Microsoft Security Exposure Management Community Call [AmericasEMEA]-20251210_110039-Meeting Recording

December 10, 2025, 4:00PM

30m 52s

Amy Jarosky (AG Consulting Partners Inc) 0:14

Welcome everyone. Thank you so much for joining us today for the Microsoft Security Exposure Management Community Call. We are very excited to have you here today and present lots of information to you. As always, we will be answering your questions along the way as well, so feel free to post.

Post any questions you may have during the presentation in the chat and then if a few minutes allow at the end, we will enable the mics if you'd like to ask your question in that way. Also note we are recording this call and the recording as well as the deck will be available on the we will be.

Actually emailing them out to you within the next few days, so if you'd like to rewatch the session, stay tuned for that e-mail in your inbox. Also, if you'd like to turn on live captions or the interpreter functionality, feel free to do so in your teams. By the More button. Again, thank you all for joining us. We really appreciate your time today and I will now turn it over to Ramy Omar.

Ramy Omar 1:22

Thank you. Thank you, Amy. So quick introduction, my name is Ramy Omar. I'm a partner success manager based out of EMEA and today I'm happy to take this starting with Lexi Lederman, who is a customer experience engineer from the customer experience engineering team.

To go through Microsoft Security Exposure Management. So hovering through the agenda for today, we're going to start with the learning objective of this session. Why do we need the Exposure Management and what is Microsoft Security Exposure Management in essence?

And then we'll go through in product demos and then as Amy mentioned, hopefully we'll be having some minutes at the end to go through Q and ES.

If you overthrow the learning objective after this training, you will be able to understand the concept of exposure management, how it's going to impact the

current cyber landscape, how to enable your identifying the prioritized vulnerabilities within the organizations, whether while you are working or within your customers as well.
And then definitely effectively utilize Microsoft Security Exposure Management solutions with in product exploration and some practical demonstrations we are going to go through this session and then how to integrate exposure management data across various Microsoft Defender products.
Allowing for unified approach to security operations and improved decision making.
We are having some acronyms that we are going to use during this slides. We don't need to go through all of them now, but I'll put a screenshot of this in the chat window so that you can go to them when you need them.
Without further ado, I'm happy to introduce Lexi, please, if you want to take over.

Lexi Falcone Lederman 3:03
Thanks so much, Ramy. Hi, everyone. Good morning, good afternoon, good evening. Thanks for being here today. So let's get started. We want to first discuss how vulnerability management has evolved and why exposure management is our next frontier. Traditionally, vulnerability management was all about asset discovery and patching endpoints and servers using.
Threat Intelligence to prioritize. As our environments expanded to include mobile identity, apps and web, we moved to risk-based approaches, contextualizing weaknesses and validating security controls. But today, our tech services have exploded. SaaS apps, cloud data and supply chain risks are everywhere. Continuous assessment and.
Risk reduction mobilization are now essential. Exposure Management picks up where vulnerability management leaves off, helping us discover, prioritize, and remediate exposures across this ever expanding surface. It's about integrating business context, not just technical findings, and mobilizing teams to proactively reduce risk before attackers.
Can exploit it as a risk oerations center.
The reality is, as we said, environments grow more complex and the gap between exposure and remediation widens. The average team is now responsible for nearly 400,000 assets, ranging from apps and data to devices, controls, networks, users.
On top of that, organizations are dealing with over 830,000 exposures, including CVES, misconfigured controls and overprivileged identities. The mean time to

remediate these exposures is about 58 days, and while that's an improvement, it's still far too slow given the pace and complexity of modern.
Certain threats. A key contributor to what's driving the slow time to remediate is the reactive nature of traditional risk management processes. Instead of proactively reducing risk, many teams are stuck in cycles of prioritizing by risk, validating feasibility, and mobilizing resources, often after the compromise.
In this era of AI, especially where attackers are growing exponentially smarter and faster every day, it's critical for organizations to shift from reactive vulnerability management to proactive exposure management.
Let's consider how most security teams operate versus how attackers approach an environment. Security teams are often structured in silos, the e-mail security team, the endpoint team, the identity team, and so on. Each group defends its own territory, often with little cross-team collaboration.
This siloed approach means that security teams are defending in lists, focusing on their silos and otentially missing the bigger picture.
Meanwhile, attackers don't think in lists, they think in graphs. They don't just look for a single surface, they map out potential attack paths. Every asset, every device, user account, cloud work, workload, SaaS app can be viewed as a node in a graph.
Attackers look for ways to chain these nodes together, moving laterally until they reach something valuable. Minor exposures like a phishing e-mail or a misconfigured endpoint can quickly escalate. They start with something simple and follow the chain, compromised endpoints, misconfigured identities, exposed data, and vulnerable workloads.
Attackers move from one asset to the next, exploiting the seams between the siloed defenses. The breach grows in scope, moving from the initial entry point to privileged accounts and sensitive data. Attackers can maintain a foothold, encrypt files, exfiltrate data, and even recon additional accounts for future attacks.
The key take away silos hurt defenders. When we defend in lists, we miss the cross silo relationship that attackers exploit. Microsoft Security Exposure Management helps us break out of this reactive cycle. By modeling our environments within the Microsoft Exposure Graph, we can identify and remediate attack paths.
Before they become a reality.
Now, how do we actually see beyond these lists and silos? MSEM, Microsoft Security Exposure Management is included with existing E3 and E5 licenses. It is as rich as the data you connect to it. So for example, if the customer is using the entire Defender

Suite.
It will provide contextualized views across their entire ecosystem. If they're only using MDI, they won't see endpoint data unless they have a valid third party connector enabled. As I mentioned, MSAM uses the exposure graph to connect, contextualize, and prioritize risks across an entire attack surface at the heart of.
Of the exposure graph is a unified asset inventory powered by both native integrations with Microsoft Defender products and connectors for third party security tools. As you can see on this slide, the connector ecosystem is extensive. All of our Defender products, Hentra ID, MDVM, Defender for Cloud or CSPM.
Plus third-party tools like Qualys, Tenable, and Rapid 7, with many more to come. By bringing all of this data together, MSEM connects the dots, so you're not just seeing isolated findings, but a contextualized view of your entire security posture.
The exposure graph then models all of these assets and their relationships automatically, revealing vulnerable crown jewels and mapping connections that could represent risk. By visualizing the entire attack surface, we can uncover gaps, prioritize remediation, and ensure that critical assets are protected.
This approach helps us move from reactive siloed vulnerability management to proactive exposure management, identifying and shutting down attack *** before they become incidents.
O Let's dive into the demo and see how this works in action.
So we're going to go to our Defender Portal, security.microsoft.com, and we're going to go to our Exposure Management tab. Once we expand that, we'll first go to Overview. This is going to give you a quick overview of your security posture.
You'll see you have your assets at a glance. In this environment we have 121 devices, 2.3 K cloud resources, 3.1 K identities. And 1st what we need to do is determine which of those assets are critical. Where are our crown jewels? So we know how to prioritize protection. So we're going to Scroll down to.
do critical asset management.
Critical Asset Management in Microsoft Security Exposure Management gives us two options. Option number one are these predefined classifications. So this is the out-of-box Microsoft has determined that these are critical assets. It's things like your DCS, your security admin identities.
Identities, things like that. If you disagree with any of these assessments, you can customize these. So for example, Microsoft believes that your security admin identities are very high criticality level. You can change that if you want to treat it

differently in your environment.
It'll also give you a nice list of all of your secondment identities.
We also have the option to create custom classifications. So for example, in this environment we've determined that all key vaults are sensitive. So we've said let's pull all of our Azure key vaults.
And categorize them as sensitive assets. These are the endpoint nodes on the graph. So these are the items that we want to make sure that we prioritize protecting. So now that we have identified our critical assets, let's go ahead and look at an example of an attack path.
We're going to go back to exposure management and attack surface attack aths. This is going to be an overview page showing us the lay of the land, our attack pass and our environment. You may notice that we have this attack pass over time and this graph is going to be dynamic and that's because things are always changing in your environment. You're adding, removing.
Changing identities, devices, adding different things into your environment, removing different things from your environment. So this is meant to be dynamic and will be constantly changing. It's not necessarily a bad sign if your attack paths are growing as long as you are.
Remediating those attack paths as they continue to increase.
We have a couple of topics here to discuss. Topic number one, top targets. So these are the top critical assets that attack paths are leading to. So 53 attack paths lead to this workbook for example.
Top entry points. These are assets that are the gateway into an attack path. So you'll see that this Terraform deployments is the entry point to two 2000 attack paths. And even maybe more importantly, you'll see choke points.
Choke oints are assets that are members of multiple attack aths. O if you're looking for a low hanging fruit where to start with remediating your attack aths, you might want to start looking at your choke oints, which is what we're going to do today.
We can go over to the Choke oints tab and the one that I'm interested in today is going to be.
Woodgrove Server One. You can see here that Woodgrove Server One has access to four critical targets and is a member of five attack paths. It's a good place for me to focus in on. If I click on this choke point, I'll get general details. I know it's a virtual machine. I get the device inventory ID.
And I can see the discovery source. So I know that this was captured by Rapid 7,

MDC and MDE. When it's captured by multiple discovery sources, it is deduped.
If I want to dive into the attack path itself, I can select View Blast Radius and that will take me to our simulated attack path graph. So you can see here we have Woodgrove Server one that can authenticate as this managed identity.
And with that managed identity, it has access to both a storage account or three storage accounts with three different crown jewels and one of those Azure key vaults that we have classified as very high criticality. So what do I do about this?
You'll notice on Woodgrove Server One, there's also this little bug icon. That means that there's a vulnerability on Woodgrove Server One. So I'm going to click into this again. I'm going to select see more details, and the first thing I see is that we have two active alerts and two incidents.
Unusual number of failed signin attempts. That could be a password spray attack, that could be a brute force attack. Definitely something happening here. Oi want to learn more about how to harden this device. I can select open device page.
And I get a summary of everything that's going on on this device. Our friend security copilot, which is now included in our E5 license, is going to give us an overview of what is most critically wrong with our device. You can see that though it has MDE enabled on it.
A lot of the features of MDE are not on and we also see this these two critically out-of-date softwares, Windows Server 2019 and.NET Framework. So I can go over to security recommendations and I think that's where I want to focus first.
Windows Server 2019 has 792 weaknesses in its current build, 21 critical CVES, 533 high vulnerability CVES. So I'm going to go ahead and open the recommendation and request remediation.
O This is just an example of how we can start with our choke point and look at how it.
Is a critical vulnerability for multiple crown jewels. Once I remediate that, then I have protected these four critical assets.
Like Amy said in the beginning, if you have questions, feel free to throw them in the chat and we will commit to answering them. All right, let's go back to our presentation now, and now we're going to talk a little bit more about posture.
So as we saw, the attack surface is vast and complex, and exposures are everywhere. But the real challenge isn't just identifying those exposures, it's knowing which ones matter most. And some helps us move beyond simply cataloging those vulnerabilities. It enables us to think in graphs and measure and prioritize exposure

across the entire environment.
Now we're going to talk about the posture element of MSIM program initiatives. Initiatives make it easier for customers to know what to do next instead of getting lost in a sea of recommendations like in traditional secure score scenarios. Initiatives group and prioritize what matters most based on common threat scenarios like business e-mail compromise or based on how teams are broken up, such as endpoint security. Initiatives give clear steps and progress tracking so teams can keep improving their security posture even after the initial deployment engagement is.
Complete by highlighting specific actions and goals. Initiatives encourage admins and teams to keep using the product after deployment, not just during set, thus directly driving active usage. Initiatives provide prioritized recommendations. Based on your organization's objectives, helping you answer critical questions like how secure are we against a specific CVE or threat? Where do we stand in our mitigation efforts? How do we quantify our exposure and track progress over time, making it easier to focus on what's important and show progress to leadership?
So let's go ahead and go into an initiative, see what it looks like. I'm going to go back to my defender.microsoft.com portal or security.microsoft.com portal, expand exposure management and we're going to go to Exposure Insights Initiatives.
So you'll see we have two different categories, domain initiatives and threat initiatives. Let's first talk about domain initiatives. So I think an example that we have here is you can see we have things like business e-mail compromise as well as endpoint security. Let's type into our endpoint security and open the initiative page. So this is a good example of an initiative that your endpoint security team might want to use as a benchmark for the progress that they're making. You can see a couple of things. First, we're going to look at history. This is going to show us the changes that have been made in our environment. So we see.
Uh, let's see on 11/20.
Eight, we saw a spike in our score. Why did that happen? Let's go down to our 11:28 date and we can see that the reason for the spike in the score was that we enabled EDR unblock mode for some of our Windows endpoints.
Each initiative has security metrics, which are containers for security recommendations. These are the actions that need to be taken to contribute to improving your endpoint security score.
So this is a really good way to hold your teams accountable for specific business

focused areas. So that's an example of a domain initiative. We also have these threat initiatives and these are aligned to actor profiles and actor technique profiles.
So actor profile is associated with those, you know, pesky bad actor groups that you read about in the news. So for example, if you have your CSO come in and say, hey, I was on the subway to work this morning and I read about canvas cyclone, what are we doing to?
Rotect ourselves from that. You can easily go into this Actor Rofile Initiative and see a list of recommended actions that you can take to better rotect your environment from the specific Actor profile.
You also can go into technique rofiles.
And this is more of a generic how are we protecting ourselves from adversary in the middle credential phishing, for example. Here are recommendations that need to be taken to better protect yourself from this technique profile. So again, these are just taking the sea of recommendations that we see in.
In something like Secure Score and sorting them into initiatives based on business context, actor profiles, technique profiles. So that way we can more accurately prioritize the steps that we're taking when we have so many changes to implement in our environment.
I also have a.
New public preview that I wanted to share with you today, which is kind of the next step for these initiatives in my opinion. So a few weeks ago, post Ignite, we released a capability in public preview, the Unified Recommendations Catalog.
This feature brings together all Microsoft Security recommendations like the initiatives into a single streamlined experience, consolidating insights from Secure Score, MSAM, CSPM, MDVM, more to come. Instead of jumping between these tools, security teams can access comprehensive guidance organized by attack surfaces. Whether it's devices, cloud identity, SaaS, apps, or data, the catalog separates misconfiguration recommendations from vulnerabilities, recognizing that these require distinct workflows and are often handled by different personas. This clarity helps teams focus on what matters most, track progress, and demonstrate improvements to leadership.
And with this catalog, organizations can gain full coverage and actionable steps to strengthen their security posture all in one place. So let's take a look at what that looks like. I go to Exposure Management Recommendations. Here is our Unified Recommendations catalog. You'll see that we're broken up by.

Workloads, so devices, cloud, SaaS, apps, identities, data. I tell my endpoint security team, hey, we have some misconfigurations in our devices catalog. And then I tell my SOC team, hey, we have some vulnerabilities.
In our devices catalog. So that way those folks can focus on the areas that are most important to them.
A couple of features in here. We have our device secure score, we have score history like we just said. And then this is like I said, this is still in public preview, so things may change a little bit. But I wanted to show under SaaS apps, identity and data. We also have this recommendations by status which could be really valuable.
So if you're working on one of these recommendations, but it's taking some time because you have to collaborate with multiple teams in your organization, you can set it to planned or like risk accepted. We're using a third party for this. We want to address this.
We're using an alternate method and then I can get a full view of my entire posture at state, what I'm doing, what my plans are, and where I'm going forward. Lastly, you can also see score comparison, which will show your score against organizations of a similar size.
So pretty excited about this. You'll notice that the data pillar is pretty light, but we are continuing to populate that as well. And like I said, public preview right now, but expect to see more in this space as it continues to evolve.
All right. And lastly, I've gotten some questions around like how does this fit into the overall Sec OPS simplest XDR narrative. So let's connect exposure management to that whole story. You can think about exposure management in a.
Proactive risk operations context, whereas you look at Simplex XDR in a reactive security operations perspective. So exposure management helps you discover, assess and remediate exposures across your apps, endpoints, network data identities.
Infrastructure where security operations tools like Simplex XDR unify those detection, investigation and response. The real power comes from integrating these two worlds.
So you use the exposure management to proactively reduce your attack surface and then you leverage Simplex XDR for rapid detection and response when incidents occur.
It's not a matter of if, it's a matter of when. The unified approach ensures you're not just reacting to threats, but actively reducing risk and improving your overall security posture.
So that's what I had for you today. What questions do we have? We have some. We

definitely have some time.
Any thoughts on this? Does this seem like a a good direction? Do you think that customers will see value in this?
It looks like mics might be off. Amy, is that right? Can folks access the chat or their mics?

Amy Jarosky (AG Consulting Partners Inc) 25:08
Yeah, I'm turning them on right now.

Lexi Falcone Lederman 25:11
OK, cool.

Amy Jarosky (AG Consulting Partners Inc) 25:24
OK, should be good to go, so feel free. If you have any questions, just take yourself off of mute.

Lexi Falcone Lederman 25:46
I have one let's see.
All right, let's hear it.

Ramy Omar 25:50
Yeah, for this loud one you were showing this uh virtual machine that was impacting 4 crown jewels of yours.
So it appears this vulnerability when we were on this virtual machine and checking it. But if we have looked to the other resources like one of these this.
One of these accounts or one of these databases that were in the post because this virtual machine was impacted. Will it appear that they might be in in a critical way as well because the previous channel or the previous post node has an impact?
From their own view.

Lexi Falcone Lederman 26:26
Let me let me get in here and make sure I fully understand the question. Let's let's reopen it so we can talk to it. I think that's a great question.
OK. So we're in here and we see our vulnerability on Woodgrove Server One. So I think, can you see your question again now that we're looking at it?

26:45
Product.

Ramy Omar 26:47
Yeah, if I'm looking or checking one of these identities on the storage accounts, will I see them vulnerable as well?

Lexi Falcone Lederman 26:52
Mhm.
Oh, so so like this this managed identity. So I know for a fact that the reason that this vulnerability get is able to access is because of the outdated Windows Server. There's a CVCVE on there that basically gives the user, if they're able to exploit it, ability to. To behave as many managed identities. So I think your question was would this managed identity also show vulnerability because the server has access to it? Is that right?

Ramy Omar 27:30
Exactly.

Lexi Falcone Lederman 27:31
Yeah, so I don't think so because there's no step that you can take to harden this managed identity, right? You have to start with the source. So I think that this is where the the entry point is and this is where the vulnerability is cause if I harden this managed identity.
The the bad actor would just use a different one.

Ramy Omar 27:56
Mm-hmm.

Lexi Falcone Lederman 27:58
So it's really about getting to the source of the issue instead of sending you on a kind of wild goose hunt.
So it's all about prioritization. Does that answer the question?

Ramy Omar 28:08

Yeah, sort of, which might be misleading because if we are having, we can.
We can investigate it, but it but the other server might be impacting other identities as well. In in our occasion here it's happened to be 1 managed identity, but it might be impacting others as well. So mitigating the source makes sense.

Lexi Falcone Lederman 28:26

Exactly, yeah.
And then I see a question, what kind of licensing is needed for exposure management? So it is included with whatever license you are currently using. So for example if you are, if you have.
MDE and not MDI, then you're going to get signals from MDE, but you're not going to get any signals from MDI. So it'll just say I think it says like not available. Let me see if I can find an example.
It'll just be Gray and say not available for any recommendation that doesn't have signals coming into it. So it's not an additional license. You don't have to pay any extra. It sees its most value with an E5 license. It sees more even more value for when all of your Defender products are.
Deployed. We also have, like I said, the third party connector options. So these are the available external connectors today, but this is going to increase exponentially to more of like the data connectors that we have available in Sentinel within the next year or so.
O We really want this to be a one stop shop for your entire exposure across your entire environment, even if you're not a Microsoft only shop.
What else?
Great. Well, thank you all for your time today. Here is a feedback form. If you have feedback from the training, we'd love to hear it. If you have further questions, you can always feel free to reach out. Happy to help. And yeah, thank you all so much for your time.

Amy Jarosky (AG Consulting Partners Inc) 30:26

Thanks everyone.

Ramy Omar 30:30

Thank you. Thanks everyone. Thank you, Lexi.

Amy Jarosky (AG Consulting Partners Inc) stopped transcription