Detecting & Mitigating Ransomware Threats in AWS Architecture Using AWS Services.

(Major-Project)

A project report submitted to the Srinivas University as partial fulfilment for the award of the degree of

Bachelor of Technology in Cloud Technology and Information Security

Submitted By

Delvy Austin Fernnandes

USN: 1SU19CI010

Under the Guidance of

Dr. A. Sasi Kumar

Assistant Professor

Dept. of CTDS

SUIET

Department of Cloud Technology & Data Science

College of Engineering and Technology

SRINIVAS UNIVERSITY

Mukka, Mangalore – 574146

January 2022

BONAFIDE CERTIFICATE

This is to certify that this project report entitled "**Detecting & Mitigating Ransomware Threats in AWS Architecture Using AWS Services**" is submitted to Srinivas University College of Engineering and Technology, Mukka, is a Bonafide record of work done by **Delvy Austin Fernandes** under my supervision.

Dr. A. Sasi Kumar
Assistant Professor
Dept. of CTDS
SUIET

Prof. Daniel Selvaraj
Head of Department
Department of Cloud Technology and Data Science
Srinivas University, Mukka

Date:
Place: Mukka

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND NOMENCLATURE

ABSTRACT

1. Title of the Project – Student Name, USN Number, University Name, institution Name, Department, Class, Semester, Batch, Supervisor Name
2. Agenda
3. Abstract
4. Introduction
   - 4.1 The Domain
   - 4.2 Problem Statement
   - 4.3 The Technology
     - (i) Hardware Requirements
     - (ii) Software Requirements
     - (iii) Operating System
   - 4.4 Objectives of the Project
5. Literature Survey / Related Works
   - 5.1 Literature Review
   - 5.2 Existing Systems
   - 5.3 Proposed System-Planning
   - 5.4 Motivation to implement
6. System Design Methodology
   - 6.1 System Architecture Diagram
   - 6.2 Description of work
   - 6.3 Algorithms implemented (if any)
7. Implementation / Results (Optional)
   - 7.1 Experimental Setup
   - 7.2 Comparative study
   - 7.3 Proposed Results
8. Conclusion
9. Future Enhancements (Optional)
10. References

1. Title

Detecting & Mitigating Ransomware Threats in AWS Architecture Using AWS Services.

2. Agenda

In this project we will do three things:

Protect:

Use AWS Systems Manager to update and configure our EC2 instances – to mitigate system vulnerabilities.

Detect:

Use Guard Duty, Security Hub, and Systems Manager to detect malicious behaviour by an EC2 instance and investigate it further for the presence of ransomware.

Respond:

Use Systems Manager automation to gather data from an affected system, snapshot it, and isolate it. This enables the incident response team to do further investigation and forensic work.

3. Abstract

Protect, Detect and Respond Threat detection can continuously monitor our AWS accounts and workloads for malicious activity and deliver detailed security findings for visibility and remediation. Early detection of abnormal network activity is key to mitigating ransomware threats and their impact.

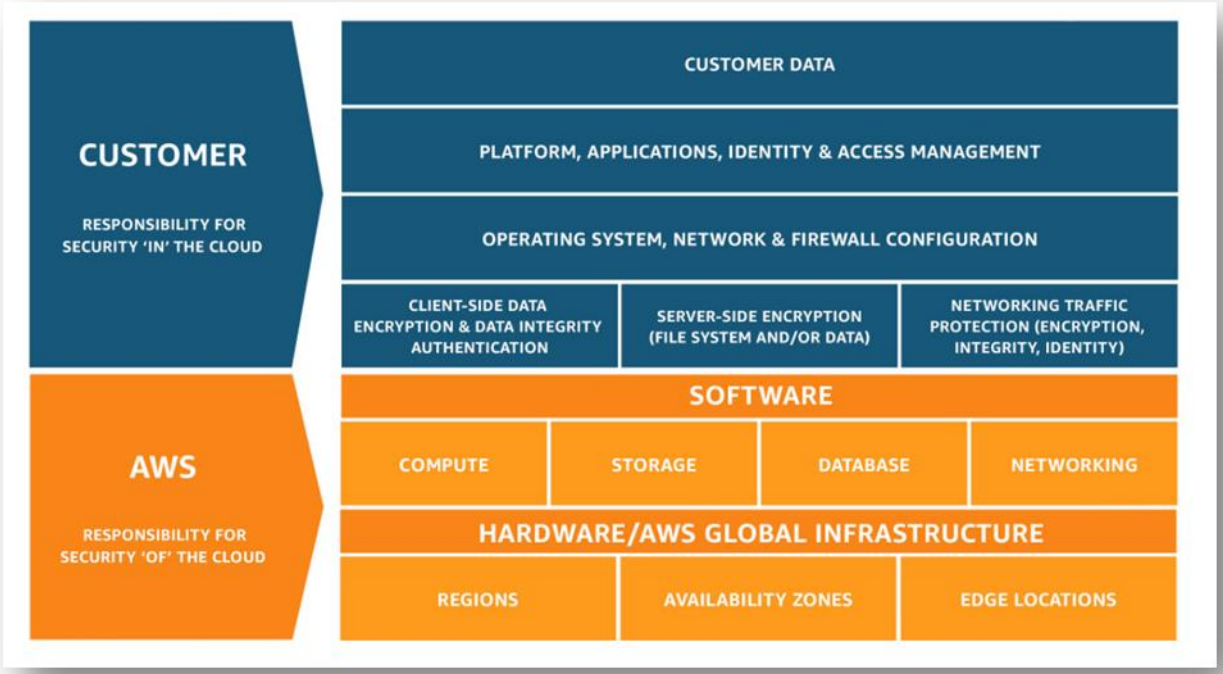
4. Introduction

Criminal organizations use sophisticated methods to compromise their victims' systems and encrypt the data, usually with the goal of extorting money from the victim. An AWS customer benefits from

AWS data centres and network infrastructure, which are architected to protect information, identities, and applications.

4.1 The Domain

Concept of shared responsibility model in AWS:



4.2 Problem Statement

The Vulnerability Aspect:

Running in AWS alone, however, is not enough to protect the systems from ransomware or other cybersecurity threats. User retains the responsibility for securing the aspects of the environment one controls it. (Concept of AWS Shared Responsibility Model) AWS provides users with a robust set of tools to keep their environment secure at scale. In this project we will

explore how some of these tools can enhance our ability to protect against ransomware, detect malicious activity, and respond to malicious activity if it is detected.

According to Gartner, by 2025, ransomware attacks are expected to increase by 700% and at least 75% of IT organizations will face one or more attacks.

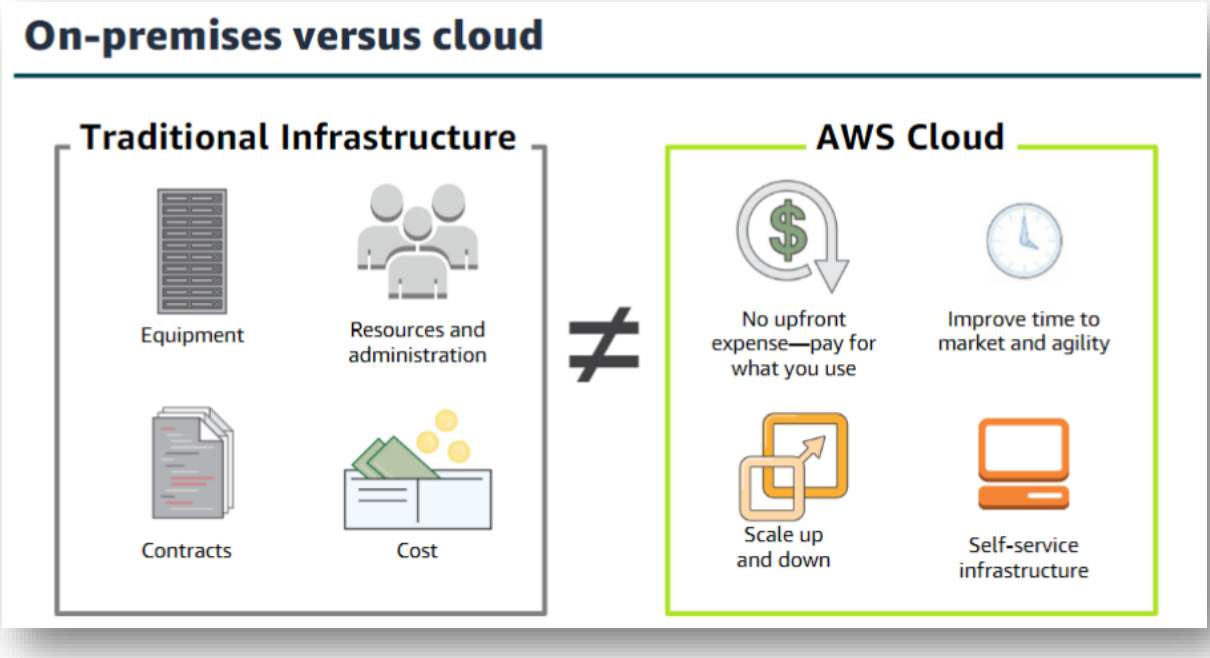
- Gartner, January 2021.

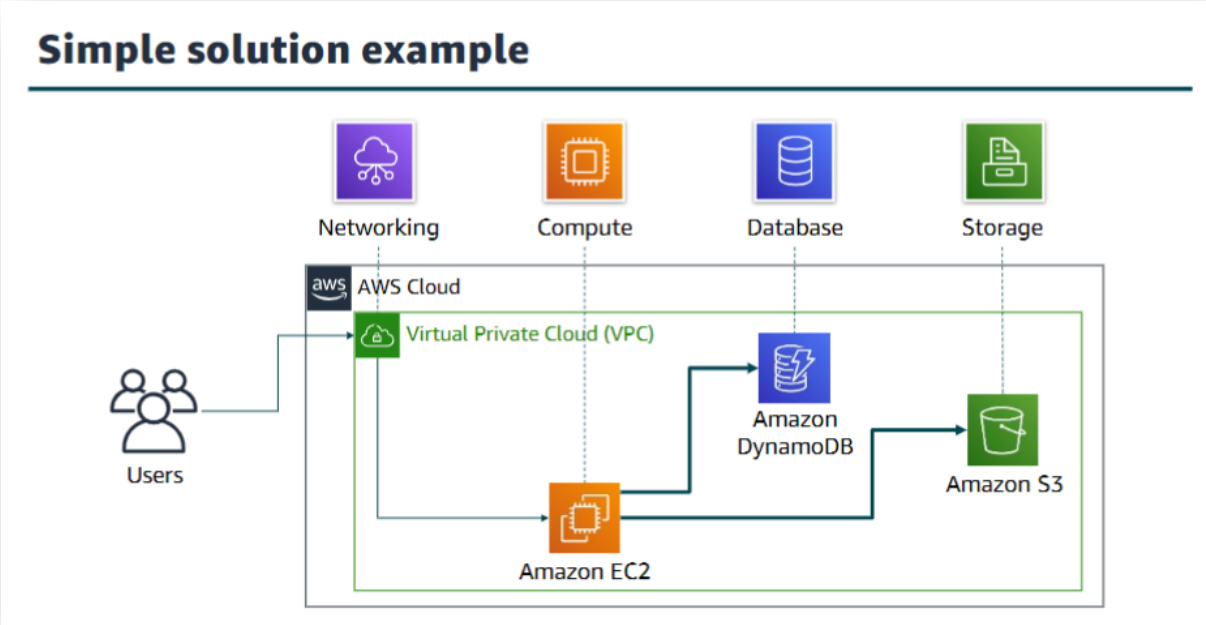
S3 buckets are advertised by AWS as extremely durable. Recent Ermetic research found that misconfigurations of S3 buckets and access-related factors made exposure to potential ransomware in the real-world sample studied extremely common. This potential risk calls for organizations to take urgent action to correct any such S3 bucket misconfigurations and access-related factors.

- Ermetic research

https://n2ws.com/blog/aws-disaster-recovery/how-to-laugh-at-ransomware-cyber-criminals-with-aws-backup

4.3 The Technology





Cloud security at AWS is the highest priority. AWS has technology that helps customers protect and recover their systems from ransomware attacks, including services and features that provide infrastructure and data backups, the AWS-Well Architected Tool, and strong security controls using AWS security services.

AWS Systems Manager

It's useful in gaining operational insights into AWS and on-premises resources. AWS Systems Manager is a secure end-to-end management solution for hybrid cloud environments.

AWS CloudTrail

AWS CloudTrail logs all API calls.

Amazon Server-Side Encryption with Amazon Simple Storage Service (Amazon S3) managed encryption keys (SSE-S3) can digitally sign and encrypt the logs and store them in a secure Amazon S3 bucket.

Amazon Virtual Private Cloud (VPC) Flow Logs monitor all network activity going in and out of your VPC.

Amazon CloudWatch monitors your AWS environment and generates alerts.

Amazon Guard Duty correlates activity in your AWS environment with threat intelligence from multiple sources that provide additional risk context and anomaly detection.

Amazon Macie can identify sensitive data, classify, and label it, and track its location and access.

AWS Services to be Used

AWS Security Hub:

It automates response and remediation. AWS Security Hub is a cloud security posture management service that performs security best practice checks, aggregates alerts, and enables automated remediation.

AWS Systems Manager:

centralizes operational data from multiple AWS services and automates tasks across your AWS resources. You can create logical groups of resources such as applications, different layers of an application stack, or production versus development environments. It gains operational insights into AWS and on-premises resources. AWS Systems Manager is a secure end-to-end management solution for hybrid cloud environments.

AWS CloudTrail:

It logs all API calls. AWS CloudTrail monitors and records account activity across AWS infrastructure, giving you control over storage, analysis, and remediation actions.

Amazon Server-Side Encryption with Amazon Simple Storage Service (Amazon S3) managed encryption keys (SSE-S3) can digitally sign and encrypt the logs and store them in a secure Amazon S3 bucket.

Amazon Virtual Private Cloud:

Amazon VPC flow Logs monitor all network activity going in and out of VPC. Amazon VPC gives full control over our virtual networking environment, including resource placement, connectivity, and security.

Amazon CloudWatch:

It monitors your AWS environment and generates alerts. Amazon CloudWatch it Observes and monitors resources and applications on AWS, on-premises, and on other clouds. Amazon CloudWatch collects and visualizes real-time logs, metrics, and event data in automated dashboards to streamline our infrastructure and application maintenance.

Amazon GuardDuty:

It correlates activity in AWS environment with threat intelligence from multiple sources that provide additional risk context and anomaly detection.

Amazon Macie:

It can identify sensitive data, classify, and label it, and track its location and access.

(i) Hardware Requirements

(ii) Software Requirements (Front End & Back End Tools)

(iii) Operating System

4.4 Objectives of the Project

5. Literature Survey / Related Works

Security and compliance resources

- **Security and compliance resources AWS Security Reference Architecture (AWS SRA)**
- **The European Union Agency for Cybersecurity (ENISA)**
- **U.S. Cybersecurity & Infrastructure Security Agency (CISA)**

5.1 Literature Review

Ermetic Whitepaper: Misconfigurations Leading to AWS S3 Ransomware Exposure

https://l.ermetic.com/wp-aws-s3-ransomware-exposure-report

Securing your AWS Cloud environment from ransomware
https://d1.awsstatic.com/WWPS/pdf/AWSPS_ransomware_ebook_Apr-2020.pdf

Ransomware recovery AWS Elastic Disaster Recovery | Ransomware Recovery | AWS (amazon.com)

Best Practices for Security, Identity, & Compliance Security, Identity & Compliance | AWS Architecture Center (amazon.com)

AWS Security IncidentResponse Guide
https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf

Classic Intrusion Analysis Frameworks for AWS Environments: Application and Enhancement Classic Intrusion Analysis Frameworks for AWS Environments: Application and Enhancement - AWS Whitepapers (amazon.com)

Base paper

https://aws.amazon.com/blogs/apn/protect-detect-and-respond-to-ransomware-with-presidios-ransomware-mitigation-kit/

AWS White Paper Security Pillar - AWS Well-Architected Framework - Security Pillar (amazon.com)

5.2 Existing Systems

5.3 Proposed System-Planning

5.4 **Motivation for Implementation:**

Ransomware has been a prominent threat to enterprises since the late 1990s. In 2020, the FBI's IC3 (Internet Crime Complaint Centre) received 2,474 complaints identified as ransomware with adjusted losses of over $29.1 million. Those complaints, however, represent only the attacks reported to IC3. The actual number of ransomware attacks and costs are much higher.

6. System Design Methodology

6.1 System Architecture Diagram

6.2 Description of work

6.3 Algorithms implemented (if any)

7. Implementation / Results (Optional)

7.1 Experimental Setup

7.2 Comparative study

7.3 Proposed Results

8. Conclusion

9. Future Enhancements (Optional)

10. References

Format:

Author names, (Year), Title of the article, Journal name, Volume Number(Issue Number), Page Numbers.

Example Format:

Cvitic I., Perakovic, D., Perisa, M., & Gupta, B. (2021). Ensemble machine learning approach for classification of IoT devices in smart home. International Journal of Machine Learning and Cybernetics, 12(11), 3179-3202.

(B) PROJECT DOCUMENTATION (Like Project Report Format) – (Optional)

Submission Date: 07-Dec-2022

Abstract

Protect, Detect and Respond

Threat detection can continuously monitor our AWS accounts and workloads for malicious activity and deliver detailed security findings for visibility and remediation. Early detection of anomalous network activity is key to mitigating ransomware threats and their impact.

In this workshop we will do three things:

- Protect: Use AWS Systems Manager to update and configure our EC2 instances – to mitigate system vulnerabilities.
- Detect: Use Guard Duty, Security Hub, and Systems Manager to detect malicious behavior by an EC2 instance and investigate it further for the presence of ransomware.
- Respond: Use Systems Manager automation to gather data from an affected system, snapshot it, and isolate it. This enables the incident response team to do further investigation and forensic work.

Detecting Ransomware using AWS Services

Ransomware has been a prominent threat to enterprises since the late 1990's. In 2020, FBI's IC3 (Internet Crime Complaint Center) received 2,474 complaints identified as ransomware with adjusted losses of over $29.1 million. Those complaints, however, represent only the attacks reported to IC3. The actual number of ransomware attacks and costs are much higher.

Cloud security at AWS is the highest priority. AWS has technology that helps customers protect and recover their systems from ransomware attacks, including services and features that provide infrastructure and data backups, the AWS-Well Architected Tool, and strong security controls using AWS security services. In this workshop, we will learn some of the basics of how to protect, detect, and respond to ransomware using AWS Services.

There are six best practice areas for security in the cloud:

- Security
- Identity and Access Management
- Detection
- Infrastructure Protection
- Data Protection
- Incident Response

Before you architect any workload, you need to put in place practices that influence security. You will want to control who can do what. In addition, you want to be able to identify security incidents, protect your systems and services, and maintain the confidentiality and integrity of data through data protection. You should have a well-defined and practiced process for responding to security incidents. These tools and techniques are important because they support objectives such as preventing financial loss or complying with regulatory obligations.

The AWS Shared Responsibility Model enables organizations that adopt the cloud to achieve their security and compliance goals. Because AWS physically secures the infrastructure that supports our cloud services, as an AWS customer you can focus on using services to accomplish your goals. The AWS Cloud also provides greater access to security data and an automated approach to responding to security events.

There are seven design principles for security in the cloud:

- Implement a strong identity foundation: Implement the principle of least privilege and enforce separation of duties with appropriate authorization for each interaction with your AWS resources. Centralize identity management, and aim to eliminate reliance on long-term static credentials.
- Enable traceability: Monitor, alert, and audit actions and changes to your environment in real time. Integrate log and metric collection with systems to automatically investigate and take action.
- Apply security at all layers: Apply a defense in depth approach with multiple security controls. Apply to all layers (for example, edge of network, VPC, load balancing, every instance and compute service, operating system, application, and code).
- Automate security best practices: Automated software-based security mechanisms improve your ability to securely scale more rapidly and cost-effectively. Create secure architectures,

including the implementation of controls that are defined and managed as code in version-controlled templates.

- Protect data in transit and at rest: Classify your data into sensitivity levels and use mechanisms, such as encryption, tokenization, and access control where appropriate.
- Keep people away from data: Use mechanisms and tools to reduce or eliminate the need for direct access or manual processing of data. This reduces the risk of mishandling or modification and human error when handling sensitive data.
- Prepare for security events: Prepare for an incident by having incident management and investigation policy and processes that align to your organizational requirements. Run incident response simulations and use tools with automation to increase your speed for detection, investigation, and recovery.

Security and compliance resources

- AWS Security Reference Architecture (AWS SRA)

- The European Union Agency for Cybersecurity (ENISA)

- U.S. Cybersecurity & Infrastructure Security Agency (CISA)
-

Base paper

https://aws.amazon.com/blogs/apn/protect-detect-and-respond-to-ransomware-with-presidios-ransomware-mitigation-kit/

AWS White paper

Security Pillar - AWS Well-Architected Framework - Security Pillar (amazon.com)

Useful links

Securing your AWS Cloud environment from ransomware

Ransomware recovery

Best Practices for Security, Identity, & Compliance

AWS Security IncidentResponse Guide

Classic Intrusion AnalysisFrameworks for AWSEnvironments: Applicationand Enhancement

Ransomware Risk Management on AWS Using the NIST Cyber Security Framework (CSF)

AWS Services Used

AWS Systems Manager helps with systems hardening via patch management and configuration management.

AWS Systems Manager helps maintain security and compliance by scanning your instances against your patch, configuration, and custom policies.

You can define patch baselines, maintain up-to-date anti-virus definitions, and enforce firewall policies.

You can also remotely manage your servers at scale without manually logging in to each server.

Systems Manager also provides a centralized store to manage your configuration data, whether it's plain text, such as database strings, or secrets, such as passwords.

WS Systems Manager can also be helpful in an incident response scenario if your traditional server management infrastructure becomes unavailable.

AWS Systems Manager Agent (SSM Agent) is preinstalled, by default, on the following Amazon Machine Images (AMIs):

- Amazon Linux
- Amazon Linux 2
- Amazon Linux 2 ECS-Optimized Base AMIs
- macOS 10.14.x (Mojave), 10.15.x (Catalina), and 11.x (Big Sur)
- Ubuntu Server 16.04, 18.04, and 20.04
- Windows Server 2008-2012 R2 AMIs published in November 2016 or later
- Windows Server 2016 and 2019

Patching

Systems patching is the most basic component of a vulnerability management program. (Note: While we do not cover it as a part of this builder session, AWS Inspector can help you with vulnerability scanning in AWS) AWS Systems Manager gives you the ability to deploy patches to your EC2 instances and on-premises systems. You can even patch systems that are isolated from the internet or the rest of your network by creating a VPC endpoint.

Security Hub

Used to detect a misconfigured security group and integration between Security Hub and GuardDuty to detect an EC2 instance communicating with a known malicious IP address.

You may get a warning message ***AWS Config*** *is not appropriately enabled on some accounts. AWS Config is required for Security Hub's security checks. Review remediation steps for the related findings for CIS 2.5. If you recently enabled AWS Config, note that it can take up to 12 hours for Security Hub to detect the change.* Please ignore this message as there is no impact the labs

AWS Security Hub *gives you a comprehensive view of your security alerts and security posture across your AWS accounts. AWS provides a range of powerful security tools at your disposal, from firewalls and endpoint protection to vulnerability and compliance scanners. Oftentimes this leaves your team switching back-and-forth between these tools to deal with hundreds, and sometimes thousands, of security alerts every day. With Security Hub, you now have a single place that aggregates, organizes, and prioritizes your security alerts, or findings, from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access*

Analyzer, AWS Systems Manager, and AWS Firewall Manager, as well as from AWS Partner Network (APN) solutions. AWS Security Hub continuously monitors your environment using automated security checks based on the AWS best practices and industry standards that your organization follows. You can also act on these security findings by investigating them in Amazon Detective or by using Amazon CloudWatch Event rules to send the findings to ticketing, chat, Security Information and Event Management (SIEM), Security Orchestration Automation and Response (SOAR), and incident management tools or to custom remediation playbooks.

GuardDuty

GuardDuty can detect machines that communicate with known malicious IP addresses including C2C communication. GuardDuty findings can be centrally aggregated in Security Hub. In this section we will find one of our EC2 instances talking to a known malicious IP address.

CloudWatch

A sudden increase in EC2 instance's resource utilization, specifically – CPU and Disk – may indicate malicious activity on that instance. CloudWatch metrics allow you to track instance resource utilization and allows you to set alerts when anomalous activity is detected. We are going to take a look at resource utilization by WebServer1 – since that's where we saw potentially malicious communication coming from.

Using CloudWatch anomaly detection

When you enable anomaly detection for a metric, CloudWatch applies statistical and machine learning algorithms. These algorithms continuously analyze metrics of systems and applications, determine normal baselines, and surface anomalies with minimal user intervention.

The algorithms generate an anomaly detection model. The model generates a range of expected values that represent normal metric behavior.

You can use the model of expected values in two ways:

- *Create anomaly detection alarms based on a metric's expected value. These types of alarms don't have a static threshold for determining alarm state. Instead, they compare the metric's value to the expected value based on the anomaly detection model.*
  You can choose whether the alarm is triggered when the metric value is above the band of expected values, below the band, or both.
  For more information, see Creating a CloudWatch alarm based on anomaly detection.
- *When viewing a graph of metric data, overlay the expected values onto the graph as a band. This makes it visually clear which values in the graph are out of the normal range. For more information, see Creating a graph.*
  You can enable anomaly detection using the AWS Management Console, the AWS CLI, AWS CloudFormation, or the AWS SDK. You can enable anomaly detection on metrics vended by AWS and also on custom metrics.
  You can also retrieve the upper and lower values of the model's band by using the

GetMetricData API request with the ANOMALY_DETECTION_BAND metric math function. For more information, see GetMetricData.

https://docs.aws.amazon.com/whitepapers/latest/aws-overview/security-services.html