**Identity as the New Perimeter - Michael Kohronas**

In this assignment, I watched the risky.biz podcast featuring Samie Laine. Samie Laine is the director of technology strategy at Okta. He describes his role to be more like a principal security architect. Samie Laine brings up a great point right away. He discusses how not every computer being used in large enterprises has end-point protection. This also stands true to where I am interning since we are allowed to log in with our personal devices. This is made possible since we use OKTA to verify users' identities when they are logging into our SSO. Previously Sami Laine pointed out companies using keys to distribute roles and permissions. This became problematic since keys sometimes were floating out there unnoticed which would become a security risk. The host pointed out that the end-point protection that is usually on workstations eats a lot of resources. This is true for everyone. Sami Laine pointed it out with his current work laptop and at my internship we have the same complications. Sami Laine also mentioned he had a neighbor who worked for an endpoint protection company. His neighbor stated that even though he works for this company he doesn’t have high hopes for end-point protection. Crowdstrike cannot detect malicious files it can only prevent the execution of them once they are executed. This requires extra end-point protection software to be on the system to try and detect malicious files and remove them prior to their execution. Between the issues of the usage of unsecured keys and hefty endpoint protection, Samie Laine mentions that identity can help mitigate some of these issues. When setting up an identity management software implementing SSO helps as well. SSO is extremely practical and most companies should have this implemented already. When a user tries to log in to a system your SSO will usually require an identity check. This can be done through many identity management software but the main one is OKTA. There are several identity verification methods. You can use your phone number to verify your identity sometimes. This identification method is not great due to sim swapping. the stronger method would be using a code linked to an authentication app; a biometric key; fingerprint/password/faceID on the workstation then Okta will verify the IP address & serial number of the workstation to verify identity. It is important to make use of secure identity verification methods. Once the user is verified then Okta will look into UBA. The UBA can be configured by the company to how they desire. There are some key things to look out for when configuring UBA. The time the user usually signs on, the location the user signs on from, and the tasks the user is performing on the system. (There is more that can be configured although, these are the main ones in my opinion). Okta can do this due to its machine-learning capabilities. It can learn about a user's behavior and detect if anything is out of the ordinary. In my internship, they have me looking over suspicious activity. A lot of the time it is just grey noise although they hone in on what is most likely to be malicious by detecting anomalies. If a user logs in from California then a few hours later New York it puts a flag up in our system. Sometimes these users were traveling due to work-related reasons but the system wouldn’t know that unless this activity happens frequently. There should be other systems set up like step-up permissions where a user/admin can request escalated privileges for a certain period of time. This ensures even if someone logs into your account and if Okta doesn’t flag it or prevent the connection completely they wouldn’t have permission to change anything of significance. There should only be a select few accounts that have permanent admin. With Okta or any strong identity management software, it makes it extremely difficult for an adversary to get into a system. This doesn’t get rid of the need for endpoint protection like CrowdStrike since identity management isn’t perfect yet. However, in a few years when identity management becomes even stronger, it will be nearly impossible to access someone's account between machine learning, artificial intelligence, user behavior analytics, and MFA. I overall agree with Sami Laine. He is absolutely right when he says that Identity is the new perimeter of security. Even he acknowledges that in the current state, it cannot protect a system completely but it acts as a strong frontline of defense. Without Identity management software there would be a lot more vulnerabilities on our systems and a much weaker frontline of defense.

**Links**

<https://help.okta.com/en-us/content/topics/security/proc-security-behavior-detection.htm#:~:text=Behavior%20Detection%20analyzes%20patterns%20of,to%20changes%20in%20user%20behavior.>

<https://kineticit.com.au/article/multi-factor-authentication/>

<https://www.okta.com/products/okta-ai/>

<https://www.linkedin.com/pulse/top-5-reasons-move-away-from-active-directory>

<https://www.pcmag.com/picks/the-best-identity-management-solutions>