How to Build an Effective Cloud Threat Intelligence Program in the AWS Cloud

Dave Shackleford
The cybersecurity community has been thinking about and discussing the topic of threat intelligence for a number of years. Threat intelligence is not a simple concept to clarify, however. For example, what data do you collect to aggregate and collectively identify as threat intelligence? Many analysts agree that threat intelligence does not consist of just one type or one source of data, and is not gathered purely from either internal or external sources (a combination is most prevalent). Threat intelligence is also not one form of analysis or reporting. It can mean different things to different organizations. In this paper, we discuss what threat intelligence is, why it’s important, and how to develop a cloud threat intelligence (CTI) program that improves an organization’s security posture and increases the speed and effectiveness at which analysts can resolve security events.

### Threat Intelligence

What, exactly, constitutes “threat intelligence”? Threat intelligence is the set of data collected, assessed, and applied with regard to:

- **Security threats**: The types of security events and potential methods of unauthorized access deployed against an investigation
- **Bad actors**: The individuals behind the security events taking place in organizations’ environments
- **Exploits**: Exploit tools, code, and other mechanisms in use during security events
- **Malware**: Code, usually automated, that performs a variety of unauthorized or illegal actions once executed
- **Vulnerabilities**: The means by which unauthorized access attempts and security events manifest on targeted systems and environments
- **Compromise indicators**: Unique attributes and detectable signs of events and behaviors indicating unauthorized activity
Why Focus on Threat Intelligence?

Why should organizations focus on threat intelligence? There are multiple answers to this question, some simple and others more complicated. One simple response might be that bad actors are innovating faster than defenders. The more complicated answers have a few distinct elements, though:

- **“Productization” of malware**—Bad actors are building enterprise-class software “attack kits” that are sold freely on underground markets. Many of these are built to perform specific actions, such as encrypting data (ransomware) and mining cryptocurrency. We’ve also seen significant reuse of malware and command and control (C2) protocols, as well as service-based malware companies (that, for instance, rent botnets). These business-focused initiatives on the part of bad actors are actually useful in building more effective threat intelligence about them over time.

- **Wisdom of crowds**—Few unauthorized activities are unique, so other organizations have likely seen any particular type of activity before. Repeated unauthorized patterns and indicators can easily be broken down into recognizable elements, which can then be shared directly or through some third-party intelligence dissemination services.

- **Service provider visibility**—With more bad actors and unauthorized activity patterns seen constantly, service providers that host systems and content can develop threat intelligence based on large quantities of data spanning numerous industries and types of clients. These capabilities can be integrated into in-house threat intelligence functions or used standalone in the service provider environment. Leveraging this large-scale threat intelligence production can be another way to benefit from different organizations’ experiences to help optimize defenses.

As organizations progressively move assets into the cloud, the need to emphasize threat intelligence is even greater. Bad actors know that organizations are moving into the cloud and targeting essential assets and infrastructure more than ever before. Building unauthorized activity and bad actor profiles in software-defined data centers can provide clues to security events and unauthorized activity patterns, assets and specific targets, and new cloud-focused techniques that analysts should be aware of when updating security detection and response playbooks.
As unauthorized activities grow more sophisticated, investigators have to aggregate and analyze more discrete pieces of information about security events and bad actors to potentially determine what is happening. Threat intelligence can play a major role in improving the state of security incident-handling operations, either through proactive threat hunting activities or during active investigations based on detection scenarios. Intelligence-driven investigations are based on the preservation of the relationships between the components of individual unauthorized activities so that they can be clustered as a campaign. Some of the investigative components involved in building threat intelligence include:

- **Malware analysis**—While potentially time-consuming, this can be extremely valuable in developing detailed threat intelligence. This intelligence could be relatively lightweight (with simple observations of behavior or file attributes) or complex (specific code snippets or internal details only gleaned from reverse engineering). Because many bad actors’ campaigns leverage various types of malware, such as ransomware, cryptocurrency mining agents, and so on, efforts in malware inspection and analysis are invariably useful.

  While analysis for cloud-focused malware doesn’t differ from traditional malware analysis processes or tools, security operations teams may find that building malware sandboxes in the cloud is more efficient and productive than bringing samples and artifacts on premises. Likewise, some malware analysis may be handled and processed automatically by cloud-native guardrails and services that detect indicators and behaviors when they are seen or occur.

- **Network analysis**—Many aspects of threat intelligence rely on deep network analysis and indicators. The first key element of network analysis is behavioral flow data that can help analysts build patterns of communication within a network environment. The second is threat detection, with deep analysis of traffic at all layers to look for specific patterns matching exploits, C2 behavior, exfiltration of data, and more.

  In the cloud, the only factors that change are how analysts inspect traffic and some of the specific indicators assessed. Network flow data can be acquired easily with controls, such as Amazon VPC Flow Logs, and then sent to storage nodes for processing and analysis. Capturing traffic and analyzing the data for specific patterns and unauthorized access attempts may require packet mirroring with tools such as Amazon VPC Traffic Mirroring, which can send select network traffic to analysis platforms, third-party firewalls, or network detection and response (NDR) and intrusion detection platforms that are easily integrated from the cloud marketplace.

---

1. This paper mentions solution names to provide real-life examples of how cloud security tools can be used. The use of these examples is not an endorsement of any solution.
• **Big data analysis of log/event patterns and security analytics**—In many ways, security analytics services and platforms are somewhat like a SIEM platform at larger and faster scale. SIEM tools normalize and correlate data to allow analysts to more accurately detect related events and find patterns of events that indicate anomalous behavior. Security data analytics do the same, but with larger datasets (and aided by machine-learning capabilities). In this way, incident detection and response efforts could potentially be more targeted and in-depth than they are currently.

For the cloud, most security event information will largely come from cloud control plane logging, any cloud assets producing logs, network data, and third-party intelligence (covered next). Native services, such as AWS Security Hub, Amazon Detective, and Amazon GuardDuty, can analyze huge quantities of information to produce security events or notifications. Leading cloud-native SIEM solution providers, such as Sumo Logic and Securonix, are excellent options for security analytics as well.

• **Underground analysis**—Third-party threat intelligence feeds may also be valuable in providing details of threats, most often in conjunction with malware analysis, network analysis, and event analytics processing. Many threat intelligence and other security providers pay close attention to the threat landscape, new unauthorized activity patterns, and specific indicators of attacks (IoAs) seen in the wild, and can offer current details about unauthorized activities that organizations may not have seen yet.

In the cloud, both cloud service providers and third-party partners can offer this type of underground analysis and content, which analysts then often analyze in context with other internal data. Providers such as Recorded Future have been progressively offering more cloud-focused threat intelligence feeds for some time.

Additionally, teams can help build knowledge of the types of bad actors. These groups might include unsophisticated actors, organized illegal campaigns, competitor or insider activity, and state-sponsored actors. Over time, it is possible to develop patterns and tactics used by bad actors that are more tuned to the types of organizations, assets, and cloud services in use by gathering and analyzing threat intelligence data.
Building Cloud-Focused Threat Intelligence

Organizations can gather a variety of threat intelligence. The first type is what we refer to as indicators of compromise (IoCs). These fall into several categories:

- **Atomic**—These are simple, static aspects of unauthorized activity that cannot be broken down. Examples include IP addresses, email addresses, and vulnerability identifiers.

- **Computed**—These are derived from captured/gathered data in the environment. Examples include hash values and regular expression (regex) pattern matches.

- **Behavioral**—Collections of atomic and computed indicators can present behavioral indicators over time. For example, imagine that `<IP X>` communicated with `<IP Y>` with `<pattern match>` for `<XX seconds>` and retrieved `<Z hash value>` file.

While IoCs are valuable and useful, better areas for mature security analysts to focus on are tactics, techniques, and procedures (TTPs), which are groups of IoCs and behaviors noted consistently together in patterns. More relevant and useful threat intelligence usually refers to any information pertaining to the TTPs bad actors use to carry out campaigns. Security analysts and researchers can learn how bad actors operate and monitor ongoing campaigns via technical indicators and available information.

To enable a robust threat intelligence function within the security operations organization, both external and internal threat intelligence is important. Generally speaking, external threat intelligence consists primarily of warnings and indicators coming from third-party organizations. Internal threat intelligence is built from indicators actually noted in the environment, such as historical events and real alerts and data points. Internal threat intelligence can provide longer-term baselines and value to the organization for monitoring and defensive strategy. Internal data can also help develop better IoAs and IoCs. External threat intelligence may resemble the same types of data gathered from internal threat intelligence teams (IoCs and behaviors), but is offered and provided by third-party providers.

The cloud shifts threat detection in a number of ways. First, analysts should ensure that they are gathering indicators internally, in hybrid configurations, and in cloud-native scenarios. All of these together will potentially be needed to develop a comprehensive analysis of threats in their environments. Second, analysts should bring in more cloud-native cloud intelligence, ranging from intelligence components, such as URLs, IPS signatures, and more static measures, to behavior patterns seen in the environments. Finally, they need more focus on cloud-specific security events, targeting, and scenarios.
A good example is the MITRE ATT&CK® framework for cloud events, which includes the following phases:

- **Initial Access**—The period when a bad actor finds an initial means of ingress into cloud accounts or resources. In the cloud, this might include unauthorized use of internet-facing applications and systems.

- **Persistence**—The phase when a bad actor seeks to stage a foothold in the victim’s environment to ensure they can return at will. After gaining unauthorized access to a cloud environment or asset, they may try to manipulate accounts, create redundant access, or create new accounts.

- **Privilege Escalation**—In a cloud setting, the most common method for this is to attempt access with or to valid accounts within the environment, or to manipulate identity role assignment to then use these valid accounts.

- **Defense Evasion**—Bad actors will usually seek to avoid defenses in unauthorized activity scenarios. Some of the common ways that they may seek to avoid defenses in a cloud environment include reverting cloud instances to a previous state, starting resources in unused regions, or looking to compromise or use legitimate accounts.

- **Credential Access**—Many bad actors will seek to leverage existing accounts and credentials in the cloud to perpetuate or advance unauthorized access.

- **Discovery**—There are many opportunities/locations for asset and service discovery in the cloud, including cloud service discovery, network share and service discovery, and more.

- **Collection**—The goal of many bad actors is to access and collect data and other assets of value. Their focus is usually on cloud storage, as well as other exposed cloud data.

- **Exfiltration**—After gaining unauthorized access to data, many campaigns lead to eventual exfiltration of data to a location under the bad actor’s control.

- **Impact**—The final potential stage of the ATT&CK framework is eventual cloud service impact, which is categorized in the current model as Resource Hijacking.

Threat intelligence programs should ideally align with known models so that IoCs and TTPs can be more accurately developed and analyzed in the context of real-world scenarios.

---

https://attack.mitre.org/matrices/enterprise/cloud/
Creating a Comprehensive Cloud Threat Management Ecosystem

Building a cloud threat intelligence model requires a number of important elements. Analysts should keep in mind data diversity, data analysis capabilities, and data quality when looking to create cloud threat intelligence. We discuss these factors and more in the following sections.

Data Diversity

The first key aspect of threat intelligence capability is data diversity. Consider these questions:

- **Where does the data originate?** Look at cloud service providers, partners, and internal threat intelligence sources.
- **What type(s) of data do you have?** In the cloud, there are now many varieties of data to process, such as network flow data, cloud control plane logs, workload events, and others.
- **Do IoC artifacts come in one format (i.e., file hashes) or multiple?** Security data formats will need to be collected, processed, parsed, and integrated with other data.
- **What specifics are available and provided (e.g., vertical/industry, geography)?** Some providers offer threat intelligence data specific to certain verticals and industries, as well as technologies such as industrial control systems and others.

Data Analysis Capabilities

The second aspect of cloud threat intelligence is data analysis capabilities. The cloud offers more capacity to analyze and process data at significant scale, compared to internal and on-premises data analytics. Be sure to ask the following questions:

- **What kind of analysis can be performed?** The cloud offers more tools, services, and data processing capabilities than traditionally available on premises, so this is usually a strong feature of cloud threat intelligence.
- **To what depth is analysis done?** For example, does the analysis focus more on basic IoCs or full behavioral introspection? Most internal threat intelligence can be built from IoCs such as AWS CloudTrail log data and specific data points, network logs such as Amazon VPC Flow Logs, and others. However, more detailed and thorough analysis is available with services such as Amazon GuardDuty or AWS Security Hub.
- **Is the data correlated with other information?** For detailed threat intelligence correlation, analysts will likely use a security event management platform or service, such as a SIEM. A wide variety of cloud-native and cloud-centric services can ingest cloud event data to provide deeper correlation and analysis capabilities.
Data Quality

The third key element of cloud threat intelligence is data quality. In traditional threat intelligence programs, data gathered may be somewhat unclear depending on its source, requiring additional analysis and investigation to verify accuracy. In cloud-centric scenarios, this is less common, because the data is provided directly from service providers or gathered from the environment itself. However, it’s still a good idea to answer the following questions:

- Does the data go through a QA process?
- Is data revisited/re-analyzed to ensure it is still accurate?
- When are indicators “expired”?

Many of these are questions to ask cloud providers and threat intelligence service providers as part of contract negotiations, but for any data gathered or developed, organizations need to determine the expiration strategy/life cycle for developing and maintaining threat intelligence data on an ongoing basis. Often, threat intelligence data is limited in its applicability after more than several days.

Agents for Workloads

To implement cloud-based threat intelligence, analysts will need to adapt the tools and services they use. First, any agents for workloads should be specific to cloud environments. Cloud workload protection platforms (CWPPs) are workload-centric security offerings that target the protection requirements of server workloads in modern hybrid data center architectures.

CWPPs should provide visibility and control for physical machines (ideally), virtual machines, containers, and serverless workloads, regardless of location. CWPP offerings protect the workload from unauthorized access, typically using a combination of network segmentation, system integrity protection, application control, behavioral monitoring, host-based intrusion prevention, and optional anti-malware protection. In many cases, the vendors in this space may reference zero trust and microsegmentation capabilities, as well as endpoint detection and response (EDR) functionality. Leading providers include functionality such as strong endpoint malware sandboxing and detection/response, threat intelligence integration, encryption for data at endpoints, and application control/whitelisting. More advanced detection and prevention capabilities may also include exploit prevention/memory protection and behavioral monitoring.

Traditional endpoint security vendors have typically offered a subset of this technology, but it’s important to find a vendor that can cover both on-premises and cloud workloads equally well and be able to protect containers and serverless platforms. Mature CWPP platforms should ideally support all container types and serverless environments in PaaS and IaaS clouds and offer agentless protection (especially in containers and serverless) and centralized management.
Organizations looking at agent-based solutions should be sure to test that the events and detection capabilities are cloud-aware. In other words, prevention and detection events should align with cloud-specific patterns and frameworks, such as ATT&CK for cloud, not just traditional security events largely seen in on-premises environments. Leading providers, such as CrowdStrike, have adapted their detection models to focus on cloud-specific attempts and events.

**Cloud Fabric Services**

A wide variety of cloud-native services is also available, including Amazon GuardDuty, AWS Security Hub, Amazon Detective, and others that can collect, aggregate, and correlate security event data and other information to provide more correlated and deeply analyzed data. Cloud threat intelligence from these services is more thoroughly analyzed through machine learning and massive scale analytics from data seen within cloud environments. Amazon GuardDuty is a managed threat intelligence service in Amazon Web Services (AWS) that collects and analyzes AWS CloudTrail logs, Amazon VPC Flow Logs, DNS logs, and external threat intelligence from third-party solutions available in AWS Marketplace. For example, Amazon GuardDuty can show details of a brute force event against the SSH service running on an Amazon EC2 instance in AWS, with information about the source (see Figure 1).

In this case, a cloud-native service is providing details about the source IP address and port of the event, the country of origin, and the service provider in use. For organizations that are tracking bad actors’ campaigns, this may be extremely valuable information, because it represents strong atomic IoCs.

**Use Cases and Scenarios**

To build an effective CTI program, it’s helpful to consider some use cases and usage scenarios, as described in the following sections, to get value from the data with cloud threat intelligence.

**Simple Direct Match/Correlation**

Directly matching specific data points between different detection services and tools can help build a more thorough analysis of unauthorized activity scenarios. For example, the Amazon Detective service could be queried for information related to the source IP address of the Brazilian actors noted in the previous SSH event data from Amazon GuardDuty. See Figure 2 on the next page.
Risk Scoring

Two other critical elements of threat intelligence are risk scoring and prioritization. Especially in busy cloud environments, these computed threat indicators can help direct focus for security operations teams. An example of analytics processing for risks in a cloud environment comes from AWS Security Hub, where the Insights feature demonstrates computed risk based on different event and service data that may indicate anomalous or unauthorized activity. As an example, AWS Security Hub has highlighted “EC2 Instances associated with adversary reconnaissance,” as shown in Figure 3.

By clicking any of the Resource ID entries, analysts could get additional detail about the events and find out the origin of the event data.

Figure 2. Amazon Detective Intelligence Query

Figure 3. AWS Security Hub Risk Analysis
**Volume Trends**

Tracking the volume of traffic and events in the environment can potentially be useful in determining that anomalous activity is happening. Some behavioral threat intelligence indicators often rely on multiple services and event feeds for processing. For example, an analyst could determine that a system in the environment is attempting to communicate to peer workloads within a subnet or VPC through detailed analysis of Amazon VPC Flow Logs, such as those shown in Figure 4, with **REJECT** messages from failed communications attempts.

---

**Managing Cloud Threat Intelligence**

To build a program of cloud threat intelligence and manage it over time, security operations and analyst teams should adhere to the following best practices:

- **Review data sources.** For any cloud-focused threat intelligence efforts (whether internally focused or coming from a third-party provider), ensure that the data sources that are enabled are appropriate and accurate. For AWS, these should include AWS CloudTrail logs, Amazon CloudWatch logging, and services such as Amazon GuardDuty and AWS Security Hub.

- **Verify that integration is functioning.** For any third-party integration to SIEM or other deeper analytics processing services, ensure that the data from the cloud events is flowing accurately and smoothly to those services. Native API integration with providers often makes this much more streamlined.

- **Perform event review.** Ensure that the event data from services such as Amazon GuardDuty is updating properly and providing adequate event detail to analyze and assess for investigations.

- **Validate cloud security event information.** Review raw event data, such as AWS CloudTrail logs, as well as third-party services and cloud-native services such as AWS Security Hub, to help ensure that all relevant event information is being reported.
• **Assess value.** Over time, determine whether the cloud threat intelligence is providing value—that is, the threat intelligence is useful, actionable, and timely.

Managing a threat intelligence program requires dedicated focus and time, because this type of data has a finite shelf life and needs to be curated and assessed for accuracy and applicability frequently.

---

**Next Steps: Retooling and Retraining Threat Intelligence Analysts in the Age of Cloud**

Building cloud threat intelligence is a sound idea for mature security operations teams, but these programs will take time and effort to set up and realize value. The first step is to enable cloud-native services for logging and analysis, such as AWS CloudTrail, Amazon VPC Flow Logs, Amazon GuardDuty, AWS Security Hub, and Amazon Detective, to better build a monitoring and analysis ecosystem in the cloud. Integration into a cloud-native SIEM or other analytics platform is advised, and specialized solutions, such as endpoint detection and response (EDR), that have been optimized for cloud use should be strongly evaluated.

Second, build threat hunting capabilities around IoCs or TTPs, using services such as Amazon Detective, to search for compromised assets. Plan to integrate internal data where applicable, using third-party platforms that can ingest and analyze broad varieties of data.

Finally, build analytics and rules using the threat intelligence to respond more effectively to security events in the cloud, ideally with alignment to cloud-centric unauthorized activity patterns that follow ATT&CK and other industry standards.
Dave Shackleford, a SANS analyst, senior instructor, course author, GIAC technical director and member of the board of directors for the SANS Technology Institute, is the founder and principal consultant with Voodoo Security. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. A VMware vExpert, Dave has extensive experience designing and configuring secure virtualized infrastructures. He previously worked as chief security officer for Configuresoft and CTO for the Center for Internet Security. Dave currently helps lead the Atlanta chapter of the Cloud Security Alliance.

SANS would like to thank this paper’s sponsor:

aws marketplace