Certificate Management

Track Certification Expiry

What we are going to cover-

1. Certificate Generation Tool - Venafi
2. Feature – Track Certification Expiry
   * + How Venafi keep track of cert validity
     + What reports/ notification it generates about cert expiry
     + Can it also keep track, what all Cerys have been replaced and send notifications if something is about to expire/expired and not been replaced
3. AWS Platform – ACM
4. AWS use case to track certification expiry using SNS ad Lambda
   * + Can we see that what all certificates are about to expire
     + How can we automate cert replacement. any script or tool which can change certs at all required places
     + Can AWS send us notification that we have expired certificate

# Venafi – As a Service

Venafi is a SaaS based Certificate Manage service provides, which provide centralize certificate management solution.

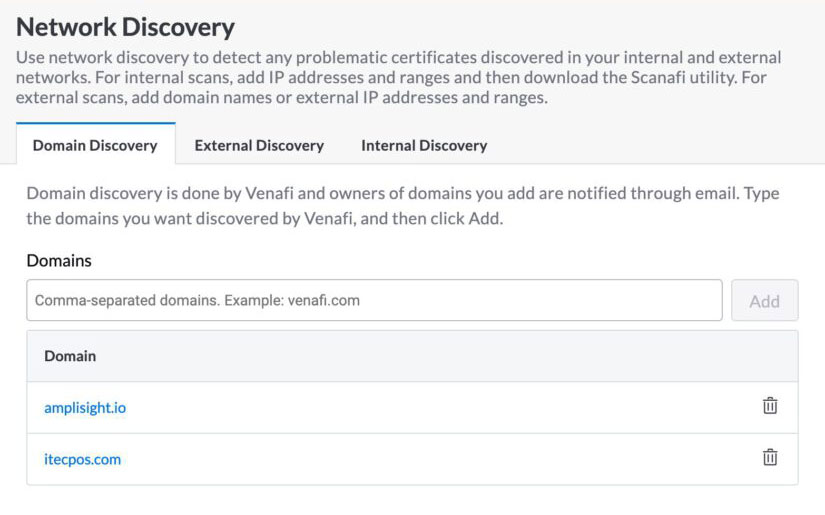
Helps to address challenges like:

1. “I don’t know about all the certs that are currently in use”
2. “I don’t know (or get wanted!) when they’re about to expire”
3. “I know a cert’s been issue but it’s not yet installed. Why not?”
4. “I can’t rotate a cert because I don’t know who owns it”
5. “There are too many certs, I can’t track them all”

The benefits of the services are:

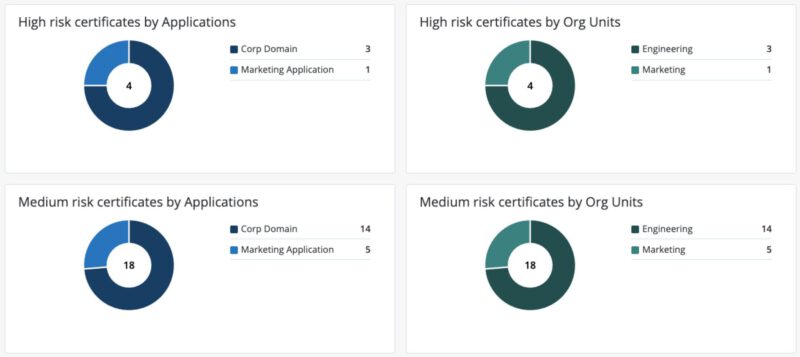
* Eliminate outages to applications, services, and security infrastructure
* Ensure organizational security policies are enforced while supporting digital transformation initiatives
* Revolutionize your machine identity management program

1. Discover Certificate:
   1. Find TLS/SSL certificates internal and external to your network



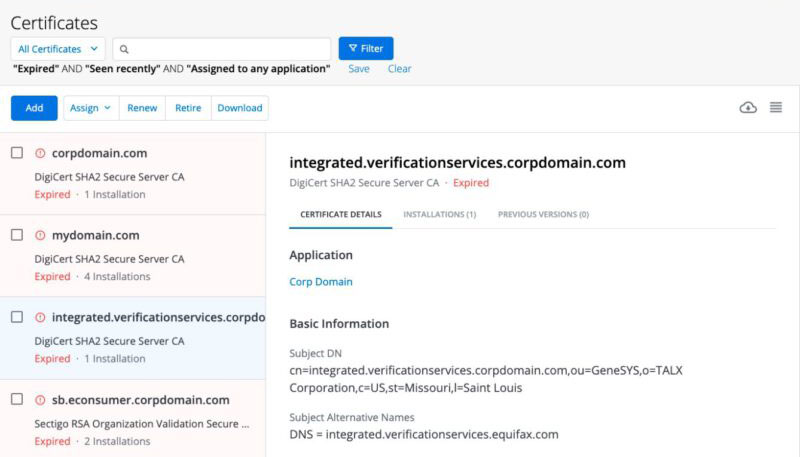
1. Allocate owners

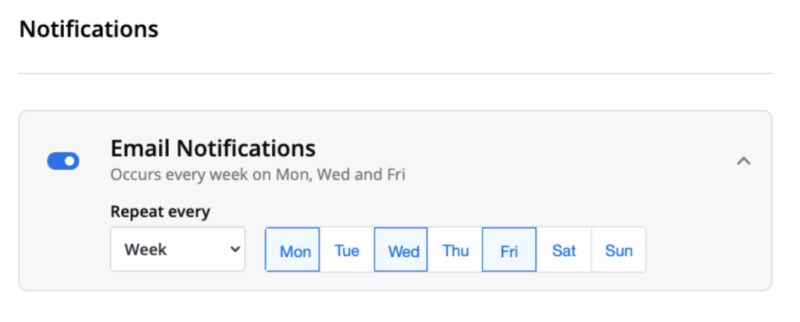
Associate certificates to applications and business units to establish prioritization, ownership and issuance policies.



1. Alerts and Notification:

Use Venafi to keep track of certificates, deliver alerts and insight to teams and application owners to prevent expiration or potential security issues.





1. Simplify and Automate

Enable self-service for public and private certificates with policy-enforced issuance without the need for certificate signing requests (CSRs). Or use our ecosystem of DevOps integrations to securely scale modern application development.





1. Integrate with AWS

Use Amazon Private CA while complying with security policies and audit requirements automatically.

Reference URL:

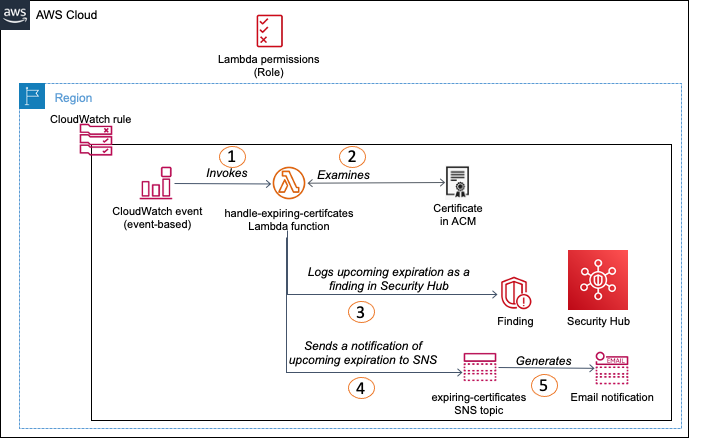
<https://vaas.venafi.com/>

# AWS – Amazon Certificate Manager

ACM provides certificate services to any workload that requires them. ACM provides managed renewals that automatically renew certificates in most cases, there are exceptions, such as imported certs, where an automatic renewal isn’t possible.

The two options for monitoring certificate expirations by using events and metrics that are published into [Amazon CloudWatch](https://aws.amazon.com/cloudwatch/) by ACM.

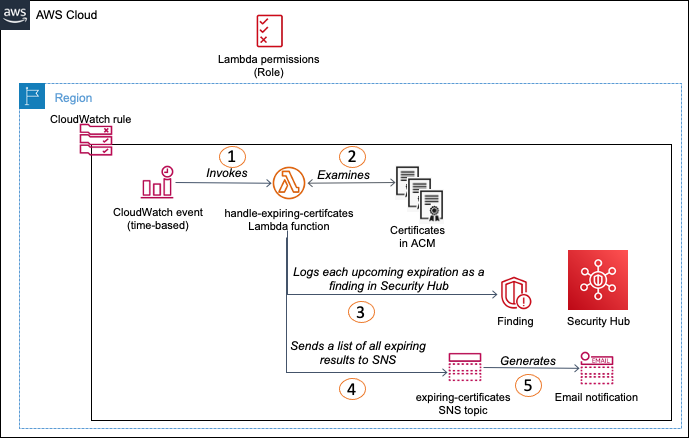
Option 1: Use a CloudWatch event to identify an expiring certificate



In Option 1, a raised CloudWatch event from ACM indicates that a certificate is approaching expiration, which initiates the solution. The option workflow is as follows:

1. CloudWatch receives the event and invokes a Lambda function.
2. The function examines the certificate indicated in the event.
3. The function logs the finding in Security Hub.
4. The function publishes a notification to an SNS topic with the expiration details.
5. SNS creates a notification (most commonly, through email) to any subscribers of the topic.

Option 2: scheduled CloudWatch rule to identify all expiring certificates



Option 2 provides a scheduled solution to examine all expiring certificates in ACM, log all the findings in Security Hub, and generate a single notification through SNS for all certificates that are found. The option workflow is as follows:

1. CloudWatch runs the rule on a timer and invokes a Lambda function.
2. The function finds all certificates that have a DaysToExpiry metric in CloudWatch.
3. The function logs all the expiring certificates as findings in Security Hub.
4. The function publishes a notification to an SNS topic with the expiration details.
5. SNS creates a notification (most commonly, through email) to any subscribers of the topic.

Reference AWS URL:

<https://aws.amazon.com/blogs/security/how-to-monitor-expirations-of-imported-certificates-in-aws-certificate-manager-acm/>