What is Red Forest - Secframe

secframe.com/docs/ramp/what_is_redforest

July 7, 2022

What is Red Forest

Microsoft's NEW privileged identity standard - Rapid Modernization Plan.

What is Microsoft’s RaMP?

Rapid Modernization Plan

RaMP’s goal out of the gate is to secure privileged access with great efficacy: in an efficient and effective manner. From the post linked above, Microsoft states:

> Securing privileged access effectively seals off unauthorized pathways completely and leaves a select few authorized access pathways that are protected and closely monitored. This diagram is discussed in more detail in the article, Privileged Access Strategy.

> Building this strategy requires a holistic approach combining multiple technologies to protect and monitor those authorized escalation paths using Zero Trust principles including explicit validation, least privilege, and assume breach. This strategy requires multiple complementary initiatives that establish a holistic technology approach, clear processes, and rigorous operational execution to build and sustain assurances over time

In a nutshell, RaMP includes some new technologies along with the previous ESAE phases 1 and 2 goals of segregation of privileges.

What is Microsoft’s ESAE and Red Forest?

The Enhanced Security Administrative Environment

Update Re: 12/15/2020. Microsoft Sunsets the Admin Forest

With just one swipe of a hand, Microsoft is retiring the idea of the standalone forest for domain administrators. I thank God that I never had the gumption to write a guide to deploy a Red Forest. The idea of designing, deploying, and managing a separate forest to secure a single domain overwhelmed many. The description and guides to create the forest were lacking. In general conversations between security and Active Directory Administrators, the idea seemed to flop.

I'll be transitioning some work from the ESAE phases into the new RaMP STANDARDS. Bear with me as I changed from

> A full guide on Microsoft's Admin Red Forest (ESAE), and how to get started.

To…

> Resources for rapid deployment for securing privileged identities

---

Securing Tier 0

Outlined in Microsoft's privileged identity blog/post/reference, the focus is on identifying and securing tier 0. They say it in some other terms… The interesting new piece of information on these posts is the fact that Microsoft specifically identified the need to secure the access to the corporation's identity system.

This new standard focuses on the first two phases of the full ESAE road map. The are some new services in RaMP that Microsoft is focusing on that will allow people and companies to quickly deploy security strategies into their identity architecture.

ESAE was Microsoft's complete framework to protect Active Directory (AD). AD, in short, is the identity and access management tool in your business network that holds passwords, credentials, users, computers, groups. AD controls your access to resources across your network;

RaMP targets securing the privileged identities in an organization while recording from the start that a company should always be in a position of "assumed breach." RaMP expands to include and expand over Active Directory because there are organizations that use alternative identity provisioning systems.

Information and Applications Privileged Credentials Resources and Servers

The conference presentation that I could find that talks about ESAE, is from an RSA conference from February in 2017 Critical Hygiene for Preventing Major Breaches ::: Presentation PDF download

Deploying a privileged identity security standard is a foundation for a long term success of the security department. Below is a timeline provided by Microsoft to deploy this security structure.

What is Information?

We define information as can be as anything that holds data such as emails in your organization, research data, credit card numbers, trade secrets. Information is often chopped up into different classifications depending on its importance: Unclassified, Secret, and Top Secret. Often the Secret and Top Secret information is the information attackers want so they can monetize their attack.

What are Privileged Credentials?

The term ‘privileged credentials’ is often used to talk about the user accounts, service accounts, or administrators in your environment. These people and processes often have access to sensitive information. Attackers often specifically target these privileged administrative credentials to gain access to the confidential data.

What are Resources and Servers?

One of Microsoft’s aims is to secure the data that is on your network. By securing the locations where the information is stored, file shares, servers, workstations, a company makes it hard for attackers become successful.

The RaMP framework outlines several quick wins, as well as a number of long term plans to secure privileged credentials. With these privileged credentials secure, attackers are less likely to move laterally and vertically through your network

RaMP’s is focused on Efficient Wins

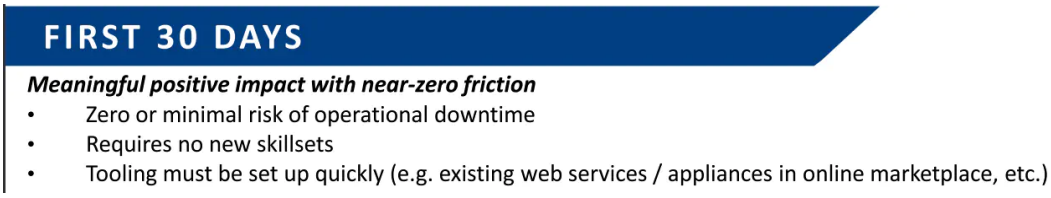
Microsoft open-sourced much of the documentation for deploying the ESAE architecture. The documentation dispersed across TechNet, GitHub, YouTube videos, and other media. Piecing together the documentation can be a bit of a hassle. The goal of these pages and this site’s structure is to put the main building blocks of a secure privileged identity framework into an easily deployable structure.

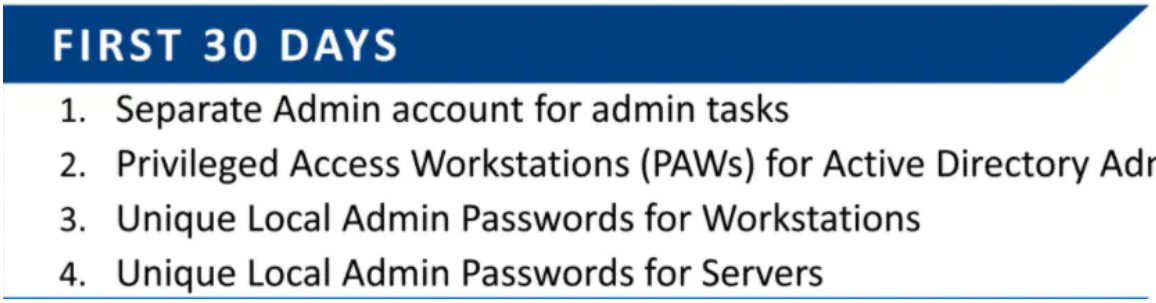
The basic outline for starting the deployment buckets the security items into sections via deployment time. The three buckets outlined are; The First 30 days, 90 days, and Beyond 90 days.

RaMP’s roadmap focuses a lot on the separation of identities and accounts that perform specific functions. I’ll continue to have the guidance on tiers available because the pages are created using a the Trusted Computing Base, a security standard introduced in 1981 that is still relevant today.

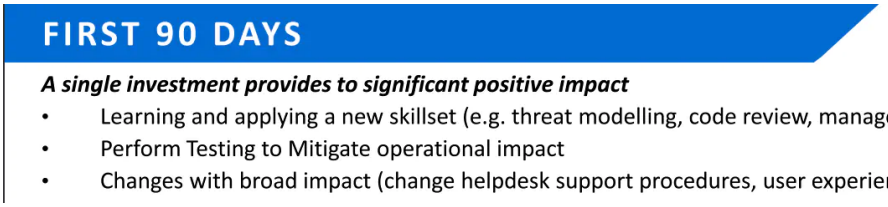
ESAE Timeline

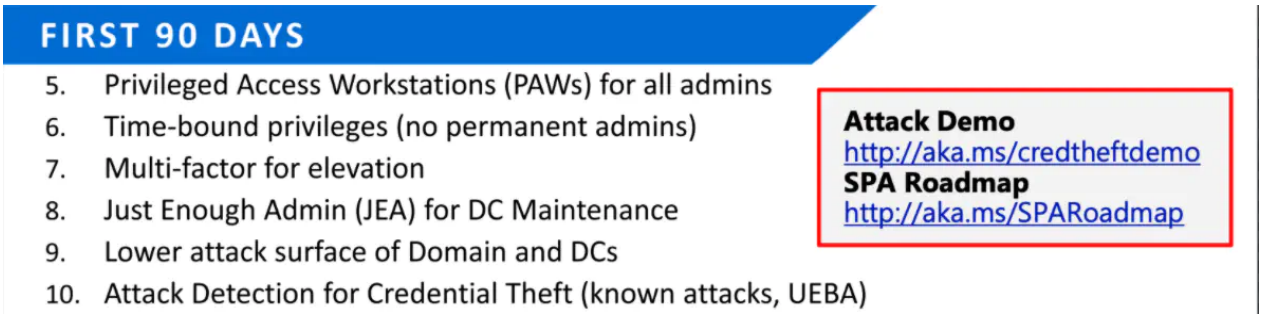
The First 30 Days





90 Days





Starting Microsoft's Phased Approach

Where to begin?

I'd like to begin the journey. I want to understand the terms and prep my probenecid savings. Let's get started with phase 1.

Take me to phase 1

I've already done some admin work and want to know what to do next. Let's get started with phase 2.

Take me to phase 2

LAPS: What is LAPS →