semperis

IDENTITY THREAT DETECTION AND RESPONSE: WHAT IT MEANS

Sean Deuby of Semperis on the Significance of ITDR Emergence in the Market

iSMG
INFORMATION SECURITY MEDIA GROUP

Identity is now the first line of attack, so how can enterprises minimize their attack surface? Identity threat detection and response (ITDR) is a newly recognized cybersecurity solutions category. **Sean Deuby** of Semperis discusses ITDR and how enterprises can best take advantage of it.

In this video interview with Information Security Media Group, Deuby discusses:

- The emergency of ITDR
- How best to respond to and remediate identity attacks
- How to hone ITDR in alignment with the NIST CSF

WHAT IS ITDR?

TOM FIELD: What is ITDR, and what's the significance of Gartner now recognizing it as a category of its own?

SEAN DEUBY: The acronym ITDR throws a lot of us for a loop because we immediately think of IT and disaster recovery, but it's not that. It's identity, threat detection, and response. Gartner defines it as correct and secure operation of the identity infrastructure rather than the individuals and resources in that infrastructure. We have enough categories to talk about endpoints, email, applications, and network. We need a category to talk about the identity infrastructure that everything else depends on — how you protect identity itself because identity has become so important — and that's the significance of it.

Sean Deuby

Deuby has over 30 years of experience in enterprise IT and hybrid identity. An original architect and technical leader of Intel's Active Directory and Texas Instruments' NT network and a 15-time MVP alumnus, he has been involved with Microsoft identity since its inception. Previously, as a technical director for Windows IT Pro, he wrote over 400 published articles on AD, hybrid identity and Windows Server.

> **“As we’ve moved to the cloud and to all these untrusted networks, identity is one of the most important things for security. It’s what all zero trust is based on. Now, Gartner has said that it’s important to make sure that organizations explicitly work on protecting their identity systems.”**

As we’ve moved to the cloud and to all these untrusted networks, identity is one of the most important things for security. It’s what all zero trust is based on. When you’re trying to access a resource across an untrusted network, you’re continually verifying the user’s identity to make sure they are who they say they are to access that. Now, Gartner has said that it’s important to make sure that organizations explicitly work on protecting their identity systems.

ATTACKERS AND LEGACY IDENTITY SYSTEMS

FIELD: You have said that identity is the first line of attack. How do you see adversaries today taking advantage of our legacy approaches to identity?

DEUBY: For most of the world, the on-premises identity system is Active Directory. Any organization with over 500 users or so has it, and it is a critical part of their infrastructure. As we have moved to the cloud, most organizations have a hybrid identity infrastructure where they take their on-premises identity and project it out into a cloud service provider — like Azure Active Directory or AWS or Okta — to provide single sign-on for web applications.

Active Directory is 23 years old, and threat actors know that many organizations have accumulated vulnerabilities over time. In operations, there’s rarely enough time to add users, groups, or applications with least privileged access to something. You have to get stuff done, so you accumulate a vulnerability here and another one there. You add a service account that has administrative rights because it needs to run SQL Server and you don’t have time to figure out how to make it a little more secure. Eventually, you’ve accumulated a host of vulnerabilities.

Service accounts can be used for “kerberoasting.” Kerberoasting is a post-exploitation attack technique that attempts to obtain a password hash of an Active Directory account that has a Service Principal Name. The threat actors know that. The tools have gotten better, and if they can gain access to Active Directory, because it’s designed to make it easy to find resources, they can gain control of the resources. So, Active Directory is involved in almost every cyberattack. Mandiant says it finds that Active Directory was either directly targeted or was used as a means to get to the target in 90% of the investigations that it does for its clients. CISOs look at their pen test reports, and they say 100% of cyberattacks go through Active Directory. The adversaries are absolutely taking advantage of it.

They may get in through endpoints and many different ways, but once they get in, they all go through this identity system.

TOOLS TO REDUCE THE ATTACK SURFACE

FIELD: How do we minimize the attack surface?

DEUBY: There are free tools that enable you to understand what your vulnerabilities are. One of the challenges of working with Active Directory is that because it's been around so long, the original highly skilled practitioners have often retired or gone on to something else. Most organizations have inherited their Active Directory environments from their predecessors. They don't know why things are done the way they are done, and they're afraid to touch things.

Semperis offers a free tool called Purple Knight, which is designed for Active Directory security vulnerability assessment. We don't see any of the data. It all runs entirely in your local environment and doesn't require any rights in the environment. It looks at Active Directory the way a threat actor would. It analyzes your Active Directory for over 130 vulnerabilities and produces a report that is about 70 pages long and gives you explicit guidance on how to remediate those vulnerabilities and rank them from most critical to least critical. It tells you what you need to do to reduce your attack surface as quickly as possible.

We have another tool called Forest Druid that is a Tier 0 attack path analysis tool. It's a sophisticated tool that requires a little practice to run and an understanding of attack path analysis, and it analyzes the attack paths from the inside out. Forest Druid looks inside for paths outward from what we call Tier 0 — the most important aspects that run the Active Directory service. It also looks for paths into Tier 0 that you might not be aware of. Maybe there's a Group Policy Object with a user that has rights to do something that can change domain controllers. Forest Druid helps reveal those vulnerabilities. You can find the tools at purple-knight.com.

RESPONSE AND REMEDIATION

FIELD: Let's talk about the R in ITDR. When attacked, how can enterprises best respond and remediate?

DEUBY: In the response department, we do what our incident response team does. We back up a copy of your Active Directory right away and get it air gapped and offline. Hopefully, you can do that before the threat actor has a chance to crypto-lock your Active Directory environment. They used to immediately lock it to gain the ransom for it. Now, the dwell time in an Active Directory in an organization is anywhere between 20 and 200 days; they don't cripple it right away.

So, get a backup of Active Directory, and restore it — hopefully malware-free — into an isolated environment where you can threat hunt and dig around and try to figure out what the threat actor has been doing without giving away that you know something has happened. If they decide it's not worth it and they lock the environment, then you've lost the initiative. But then, our incident response team can use our Active

Directory Forest Recovery tool to take a backup of your forest, without any malware on it, and restore it into an isolated environment. Then, we run some post-breach tools to find out what the vulnerabilities are.

ASSESSING ITDR MATURITY

FIELD: How should enterprises assess their ITDR maturity and understand where they need to go?

DEUBY: A first step is to run these security assessment tools. Gartner eventually will come out with its own steps for evaluating identity maturity, which falls under the same IT maturity guidelines as other aspects of IT. It's the governance. Most Active Directory environments have horrible governance because Active Directory just works and people don't pay attention to it. But we need to scrutinize it and bring it into the fold. We have to get away from the "Active Directory just works" mentality and recognize it as the critical asset that it is.

Threat actors commonly compromise Active Directory and then destroy backups because many of the on-premises backup systems depend on Active Directory. If they cripple Active Directory, either you can no longer log into your backup system or the threat actors can go in and destroy your backups. Alex Weinert, who is responsible for all of identity security for Microsoft, says that ransomware attacks are really the second phase in a campaign. The first phase is identity compromise.

THE SEMPERIS APPROACH

FIELD: How does Semperis help organizations to hone ITRD, particularly in alignment with the NIST Cybersecurity Framework?

DEUBY: Humans like to collect their problems in terms of a framework. It makes life easier. We align our products to the NIST Cybersecurity Framework. The first phase of the cybersecurity framework is to identify the threats, so we use Forest Druid and Purple Knight to identify your vulnerabilities. The next step is to protect; we protect the environment by remediating those vulnerabilities. There are a variety of ways to do that.

The third step is to detect unauthorized activity. Our Directory Services Protector product analyzes changes and shows you all of the changes that are going on in on-premises Active Directory and Azure Active Directory, as they're happening. We tap into the Active Directory replication stream, which is the

> **"Most Active Directory environments have horrible governance because Active Directory just works and people don't pay attention to it. But we need to scrutinize it and bring it into the fold and recognize it as the critical asset that it is."**

untamperable source of truth of what is going on in AD. So, a threat actor can't hide their actions. They can erase logs and do this or that, but we can see every change that's being made in Active Directory.

The fourth step in the NIST Framework is to respond. You have the ability to either manually or automatically roll back unauthorized changes to Active Directory that a threat actor might make or mistakes that an Active Directory administrator might make. This is where we use Active Directory Forest Recovery to take a backup of an organization under attack, isolate it, and threat hunt with the isolated copy of Active Directory and a tool called Active Directory Purple Knight Post-Breach. It looks for the attack paths and comes up with a method using of PowerShell scripts so that you can immediately kick the threat actor out of the production environment.

The final step is to recover. Our Active Directory Forest Recovery process enables you to recover your forest in minutes or hours instead of days or weeks and to do it malware-free into a variety of systems. If the worst comes, it enables you to quickly recover your environment and then start working on getting everything else back.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

iSMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io