corelight

WHITE PAPER

How Corelight compares to cloud native options in AWS

INTRODUCTION

As organizations increasingly move critical infrastructure and workloads to the public cloud, monitoring network traffic and activity within the cloud platform is essential for security and compliance. AWS services such as VPC flow logs, GuardDuty, Inspector and Cloudwatch are a few services that provide some protection for your cloud environments. This paper compares these AWS services to Corelight's Open Network Detection and Response (NDR) Platform offerings to help organizations determine the best options for their security and compliance needs.

GUARDDUTY VS CORELIGHT

Amazon's GuardDuty Service has an extensive catalog of detections and alerts that span many AWS offerings. GuardDuty analyzes attributes from VPC flow logs, AWS CloudTrail event logs, and DNS logs and other services to detect threats like EC2 instances mining cryptocurrency, EC2 instances compromised to scan other hosts, or EC2 instances launching DDoS attacks. Each alert has several attributes such as severity rating, alert category and remediation steps to help security personnel determine next actions. An example from their catalog is found here:

Backdoor:EC2/C&CActivity.B

An EC2 instance is querying an IP that is associated with a known command and control server.

Default severity: High

- **Data source:** VPC flow logs

This finding informs you that the listed instance within your AWS environment is querying an IP associated with a known command and control (C&C) server. The listed instance might be compromised. Command and control servers are computers that issue commands to members of a botnet.

A botnet is a collection of internet-connected devices which might include PCs, servers, mobile devices, and Internet of Things devices, that are infected and controlled by a common type of malware. Botnets are often used to distribute malware and gather misappropriated information, such as credit card numbers. Depending on the purpose and structure of the botnet, the C&C server might also issue commands to begin a distributed denial of service (DDoS) attack.

Note

If the IP queried is log4j-related, then fields of the associated finding will include the following values:

- service.additionalInfo.threatListName = Amazon
- service.additionalInfo.threatName = Log4j Related

Remediation recommendations:

If this activity is unexpected, your instance may be compromised. For more information, see Remediating a compromised Amazon EC2 instance.

By contrast, Corelight's Zeek®-based Open NDR Platform utilizes a large set of custom and open source detection content combined with Suricata's® signature based alerting capabilities to provide a full suite of evidence based security data across the entire attack surface. This rich security data allows users the ability to triage, investigate and remediate security alerts across their compute resources utilizing an external SIEM or Corelight Investigator through a consistent framework, structure and language across ALL environments, providing broader coverage for an increasing attack surface.

Corelight detections can help bolster your security posture by monitoring your network for many of the attacks found on the MITRE ATT&CK® framework. If you'd like to learn more about the coverage that Corelight can provide, please explore here.

Corelight excels at spotting C2, Discovery, and more:

INITIAL ACCESS	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	C2
Drive-by Compromise	Exploitation for Defense Evasion	Brute Force	Account Discovery	Exploitation of Remote Services	Application Layer Protocol
Exploit Public-Facing Application	Hijack Execution Flow	Credentials from Password Stores	Domain Trust Discovery	Lateral Tool Transfer	Data Encoding
External Remote Services	Indicator Removal on Host	Forced Authentication	File and Directory Discovery	Remote Service Session Hijacking	Dynamic Resolution
Phishing	Masquerading	Man-in-the-Middle	Network Service Scanning	Remote Services	Encrypted Channel
Valid Accounts	Modify Authentication Process	Modify Authentication Processes	Network Share Discovery		Fallback Channels
	Modify Registry	OS Credential Dumping	Password Policy Discovery		Ingress Tool Transfer
	Process Injection	Steal or Forge Kerberos Tickets	Permission Groups Discovery		Non-Application Layer Protocol
	Rogue Domain Controller		Remote System Discovery		Non-Standard Port
	Subvert Trust Controls		System Information Discovery		Protocol Tunneling
	Valid Accounts		System Location Discovery		Proxy
			System Location Discovery		Web Service
			System Network Configuration Discovery		
			System Network Connections Discovery		
			System Time Discovery		

Remediating a compromised Amazon EC2 instance

Follow these recommended steps to remediate a compromised EC2 instance in your AWS environment:

1. **Isolate the impacted Amazon EC2 instance.**
   Investigate the potentially compromised instance for malware and remove any discovered malware. You may use On-demand malware scan to identify malware in the potentially compromised EC2 instance, or check AWS Marketplace to see if there are helpful partner products to identify and remove malware.
2. **Identify the source of the suspicious activity**
   If malware is detected, then based on the finding type in your account, identify and stop the potentially unauthorized activity on your EC2 instance. This may require actions such as closing any open ports, changing access policies, and upgrading applications to correct vulnerabilities.
   If you are unable to identify and stop unauthorized activity on your EC2 instance, we recommend that you terminate the compromised EC2 instance and replace it with a new instance as needed. The following are additional resources for securing your EC2 instances:
   - Security and Networking sections in Best practices for Amazon EC2
   - Amazon EC2 security groups for Linux instances and Amazon EC2 security groups for Windows instances
   - Security in Amazon EC2
   - Tips for securing your EC2 instances (Linux).
   - AWS security best practices
   - Infrastructure Domain Incidents on AWS
3. **Browse AWS re:Post**
   Browse AWS re:Post at https://forums.aws.amazon.com/index.jspa for further assistance.
4. **Submit a technical support request**
   If you are a premium support package subscriber, you can submit a technical support request.

GuardDuty offers two C2 specific detections which can be complemented by Corelight's extensive C2 detections. By inspecting specific TTP's used in C2 attacks, Corelight is able to provide better detection that is much harder to evade. Details of Corelight' s fifteen C2 detections can be found here. Examples of how to best utilize the data that Corelight provides can be found by clicking any of the fifteen detections.

Comparing the GuardDuty approach to the Corelight approach for detection of C2 demonstrates the power of Corelight's evidence and enrichment for protecting your network layer. Read this white paper to learn how Corelight detects C2 activity. It explains how to use the data provided to identify the compromised host and suspicious traffic, further understand how the host was compromised, and the potential blast radius of the attack.

CORELIGHT DATA VS AWS VPC FLOW LOGS

VPC flow logs allow you to capture network flow data for your VPC network interfaces and subnets. Flow log data can be used for basic security analysis, resource monitoring, and troubleshooting. For example, you can view logs to check for unauthorized traffic or suspicious IP addresses communicating with your instances. VPC flow logs can be enabled on individual network interfaces or subnets within a VPC. Logs are captured continuously and stored in CloudWatch logs or AWS S3. Flow log examples can be found here.

It is important to note that a log entry is created based upon a predefined interval and is not necessarily based upon a single network connection, creating some randomness and opacity. In other words, there may be dozens of flow log entries for a single connection between two hosts, this leads to the most pain point of feedback for VPC flow logs; they are very noisy. This high volume of logging in turn leads to massive amounts of data to parse, process and analyze. It can begin to feel like searching for a needle in a stack of needles in very large deployments, especially if multiple public or private cloud infrastructures are also used. Integration with other AWS services downstream can help manage the volume associated with VPC flow logs, such as Kinesis Firehose and Cloudwatch.


```
{
"_path": "conn",
"_system_name": "ip-172-31-48-245",
"_write_ts": "2022-06-10T14:50:59.341312Z",
"conn_state": "SF",
"duration": 0.009794950485229492,
"history": "ShADadFf",
"id.orig_h": "172.31.13.108",
"id.orig_p": 54970,
"id.resp_h": "172.31.48.4",
"id.resp_p": 1389,
"local_orig": true,
"local_resp": true,
"missed_bytes": 0,
"orig_bytes": 119,
"orig_inst.az": "us-east-2a",
"orig_inst.id": "i-091ec202e11ee9ef1",
"orig_inst.name": "webserver_apache",
"orig_inst.org_id": "084241037008",
"orig_inst.subnet_id": "subnet-00094b9af4b73f36d",
"orig_inst.vpc_id": "vpc-0acc38aed02b39559",
"orig_ip_bytes": 647,
"orig_pkts": 10,
"proto": "tcp",
"resp_bytes": 173,
"resp_inst.az": "us-east-2c",
"resp_inst.id": "i-0c3693a15bfb332ad",
"resp_inst.name": "ldap",
"resp_inst.org_id": "084241037008",
"resp_inst.subnet_id": "subnet-0c7a925e2fbf33bbd",
"resp_inst.vpc_id": "vpc-0acc38aed02b39559",
"resp_ip_bytes": 597,
"resp_pkts": 8,
"ts": "2022-06-10T14:50:54.331413Z",
"tunnel_parents": [
  "C1m3r94ETh8S3Ha7w7"
],
"uid": "CeK8V71nThRcgOdVEk"
}
```


In contrast, using Corelight's evidence based logs, users are provided connection and flow oriented log data with multilog linking through unique_ ID values. This allows security users to quickly find network and detection data, efficiently linking it to hundreds of other network attributes captured by Corelight Sensors.

Full detail of Corelight logs can be found in this detailed document. It should be easy to see that the network log data provided by Corelight goes way beyond the limited data provided by the VPC flow logs.

Corelight understands that cloud customers often ingest network data from multiple VPCs and AWS accounts. Because of the potential use of shared RFC 1918 address spaces across these various networks, using the IP address alone is not enough to identify a resource within network data. This coupled with the potential ephemeral nature of IP allocation to a resource, it may be difficult to quickly pinpoint an asset by IP alone.

To help address this problem, Corelight has developed an AWS enrichment capability within our cloud sensors. This capability enriches the conn.log with cloud native data to quickly attribute the data to a specific AWS resource, VPC, subnet and account. The above example shows the pertinent cloud native information (in green) that a user would need to narrow down exactly which endpoints are associated with a network traffic event. This data also allows for quick pivoting of AWS GuardDuty events into the logs and vice versa. This blog explains the capability in more detail.

CONCLUSIONS

Cloud native tools can be a great starting point in network-based security; however, when time and visibility are key to detecting and preventing attacks, you want the best network evidence in your corner. Corelight's suite of content and sensors provide a much deeper understanding of what is really going on with your cloud network, providing actionable evidence-based insights for analysts.

A high-level guide to the comprehensive coverage Corelight provides mapped to the MITRE ATT&CK framework can be found here. Details for each detection and how Corelight discovers them can be found in this interactive website, that details the detection and the data Corelight provides for each detection, as well as the logs where you can find the correlating data.

One of Corelight's strengths is how it allows users to fully understand alerts by providing the evidence necessary to investigate and determine the cause of the alerts. A great perspective on the value of our data can be found in this white paper.

Corelight continually adapts to the expanding attack surface adversaries leverage to gain unauthorized access and conduct their malicious operations. As networks transition to the cloud, monitoring network activity for suspicious behavior becomes even more critical for defense. Focusing on the network-based tactics, techniques, and procedures attackers must use to execute their mission remains the fundamental way to detect—and stop—them before the fully execute their plans.

Reach out to us to learn more.

Request a demo of the Open NDR Platform at **https://corelight.com/contact**

Corelight provides security teams with network evidence so they can protect the world's most critical organizations and companies. On-prem and in the cloud, our Open Network Detection and Response Platform enhances visibility and analytics, leading to faster investigations and expanded threat hunting. Corelight's global customers include Fortune 500 companies, major government agencies, and large research universities. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek®, the widely-used network security technology.

info@corelight.com | 888-547-9497