# AWS Security Series

## Part 8
## AWS Security: Threat Intelligence for the Cloud

Nitin Sharma
CyberSecurity and DevSecOps Engineer
LinkedIn: linkedin.com/in/nitins87
Quora: quora.com/profile/NitinS-1
Blog: 4hathacker.in

# Contents

$ whoami

$ Cloud Threat: GROUND REALITY VS. #MYTHS

$ Cyber Threat Intelligence and Risk

$ Data vs Information vs Risk

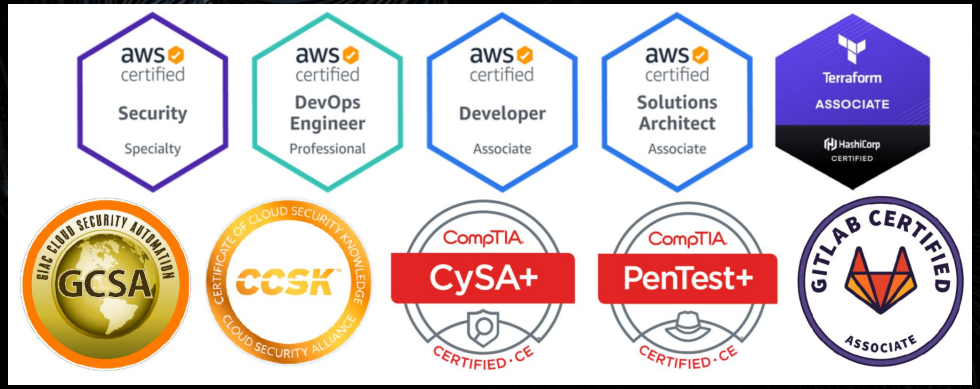
$ Types/Levels of Threat Intelligence

$ Cloud Threat Landscape with Example

$ Amazon GuardDuty: Threat Intel with Cloud Fabric

# $ whoami

- Cybersecurity and DevSecOps professional experienced in Cloud Security, Container Security and DevOps Research
- Certifications:

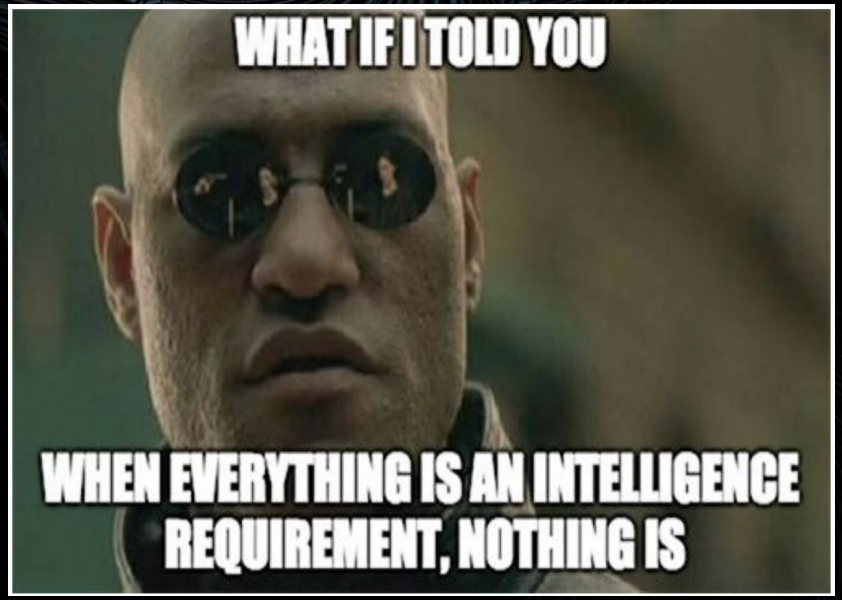




- Published author for "Securing Docker - The Attack & Defense Ways" book under CyberSecrets Publication
- Half Marathon runner, Cyclist and Fitness Enthusiast
- Helping out beginners in Cloud, DevOps and CyberSec at Quora

# $ Cloud Threats - Reality vs. Myth

"REALITY"




"MYTH"

# $ Cyber Threat Intelligence and Risk

- According to NIST, **Cyber Threat** can be defined as,

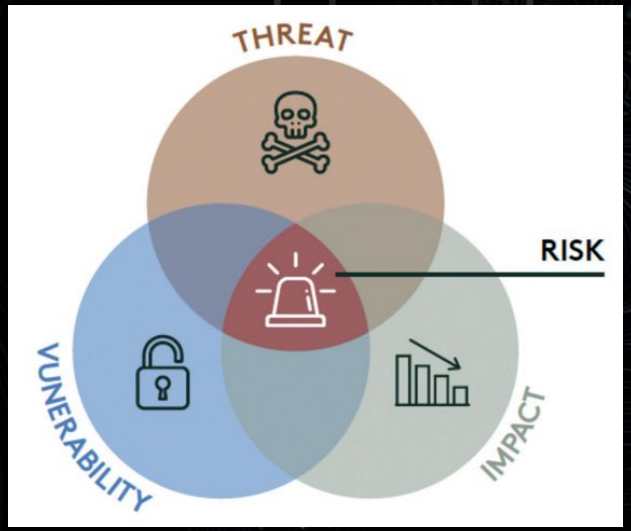
"Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service."

- According to CIA,

"**Intelligence** is knowledge and foreknowledge of the world around us - the prelude to decision and action…"

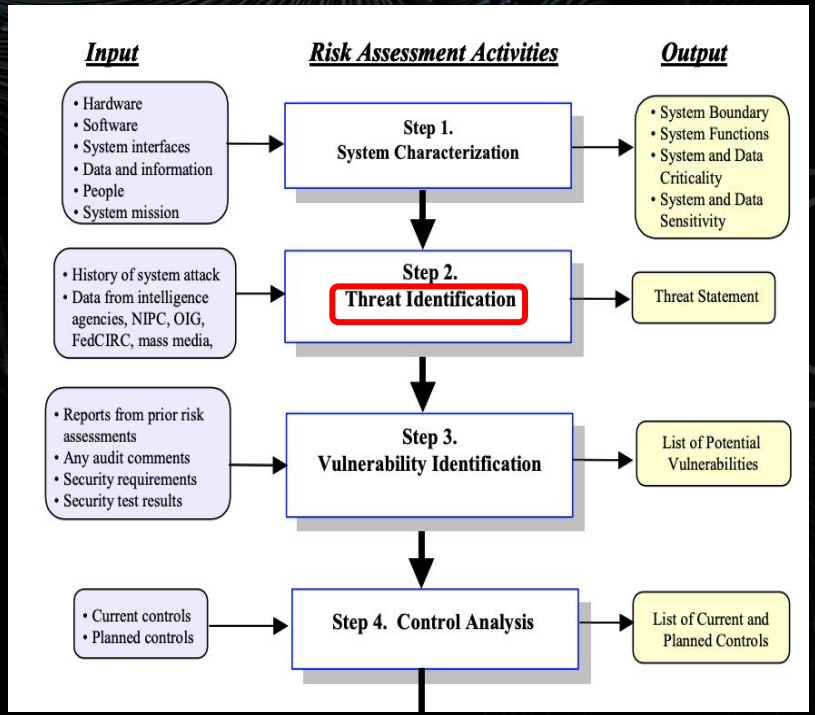
# $ Cyber Threat Intelligence and Risk

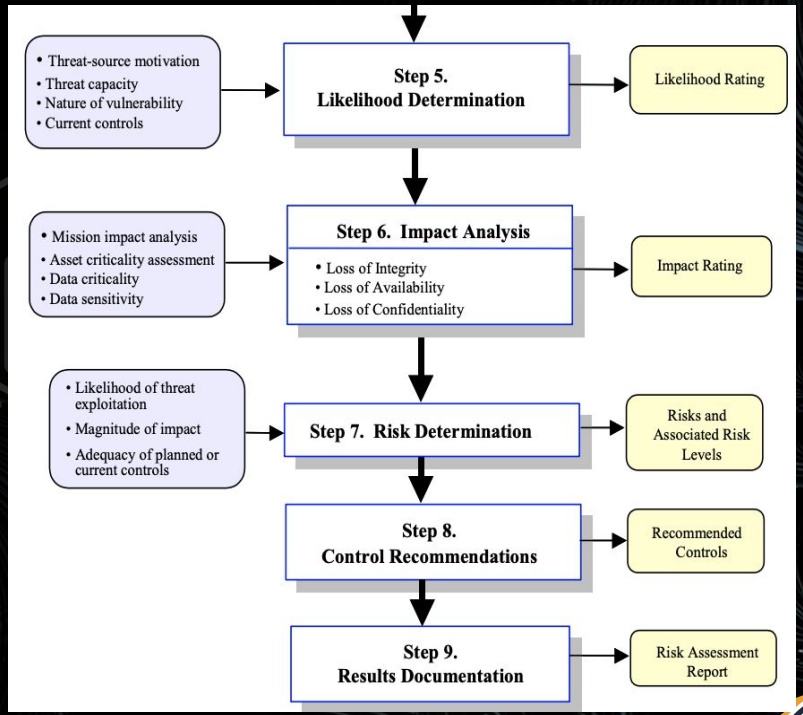
"When an organisation knows how to answer key questions regarding the threats it faces - such as **who** is likely to target **what** assets, **where**, **when**, **how** and **why** then they stand a much better chance of defending themselves."




(Source: CREST Cyber Threat Intelligence)

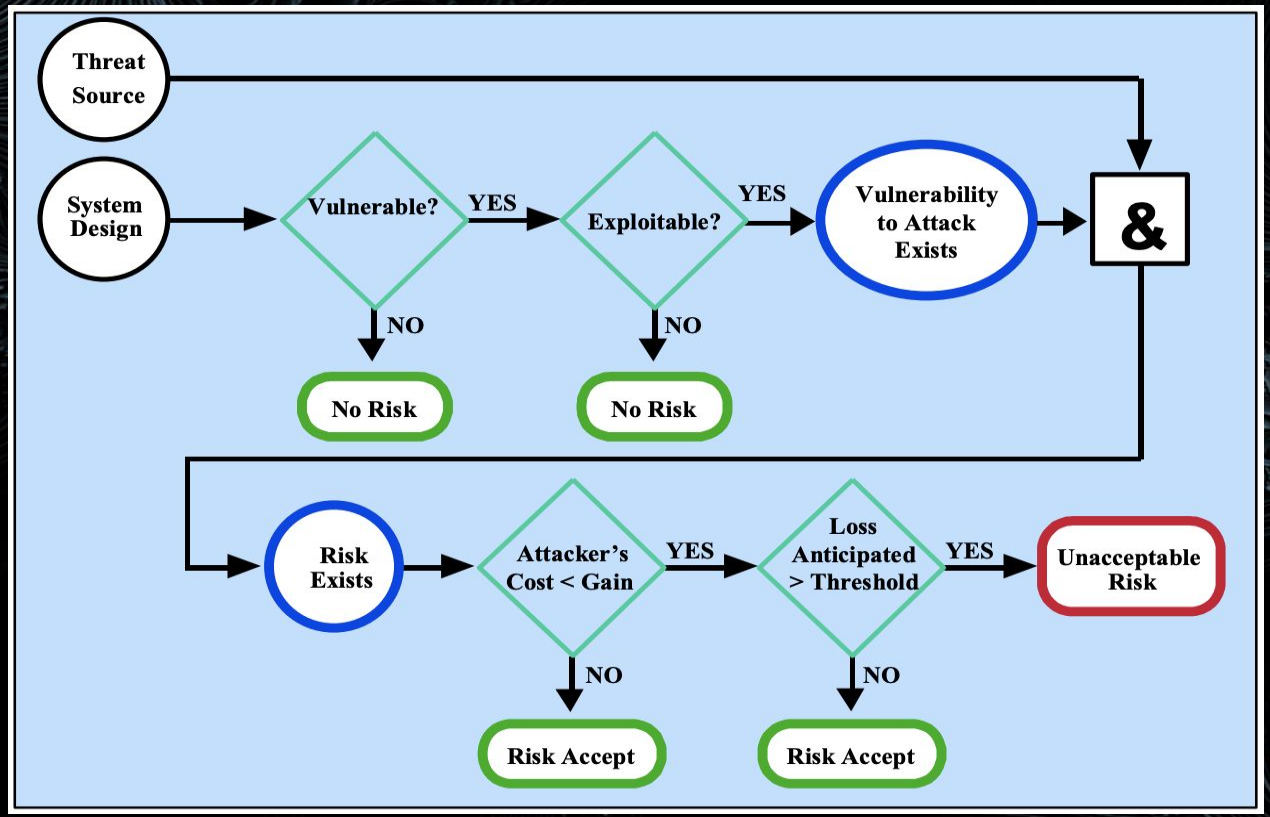
# $ Threat in Risk Assessment Methodology




(Source: NIST SP 800-30)

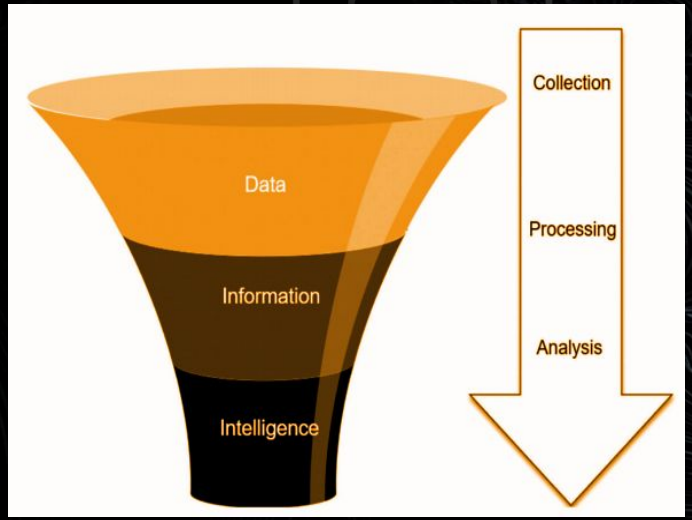
# $ Threat in Risk Mitigation Action Points




(Source: NIST SP 800-30)

# $ Data vs Information vs Intelligence

**Data**: simple facts available in large volumes. Eg. logs
**Information**: useful output from collated data. Eg. logs showing spike in suspicious activity.
**Intelligence**: processing and analysis of information that helps in decision making.



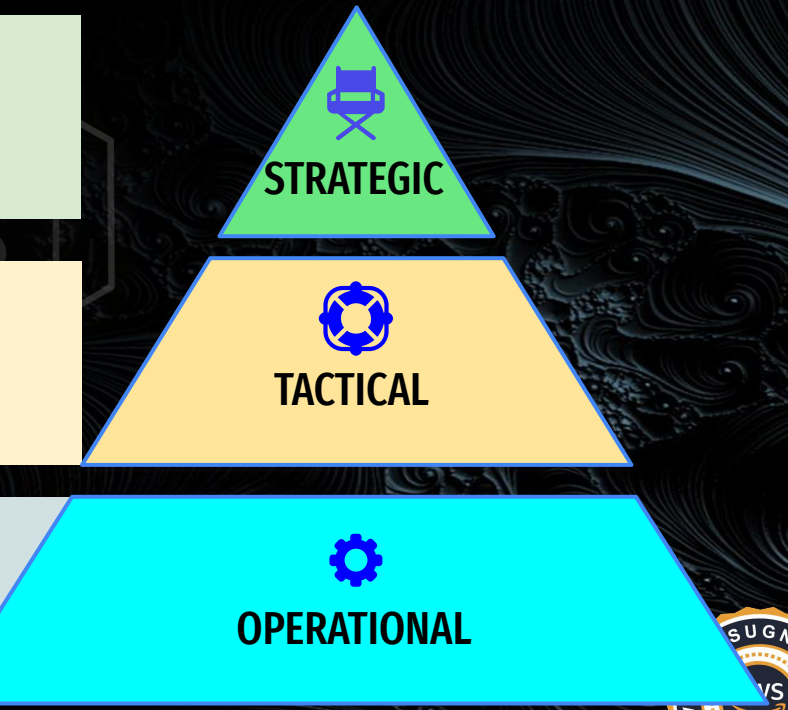

(Source: CREST Cyber Threat Intelligence)

# $ Types/Levels of Threat Intelligence

**Plain Language, business risk focused,less frequent, for senior decision makers only.**
***STAKEHOLDERS: C-Suite & Mgmt.***

**For signature based and proactive systems, combination of human and machine readable formats.**
***STAKEHOLDERS: DFIR & Threat Hunter team***

**Large volume, impending attacks, machine and human-readable, for network defenders.**
***STAKEHOLDERS: SOC Analyst, SIEM, IDS/IPS, F/W, etc.***



# $ Cloud Threat Landscape

The Notorious Nine

1. Data Breach


2. Data Loss


3. Account Hijacking


4. Insecure APIs


5. DoS Attack


6. Insider Threat

7. Cloud Abuse

8. Insufficient Due Diligence


9. Shared Technology Issues

# $ Cloud Threat Landscape

The Egregious Eleven (More Recent and Cloud Specific)

- EE1: Data Breaches
- EE2: Misconfiguration & Inadequate Change Control
- EE3: Lack of Cloud Security Architecture and Strategy
- EE4: Insufficient Identity, Credential, Access and Key Management
- EE5: Account Hijacking
- EE6: Insider Threat
- EE7: Insecure APIs
- EE8: Weak Control Plane
- EE9: Metastructure and Applistructure Failures
- EE10: Limited Cloud Usage Visibility
- EE11: Abuse and Nefarious Use of Cloud Services

# $ Cloud Security and Threat Scenario

## Imperva

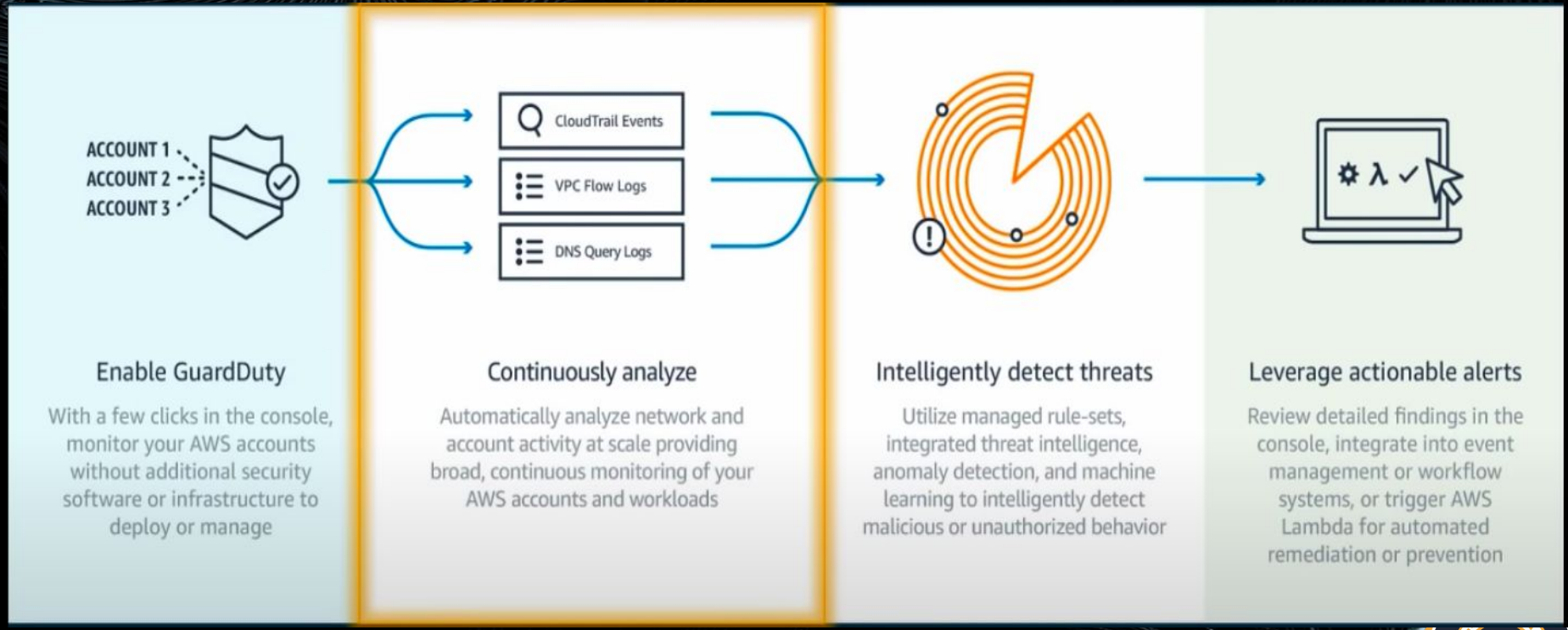
| Threat actor | Threat | Vulnerabilities | Technical impacts | Business Impacts |
|---|---|---|---|---|
| **Internal**<br>Design and Human error by an internal cloud team. | **EE1**<br>*Data Breach:*<br>Compromise of AWS server instance and AWS access key in production AWS, which led to an exposure of a database snapshot containing sensitive data. | **EE2**<br>*Misconfiguration and Inadequate Change Control* -<br>A server with access to sensitive database snapshots was configured to be internet accessible. | **EE1**<br>*Data Breach:*<br>Subset of Incapsula customers' email addresses, passwords, API keys and certificates were disclosed. | **Financial**<br>- No data available |
| | | *Undisclosed Server Vulnerability* -<br>The attacker was able to pivot from an internet facing cloud server, meaning he was able to compromise it via some undisclosed vulnerability or gross misconfiguration. | *Cloud Instance Compromised:*<br>An attacker was able to compromise an AWS EC2. | **Operational**<br>-Marketing, Security & Operations teams incident response efforts<br>-Re-issuing and rerolling tens of thousands of customer certificates, passwords and API keys |
| **External**<br>- Unknown threat actor<br>- Undisclosed bug bounty hunter | *Cloud Server and Credentials Compromise:*<br>An attacker was able to compromise an AWS EC2 service instance and abuse credentials that he found on that server. | **EE3**<br>*Lack of Cloud Security Architecture and Strategy* -<br>A server with access to production database snapshot was used for testing. It was internet facing and used AWS API keys rather than roles (temporary credentials). | *Cloud Access Key Credentials Compromised.* | **Compliance**<br>-GDPR driven breach notifications issued. |
| | | | | **Reputational**<br>N/A |

(Source: Top Threats to Cloud Computing: Egregious Eleven Deep Dive)

**Actor**: External unknown threat actor and undisclosed bug bounty hunter.

**Attack**: Compromise of an Imperva cloud server led to unauth(Z) use of an admin API key in one of the prod(n) AWS accounts in Oct. 2018, which led to an exposure of a DB Snapshot containing emails and hashed/salted passwords.

# $ Amazon GuardDuty: Introduction



# $ Amazon GuardDuty:Features

## GuardDuty Data Sources

### VPC Flow Logs

VPC flow logs

- Flow Logs for VPCs Do Not Need to Be Turned On to Generate Findings, data is consumed through independent duplicate stream.
- Suggested Turning On VPC Flow Logs to Augment Data Analysis (charges apply).

### DNS Logs

DNS Logs

- DNS Logs are based on queries made from EC2 instances to known questionable domains.
- DNS Logs are in addition to Route 53 query logs. Route 53 is not required for GuardDuty to generate DNS based findings.

### CloudTrail Events

CloudTrail Events

- CloudTrail history of AWS API calls used to access the Management Console, SDKs , CLI, etc. presented by GuardDuty.
- Identification of user and account activity including source IP address used to make the calls.

# $ Amazon GuardDuty:Features

## GuardDuty Findings: Threat Purpose Details

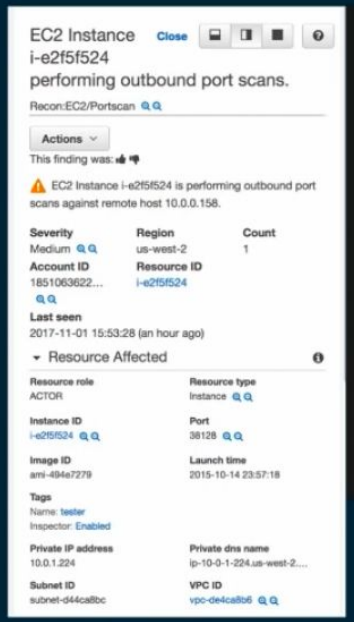
Describes the primary purpose of the threat. Available at launch, more coming!

- **Backdoor:** resource compromised and capable of contacting source home
- **Behavior:** activity that differs from established baseline
- **Crypto Currency:** detected software associated with Crypto currencies
- **Pentest:** activity detected similar to that generated by known pen testing tools
- **Recon:** attack scoping vulnerabilities by probing ports, listening, database tables, etc
- **Stealth:** attack trying to hide actions / tracks
- **Trojan:** program detected carrying out suspicious activity
- **Unauthorized Access:** suspicious activity / pattern by unauthorized user

# $ Amazon GuardDuty:Features

## GuardDuty Findings: Console / API

### AWS Management Console




Quickly See Threat Information Including:

- Severity
- Region
- Count/Frequency
- Threat Type
- Affected Resource
- Source Information
- Viewable via CloudWatch Events

### API / JSON Format


Export Finding Data for Further Analysis Including:

- Ingest into SIEM
- Data Enrichment
- Programmatic Response
- Additional Information
  - ARN
  - Span of Time
  - Resource Info

# $ Amazon GuardDuty: Features

## GuardDuty Findings: Severity Levels

### LOW

Suspicious or malicious activity blocked before it compromised a resource.

Suggestion:

Take Immediate Action(s)
- No immediate recommended steps – but take note of info as something to address in the future

### MEDIUM

Suspicious activity deviating from normally observed behavior.

Suggestion:

Investigate Further
- Check new software that changed the behavior of a resource
- Check changes to settings
- AV scan on resource (detect unauthorized software)
- Examine permissions attached to IAM entity implicated

### HIGH

Resource compromised and actively being used for unauthorized purpose.

Suggestion:

Take Immediate Action(s)
- Terminate instance(s)
- Rotate IAM access keys

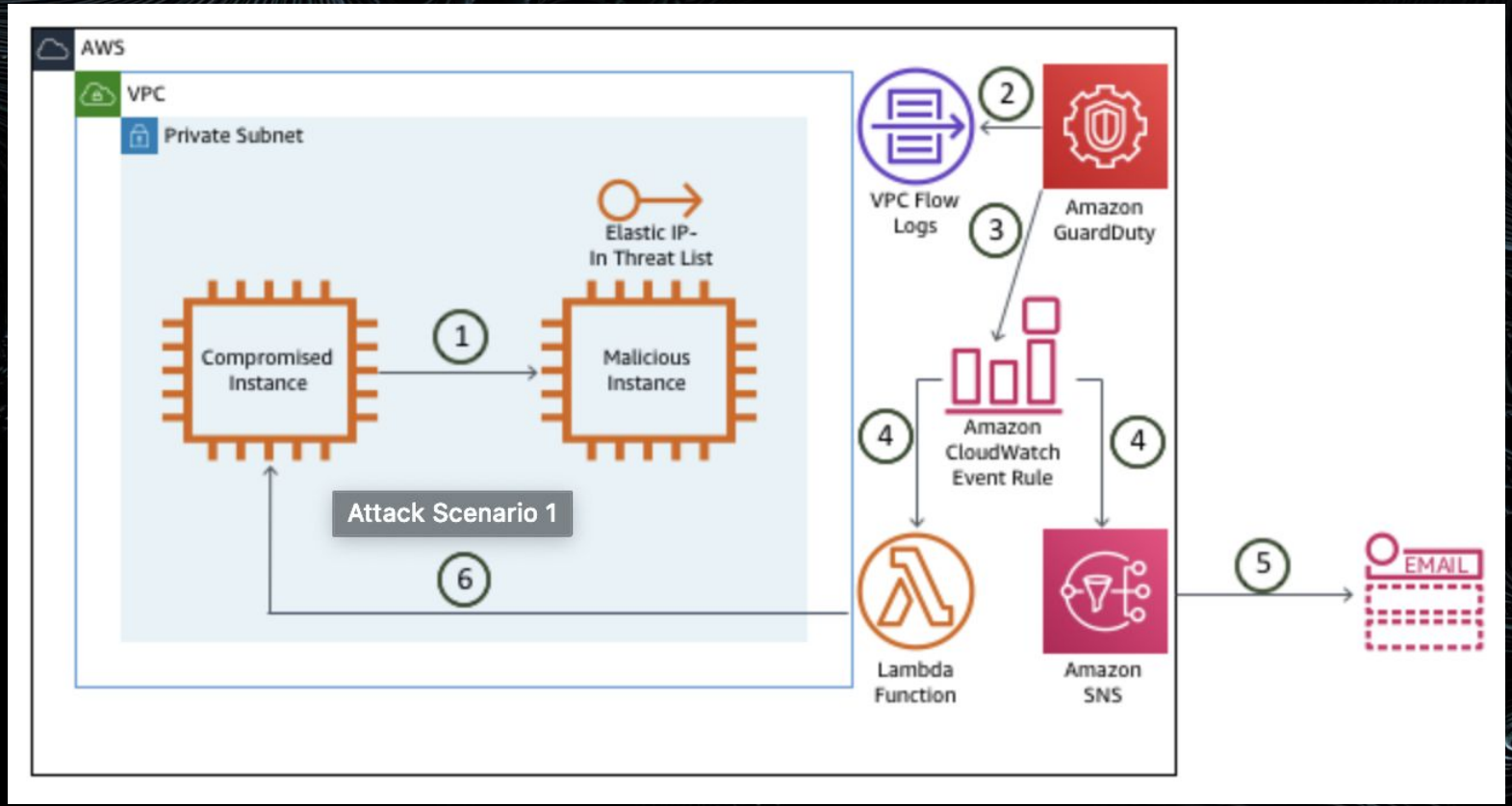
# $ Amazon GuardDuty: Features

## Responding to Findings: Remediation

- Remediate a Compromised Instance
- Remediate Compromised AWS Credentials

### Automatic Remediation


# $ Amazon GuardDuty:Demo



# $ Amazon GuardDuty:Demo

- The compromise instance pings the EIP of the malicious instance. That EIP is in a custom Threat List.
- GuardDuty is monitoring VPC Flow Logs across this threat list.
- GuardDuty generates a finding and sends this to the GuardDuty console and CloudWatch Events.
- The CloudWatch event rule triggers an SNS topic and a Lambda function.
- SNS sends you an email with the finding information.
- A Lambda Function isolates the compromised instance.



# Thank You...

**For queries feel free to connect with AWS Delhi User Group at:**

**AWS Delhi User Group (MeetUp) - Learn Together, Grow Together**

**AWS User Group Delhi NCR (Follow us on LinkedIn Page)**