” approach?
- Cloud might enable us to take back the advantage:
  - More work for attackers, for less value
  - Multiple benefactors with similar goals

Q&A

Please use **GoTo**Webinar's Questions tool to submit questions to our panel.

Send to "Organizers" and tell us if it's for a specific panelist.



Acknowledgments

Thanks to our sponsors:

And to our attendees, thank you for joining us today!