Cybersecurity, Identities, People & Process:
A Crucial Integration for the Modern Identity SOC

simeio
Identity, intelligently managed.

WHY BREACHES HAPPEN & HOW SIMEIO CAN HELP

Strengthening the Weakest Link

There's a reason certain adages stick around long enough to become clichés. "A chain is only as strong as its weakest link" is one that certainly fits that bill. Any system, any process, is only as secure and stable as its most vulnerable area.

This is especially true when it comes to cybersecurity. Organizations know they need to invest in firewalls, data loss prevention (DLP), SIEM, and anti-virus/anti-malware. They understand that in this extremely digital age, the biggest threats to an enterprise aren't traditional business dangers like physical break-ins or obtaining a global reach. It's cybersecurity. Keeping the digital wolves at bay, keeping your company safe.

But one area of cybersecurity that's often overlooked – or treated as an afterthought – is identity security. This could be a costly mistake. More specifically, traditional network edge tools can't protect you anymore as workloads and company data exist on-premise and in the cloud. Additionally, hackers are targeting legitimate user and privileged credentials, which are supposed to allow legitimate users to access systems wherever they exist.

"Identity-context" is needed to correlate user activities across environments. In many respects– identity has become the new security perimeter.

The hard truth is that no matter how strong your firewall or how sophisticated your anti-virus software may be, once a hacker has access to a privileged account, your security is at risk. Enormous risk.

Identity management is at the heart of all security efforts. Implementing smart, experienced identity management solutions and services is what make the difference between a fully secure enterprise...and one that ends up on the home page of the national news. (And not in a good way.)

Identity and Access Management (IAM) is about so much more than creating email accounts for new employees and remembering to delete them when they leave the company. To get it right, companies need to understand the complexities and nuances of what it really means to secure their identities.

More importantly, they need to have the tools in place to manage all these moving parts, permissions, and levels of access. Oracle has recognized this shift in the security landscape and in customers' needs. Not only do we need to protect our own cloud, but our customers are looking for modern techniques to help them provide consistent security controls across all cloud and on-premise environments. A 2016 Right Scale study said enterprises plan to use an average of six (6) cloud services to run their workloads. Six! Now more than ever, coordinated, simplified security management is needed. Oracle is making a big investment in the world's first Identity-based Security Operations Center (SOC) framework.

The Identity SOC framework includes new security cloud services that integrate several technologies into one homogeneous set of services. These integrated technologies include Security Information and Event Management (SIEM), User & Entity Behavior Analytics (UEBA), Identity Management (IDM), Cloud Access Security Broker (CASB) and Compliance. Each of these new services will integrate with the rest of your security fabric, but when joined together they offer the full benefit of a true Identity SOC with bi-directional controls and actionable intelligence. But before we talk about the Identity SOC and why it's important, let's first talk about each solution: Oracle Security Monitoring and Analytics Cloud Service (SIEM), Oracle CASB Cloud Service, Oracle Identity Cloud Service, and Oracle Configuration & Compliance Cloud Service. (*Continued*)

The Right SOC Tools

Oracle Security Monitoring and Analytics Cloud Service: Security Monitoring and Analytics Cloud Service acts as an aggregation point for the enterprise, providing real time monitoring with pre-defined correlation rules, sensors for every major enterprise endpoint, and advances in machine learning and data science to drive threat detection, which is critical in a world where rules and policy authoring has its typical limits.

Oracle CASB Cloud Service: Identified by Gartner as a top 10 cybersecurity technology for 2016, CASBs provide granular visibility to every interaction taking place in the cloud, and provide fine-grained control to protect against threats that originate from or proliferate into the cloud. CASBs often include big-data analytics engines which allow for mining massive amounts of data, delivering surgical insights that streamline downstream forensic analysis. And with more enterprise data in the cloud -- and mission critical workloads being moved to the cloud faster than ever before -- a reliable CASB is fast becoming an integral service in a modern SOC.

Oracle Identity Cloud Service (IDCS): Oracle's next generation comprehensive security and identity platform. It is both cloud-native and designed to be an integral part of the enterprise security fabric, providing modern identity for modern applications. IDCS provides a powerful set of hybrid identity features to maintain a single identity for each user across their on-premises and cloud services while delivering a seamless user experience.

Oracle Configuration and Compliance Cloud Service: Oracle Configuration and Compliance Cloud Service enables the IT and Business Compliance functions to assess, score and remediate violations using industry standard benchmarks in addition to your own custom rules. The Oracle Configuration and Compliance Service can assess both on-premises and cloud infrastructure. This service is built on Oracle Management Cloud's secure, unified big data platform.

A New, Single Pane

A suite of powerful tools needs an equally powerful, efficient way to monitor them all. Simply, effectively. One single, efficient pane of glass to peer through and view all systems at once. A view that correlates events across all systems (on-premises and in the cloud) and ties them together with identity context. The traditional SOC (Security Operations Center) tools provide device management and monitoring services for firewalls, intrusion protection systems, proxies, and other perimeter and preventative security technologies. Alongside change management and maintenance of security devices, monitoring system logs and events historically use a security information and event management (SIEM) platform.

The Identity SOC framework is an identity and context-aware intelligence and automation solution. It provides the agility that is needed to detect and respond to advanced threats and persistent attacks and to provide a feedback loop for adaptation and evolution. The Identity SOC must protect users, applications/APIs, content/data as well as workloads. The Identity SOC utilizes optimized dashboards and risk consoles for security professionals that is bringing in feeds from throughout your environment. Identity SOC is a great, and necessary, solution. Better still, it solves for the challenges presented by a traditional SOC: information overload, not enough skilled resources and a gap in intelligence and automation. (*Continued*)

Cybersecurity, Identities, People & Process:
A Crucial Integration for the Modern Identity SOC

simeio
Identity, intelligently managed.

WHY BREACHES HAPPEN & HOW SIMEIO CAN HELP

The Power of People and Process

Once you have the right suite of tools, how will you direct them to focus on the right identity risks? Who is going to do the monitoring? Should you keep it internal or seek outside help?

There's so much more to consider -- beyond what tool or software to invest in. Who will help you prioritize what and when applications and identities move to the cloud? To answer that laundry list of questions, you first need to answer the following questions:

- Do you have the IT resource bandwidth to handle the monitoring?
- Does your IT team have the right expertise to do so?
- Do they have the cutting-edge industry knowledge to keep on top of updates and trends and new threats?
- Do you have detailed run-books that procedurally define effective responses to particular threats?

If you're like most companies, the answer to at least one of these questions is no. Especially the question about having the right expertise to help. And you're not alone if you have a hard time finding candidates who can handle your cybersecurity needs! According to the Information Systems Audit and Control Association, more than 1 in 4 companies report that the time to fill priority cyber security and information security positions can be six months or longer.[1] It's just a fact.

The amount of intrinsic knowledge, experience and responsiveness that a skilled, staffed-up service provider can supply is all but impossible for one single company to be able to replicate. Know how. That's the value Simeio can provide, and does provide to over 200 clients (and over 100 million identities) worldwide. They provide the expertise. They provide the people.

From assessment to integration to monitoring to updating, Simeio solves security problems for their customers, every single day.

And it's not just the number of identities they protect that's impressive -- it's the huge span of services they provide. Simeio serves as your Identity SOC. They have the people, the skillset and multiple, global operation centers. These "Identity Intelligence Centers (IICs)" are like "mission control centers" with Simeio staff monitoring and protecting their customers' systems for potential hacking activity, day and night.

Simeio Solutions has completed a SOC 2 Type 2 examination, demonstrating its controls relevant to Security, as well as having achieved ISO 27001 certification showing a comprehensive business management system to detect, evaluate and treat information risks effectively. What do these certifications mean? It means they are serious about identity security! Simeio works with security technologies, on premise, in the cloud or hybrid environments. The solutions are scalable to hundreds of millions of identities: Employees, Customers, Citizens, Partners and Devices. They can and will work on any identity need a client might have.

Simply put -- if the question is identity, Simeio's answer is "yes."

[1] ISACA's "Survey: Cyber Security Skills Gap Leaves 1 in 4 Organizations Exposed for Six Months or Longer"