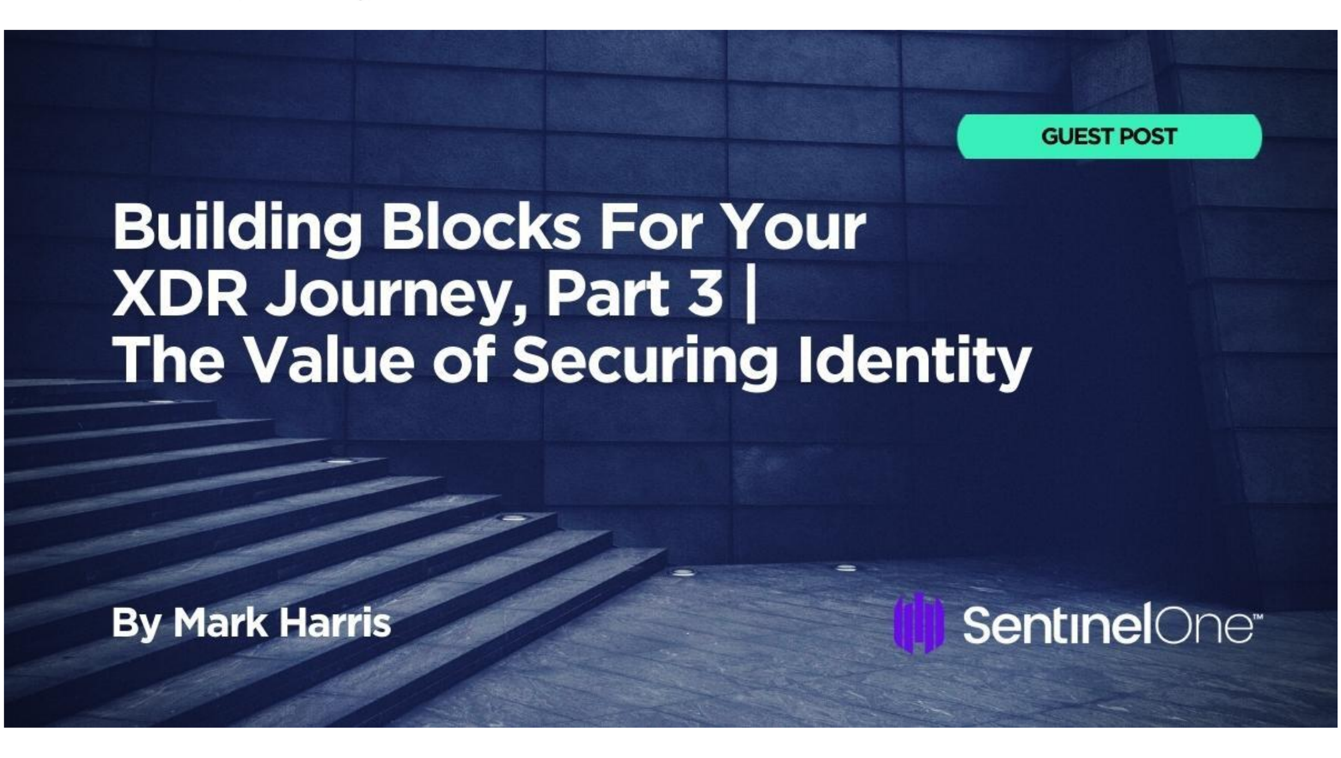
Building Blocks For Your XDR Journey, Part 3 | The Value of Securing Identity

November 21, 2022
by Mark Harris

A Guest Post by Mark Harris, former Senior Director Analyst at Gartner

This is Part 3 of our multi-part XDR (eXtended Detection and Response) blog series, where we discuss the importance and value of securing identity. If you haven't read it yet, we recommend checking out Part 1, which discusses why organizations need to extend protection beyond the endpoint to stay ahead of adversaries, and Part 2, which discusses why Endpoint Detection and Response (EDR) is a foundation and a cornerstone for any XDR strategy.



Identity, The Missing Piece

Malware authors and attackers continue to evolve the tactics, techniques, and procedures (TTPs) that they use. Vulnerabilities in applications and operating systems are regularly identified, and patching and maintaining systems to prevent those vulnerabilities from being exploited has been a constant challenge for organizations large and small. However, most attackers take a more familiar and less technical route to gain initial access: social engineering to access user credentials and data. Research suggests that nearly 50% of attacks are a result of stolen credentials. Once an attacker has control of a user's identity, they have the same privileges and access as the real user.

Social engineering has been a key element of attacks for many years, whether it be through phishing emails, or clicking on links to exploit a vulnerability. Even the simple warnings seen in Office documents such as Microsoft Word that a document has active content (i.e. Macros) are often ignored and a user will simply enable them. Repeatedly asking users to make cybersecurity decisions will inevitably lead to user fatigue and failure.

Credentials are Gold to the Attacker

Credentials are the key to the user's identity, the way systems identify and authenticate who a user is. This identity is based on an Active Directory (AD). AD effectively defines an organization structure: users are part of groups, groups have different rights and privileges to access systems and therefore data.

Multi-factor authentication (MFA) is a critical part of checking that the user is real and who they say they are. However, as with many security controls, a balance must be struck between authenticating a user too often and allowing them to get on with their work. Once authenticated, the user won't be asked to re-authenticate again for some time.

That's the upside, but the downside is that if malware is successfully installed on an endpoint, and the user has already authenticated, the malware will now have the same access rights as the user. Credentials also cross traditional boundaries and are used to manage cloud entitlements and directory systems that cover both human and machine identities.

MFA is a critical component of Identity Access Management (IAM), which controls access to the systems and services within an organization. Privilege Access Management (PAM) is a subset of IAM and controls not only the access but more fine-grained controls over what the user can do. Both focus on allowing access rather than preventing access, so again, if an attacker has taken control of a device, they are effectively authenticated in the same way as the "real" user.

Managing Identity Risk

Unfortunately, the risks associated with identity don't stop there. Once you have the credentials for one user, it's relatively straightforward to gain access to another user's credentials. There are simple-to-use, free, open-source tools that can escalate privileges from one user to another. Mimikatz is the most widely known. All an attacker needs to do once they have compromised a regular user is download Mimikatz and steal the credentials of another user to gain higher privileged access. This can then be used to connect to another device and move laterally. Access to the active directory can be gained very quickly, and then the attacker can create their own set of credentials and have free reign over the entire organization.

Many malware groups include Mimikatz as part of the malware, or at least their version of it. When combined with scripting tools like PowerShell (e.g., `Invoke-Mimikatz`), these attacks can be carried out without any further files being written to disk.

Managing AD is notoriously difficult; credential permissions and configurations are constantly changing in most organizations as workers, applications and data morph and evolve. Adapting and responding to business needs means that maintaining security is a constant battle and often leads to protection gaps and accounts being overprivileged.

> Gartner estimates that 50% of cloud security failures are due to poor management of identities, access and privileges. This figure is expected to rise to 75% by 2023.

Protecting against these sorts of complex attacks is the focus for Endpoint Detection and Response (EDR) solutions and increasingly Extended Detection and Response (XDR). By correlating and combining information from multiple endpoints, multiple security tools, the tell-tale signs of an attack can be identified. Even so, these solutions on the whole focus on the security of systems rather than users and their identities.

Identity Threat Detection and Response

A new category has recently begun to appear, Identity threat detection and response (ITDR). These solutions focus on detecting identity-based attacks, whilst identity-based attack surface management (ASM) focuses on restricting the ability for the attacker to easily move laterally by identifying misconfigurations and overprivileged accounts.

SentinelOne has introduced both an identity-based attack surface management capability with Ranger AD and ITDR with Singularity Identity.

Ranger AD analyses the active directory structure and identifies accounts that are misconfigured or over privileged. This makes it harder for the attacker to gain privileged access, at the very least making it harder for them.

Singularity Identity not only identifies identity-based attacks but works with Singularity Hologram to create network-based lures and deception to protect assets and trick attackers into revealing themselves. If an attacker gets access to one set of credentials, when they start trying to find another set of credentials to move laterally, they find some lures or "fake" credentials. As soon as they try to use them, their activity is uncovered.

Taking XDR to the Next Level

The identity-based detection and attack surface management tools are a valuable addition for the security teams. However, where it really comes into its own is when it's combined with Singularity XDR. The attack surface of both devices and identities can be reduced, but more importantly, when an identity-based attack is identified it is both stopped, and the entire attack chain can be identified to allow changes to be made to prevent it from happening again. Identity is the missing piece of XDR and significantly increases the effectiveness of both detection and response.

The open XDR capabilities of Singularity mean that automated responses can be used to remediate compromised user credentials (forcing a reauthentication or change of password for example) and interact directly with identity-based management tools such as IAM and PAM.

Threat actors' techniques continue to evolve. They have shifted away from targeting individual machines to targeting the entire organization, and that organization consists of users and identities. Identity attack surface management and detection play a pivotal role in cybersecurity. The addition of identity into Singularity XDR means there is finally the opportunity to protect the entire organization, not just the devices and infrastructure.

Parting Thoughts

As EDR evolves into XDR, the role of identity-based controls grows more important. With ITDR as one of the building blocks of a mature security strategy, organizations can more effectively secure their data and systems against sophisticated threats. By reducing the privileged access that users have to infrastructure, you can reduce the risk of data breaches and other security incidents. ITDR controls can help build a stronger defense against today's threats and better protect an organization's data and systems into the future.

If you would like to learn more about SentinelOne Singularity XDR platform, contact us for more information or request a free demo.

About the Author

Mark Harris is a Cybersecurity advisor and former Senior Director Analyst at Gartner with over 25 years of experience. At Gartner Harris was the author of a variety of market shaping research for Endpoint Protection and EDR including the EPP Magic Quadrant and Critical Capabilities as well as Market Guides and research on ransomware and other threats.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- SentinelOne Named to Deloitte Fast 500 List for 4th Consecutive Year
- Apple's macOS Ventura | 7 New Security Changes to Be Aware Of
- MITRE Managed Services Evaluation | 4 Key Takeaways for MDR & DFIR Buyers
- Decoding the 4th Round of MITRE ATT&CK® Framework (Engenuity): Wizard Spider and Sandworm Enterprise Evaluations
- Bringing Identity to the Era of XDR
- Best-of-Breed Identity Threat Detection and Response Meets Best-of-Breed XDR

©2022 SentinelOne, All Rights Reserved.
Privacy Policy Terms of Service