Large European Retailer Turns to BloodHound Enterprise

Visibility and Remediation Guidance Changed How HEMA Secures Identities

CHALLENGE

HEMA, a leading Dutch retailer since 1926 with over 19,000 employees and more than 750 stores in five countries in Europe, takes cyber security seriously and understands the risks posed by adversaries. Protecting their organization and their customers' Personally Identifiable Information (PII) is a challenging job made even more complex by three distinctly different environments to protect: Stores, Distribution Centers, and Corporate. Each environment has different demands and policies that must be enabled by Microsoft Active Directory (AD) and Entra ID (Azure AD).

HEMA's Chief Information Security Officer, Hugo van den Toorn, immediately began to focus on Identity Security. "We run routine penetration tests and quickly address the findings, but these efforts only illustrate what is possible and don't provide a holistic view of where we can improve our identity security posture", said Hugo van den Toorn.

A long-time user of BloodHound CE (previously BloodHound Legacy), van den Toorn was familiar with what BloodHound CE could do but he knew HEMA needed to scale beyond using CE for their defensive measures and turned to BloodHound Enterprise to provide continuous visibility needed by HEMA for their diverse environments.

SOLUTION

It took less than two months to evaluate BloodHound Enterprise and license the solution. The evaluation was run in HEMA's production environment and immediately provided visibility like they never had before. To be fair though, van den Toorn wasn't surprised by the level of visibility BloodHound Enterprise provided, "I had heard of BloodHound Enterprise's capabilities and knew our team would see the value immediately."

"The part I had to see to believe is BloodHound Enterprise's remediation guidance. The identification of the strategic choke points where we can quickly improve our security posture along with the clear, unambiguous recommended remediation steps written in the language our IT Operations teams utilize day in and day out is fantastic. Along with our security team, our AD and Entra ID teams have direct visibility into the BloodHound Enterprise dashboards. As such, the operations teams can take quick remediative actions and get a better understanding of the risks their environments are exposed to", van den Toorn stated.

HEMA's IT Operations teams appreciates BloodHound Enterprise's ability to serve both the security and operations teams. The security organization is able to understand where the biggest risks of lateral movement and privilege escalation while the AD and Entra ID teams can now visualize the root problem and have clear instructions on how and where to strategically mitigate to remove privileged access risks.

CUSTOMER BENEFITS

Unprecedented visibility into Active Directory & Entra ID: Visualize privileges for instant clarity on AD and Azure AD architecture.

Best practices made practical: Achieving and sustaining Tiered Administration, Least Privilege, and Credential Hygiene are now possible.

AD and Entra ID security for everyone: Harden Active Directory and Entra ID against abuse and improve directory services availability.

Elimination of 'band-aid' fixes: Directly address the risk of Attack Paths at precise Choke Points rather than fighting misconfiguration debt.

Measurably improved security posture: Meaningful, transparent measurements that illustrate the risk reduction gained from Attack Path Management.

BLOODHOUND ENTERPRISE

HEMA

> **"With BloodHound Enterprise we can visually see the differences of our three unique environments and their group structures, allowing us to improve our security posture quickly."**
>
> **– HUGO VAN DEN TOORN**
> *Chief Information Security Officer, HEMA*

USE CASE	TECHNICAL CAPABILITIES	CUSTOMER BENEFIT
Enterprise-grade solution with minimal maintenance.	Delivered as a full SaaS solution with REST APIs, User Management, built-in training, reporting, signed binaries for local data collection, and enterprise support model with assigned customer success technical account manager.	Minimal setup and zero ongoing maintenance.
Continuous visibility of all AD and Entra ID Attack Paths.	Fully automated real-time data collection and analysis with Attack Path identification, prioritization based on Tier 0 exposure percentage, and risk trend reporting over time.	Always aware of AD and Entra ID exposure with real-time updates to environmental changes.
Empirical Attack Path Exposure for the security team and C-Suite.	BloodHound Enterprise creates a baseline of AD, identifying each Attack Path and the number of users/computers that can traverse the path. Then as AD changes are made, BloodHound Enterprise continuously measures and reassesses the overall risk.	Enterprises understand the current state security posture of their AD and Entra ID environments and as they make improvements can see their posture improve.

BLOODHOUND ENTERPRISE: MAP ATTACK PATHS TO MANAGE IDENTITY RISKS

From SpecterOps, experts on adversary tradecraft, and the creators of BloodHound CE used by penetration testers worldwide, BloodHound Enterprise delivers a first-of-its-kind platform to manage identity risk in your hybrid environment. BloodHound Enterprise constantly identifies the most strategic and impactful Attack Path choke points and gives you practical, precise, and safe remediation guidance to eliminate millions of abusable pathways.

BLOODHOUND ENTERPRISE PROVIDES:

- Continuous, Comprehensive Attack Path Mapping
- Empirical Impact Assessment of Attack Path Choke Points
- Practical, Precise, and Safe Remediation Guidance
- Continuous Empirical Security Posture Measurement

Learn more at **bloodhoundenterprise.io**

SpecterOps was founded with the belief that only with true knowledge of how adversaries operate, will organizations be able to defend themselves against the devastating effects of modern attacks. Organizations with a comprehensive understanding of how adversary capabilities and methodologies can be utilized against their environments, and how to detect those activities, can gain crucial confidence in the safety of their most critical assets and data.

SpecterOps
100 North Pitt Street
Alexandria, VA 22314
info@specterops.io

BLOODHOUND
ENTERPRISE