KuppingerCole Report

WHITEPAPER

by Martin Kuppinger | November 2015

Protecting the keys to your kingdom against cyber-attacks and insider threats

All organizations today are under constant attack, and high-privilege accounts are a primary target, allowing attackers to cause maximum damage due to the elevated privileges. While external attacks increase, internal attacks remain at a high level – perimeter security in itself does not protect sufficiently anymore. Privilege Management is a must for any organization.

by **Martin Kuppinger**
mk@kuppingercole.com
November 2015

Commissioned by Thycotic

Content

Table of Figures

Related Research

Leadership Compass: Privilege Management - 70960

Snapshot: Thycotic Secret Server - 70633

Vendor Report: Thycotic - 71112

1 Introduction

Privilege Management is a must for any organization today. Internal attackers abusing their entitlements and external attackers hijacking internal accounts with elevated privileges put every organization at risk. The challenges range from the theft and leakage of sensitive information and intellectual property to attacks which put parts of the IT infrastructure out of order. With smart manufacturing and with the ever-increasing shift towards everything and everyone becoming connected, the number of attack targets, attack surfaces, and attackers will continue to grow.

Privilege Account Management is by far more than just managing a few administrators within a particular system environment. It is about all systems and a variety of account types on these systems. Thus it requires not only functionally comprehensive solutions, but approaches that work for all types of organizations and an ever-growing number of users.

Setting up Privilege Account Management nowadays is a #1 requirement for mitigating Information Security risks and improving cyber-attack resiliency. This requires understanding the Privilege Account Management Challenge and setting up an action plan that covers not only technical but also organizational aspects and supports the entire Privilege Account Management cycle. This whitepaper explains the challenges, describes the Privilege Account Management cycle, and looks at the major elements of a Privilege Account Management action plan.

Thycotic with its Secret Server product is one of the leading providers of Privilege Account Management solutions, delivering a product that is focused on rapid implementation and easy use while covering both a broad and deep set of functionality at the enterprise level.

2 Highlights

- Privilege Account Management Challenges: Types of attackers, types of accounts, anatomy of attacks
- Privilege Account Management Cycle: Covering all challenges, beyond point solutions
- Building Blocks of Privilege Account Management solutions
- Thycotic Secret Server: Lean, rapid-to-deploy, yet comprehensive and enterprise-ready tool for Privilege Account Management
- Privilege Account Management action plan

3 The Privilege Account Management Challenge

All organizations are subject to attacks, by both internal and external attackers. Privileged accounts, i.e. accounts with elevated entitlements, well beyond shared administrative accounts, are a primary target. They allow for more advanced attacks, causing more damage, granting access to more data, etc. Organizations most know, manage, and protect these accounts. Too many of these attacks remain undetected or are identified too late, allowing attackers to run advanced persistent attacks.

It is a fundamental misbelief that any single organization might not be a target of attackers. Every single connected system is a target today. Attackers constantly run automated attacks, either to directly place malware on systems or to identify entry points to networks for more advanced attack scenarios. Small and medium-sized organizations, even in non-critical industries, not only are a potential victim of blackmailing and other scenarios, but might just become a stepping stone for attacks on other organizations.

Don't ignore the insider

Attacks are performed by both internal and external attackers. While today's main attention is on external cyber-attacks, the reality is that not only has the number of internal attacks remained stable at a high level, but several of the most prominent and severe incidents of the past years, in particular around information leakage, have been caused by internal attackers. Whether it is the theft of data relevant to tax fraud investigation from Swiss banks; the Wikileaks case; or the Snowden revelations: All of these were performed by insiders. There is no reason to underestimate the risk caused by external attackers – but there is also no reason for ignoring the insider threat.

Furthermore, a primary target of all advanced types of external attacks is hijacking internal, privileged accounts. Malicious insiders generally already have access to such accounts or can find ways of elevating privileges of accounts they are entitled to use. At the end, both internal and external attackers have one simple primary target in their attacks: Gaining access to privileged accounts, allowing them to "successfully" execute their attacks.

It's not only about the root account

Privilege Account Management is bigger than most people believe. It is not only about managing the root account on Unix or Linux machines or the Admin account on Windows machines. It is not only about administrators. It is about a vast number of accounts across all systems and services in the IT environment, not only on premises but also in the cloud.

Furthermore, Privilege Account Management doesn't only cover shared accounts. These are a major challenge, due to the inherent security issues associated with shared use of accounts by various persons, but Privilege Account Management is about more. Figure 1 displays the two main dimensions of Privilege Account Management. While there is the challenge of managing shared accounts, displayed on the x-Axis, there is also the challenge of correctly dealing with accounts that have elevated privileges. These commonly include individual accounts that are assigned to an individual user. However, these accounts e.g. might be hijacked and fraudulently used for attacks.

Privilege Account Management is not only about shared accounts

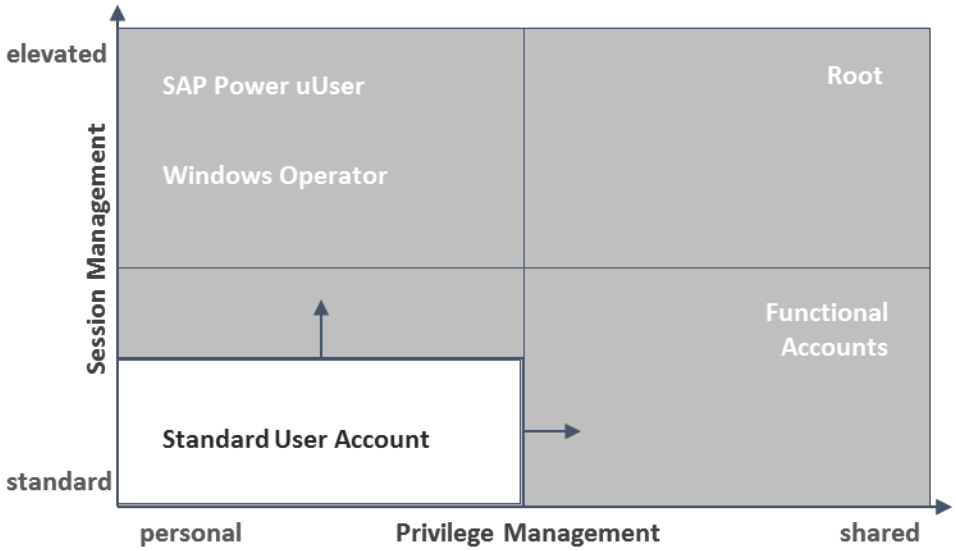

Fig. 1: Privilege Management is not only about shared accounts.

A frequently underestimated aspect of Privilege Account Management is the breadth of systems and the variety of accounts that are concerned. Network components, host operating systems, hypervisors, guest operating systems, all the layers within applications, but e.g. also all the system accounts on client systems and the various operators and administrators in cloud environments are in the scope of Privilege Account Management.

A special variety are technical or functional user accounts, which are a perfect sample for privileged accounts from two angles. On one hand, they commonly are both shared and privileged in the sense of having elevated privileges. The latter is just due to their nature – systems operate activities for many users through these accounts, thus they must have the superset of entitlements of all these users. On the other hand, functional accounts are commonly weakly managed, if at all.

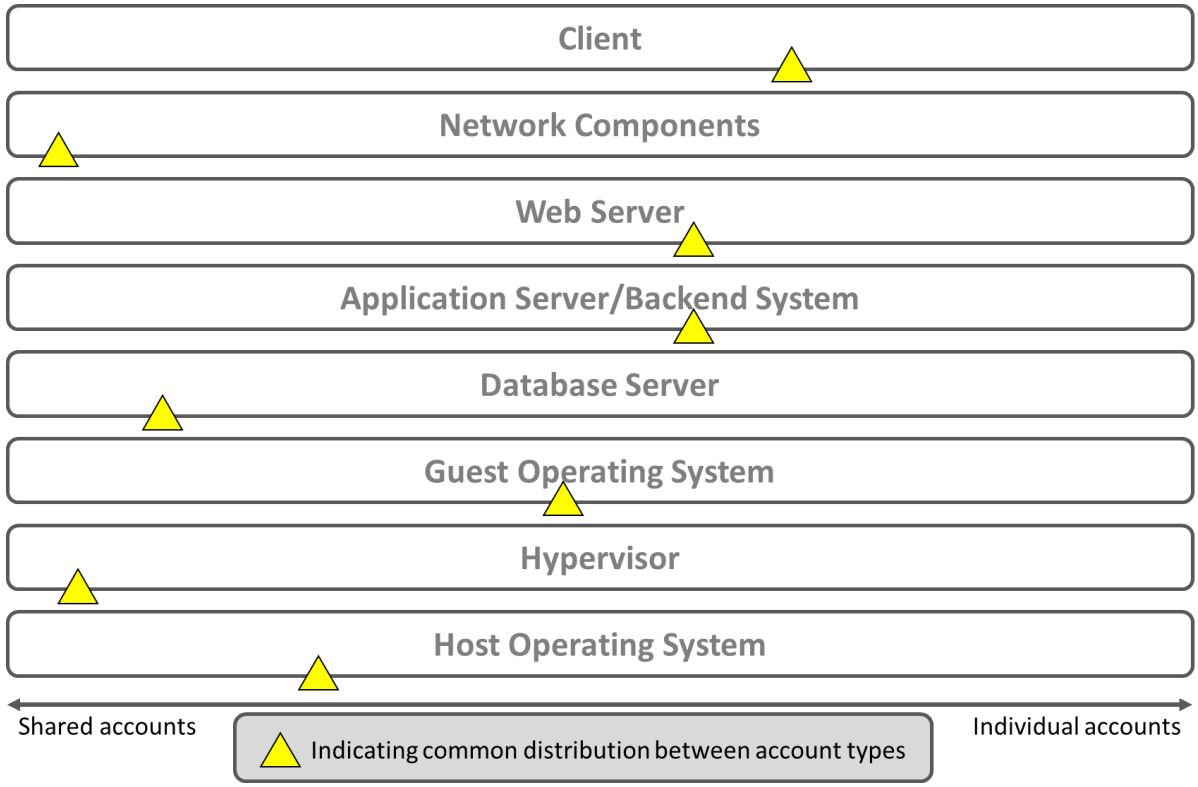

Fig. 2: There are far more privileged accounts than most people expect – at all levels of the IT infrastructure.

Don't forget to identify all the built-in accounts

Another common sample of vastly ignored yet sensitive accounts are local system and service accounts. These are a common attack target, using Zero Day Attacks or just building on the fact that many systems are under-managed and rarely patched. Simply said: Privilege Account Management is about far more than just a few administrators, it is a challenge that affects all systems and a multitude of user accounts.

The attackers are already in

Perimeter security is fine as a first line of defense. However, it does not solve the Privilege Account Management challenge. Consider the attacker is already in your network. Obviously, that is the case for the internal attacker. While internal attackers are widely ignored and many organizations still focus on perimeter security, internal attacks account for massive damage. Moreover, in these days of increased mobility, cloud computing, and thus de-perimeterization, we just do not have the single, closed perimeter anymore where we can set up our defense. We must protect at core. A major element therein is limiting and controlling the use of privileged accounts.

Over the past years, a variety of attacks have been publicly described. The "anatomy of attacks" is increasingly well-known. While the attack vectors in use vary and new Zero Day attack vectors appear more or less on a daily basis, there are basically two approaches for attack. One is trying to use weaknesses for placing malware on systems, for "direct use" such as botnets, blackmailing, etc.

The other approach is what is commonly called Advanced Persistent Threats (APTs). While the term might be questioned, the concept is a challenge for any kind of organization and displays perfectly well the need for protecting privileged accounts.

External attackers try hijacking privileged accounts

Such attacks commonly start with social phishing or attacks relying on so-called Zero Day attacks – sometimes using still unknown ("before day zero") vulnerabilities. Often, system-level accounts with elevated privileges at local level or subsequent privilege elevation are the scope of this initial attack. Once first systems are affected, the attacks try to sprawl and gain access on accounts with elevated privileges. The target is control of privileged accounts. These hijacked accounts subsequently are used for the attack, delivering data back to remote servers. Some of these attacks are known to have been running several months or even years, before they were detected. It is simply naïve to believe that all attacks are detected.

But regardless of which type of attack you look at privileged accounts are at the center of attention of every attacker, be it internal or external. Thus, adequately protecting such accounts and identifying and blocking abuse is a mandatory element in every strategy for increasing cyber-attack resiliency.

The main challenges of Privilege Account Management

Privilege Account Management is a challenge for any organization. When implementing or expanding a Privilege Management approach, organizations must focus on covering the entire "Privilege Account Management Cycle":

- **Understand** the need for Privilege Management and its breadth and depth;
- **Identify** privileged accounts across all systems;
- **Protect** access to privileged accounts and restrict use;
- **Monitor** privileged account use;
- **Detect** anomalies in privileged account use indicating potential fraudulent activities;
- **Respond** to privileged account on time and with targeted actions;
- Continuously **improve** your Privilege Management.

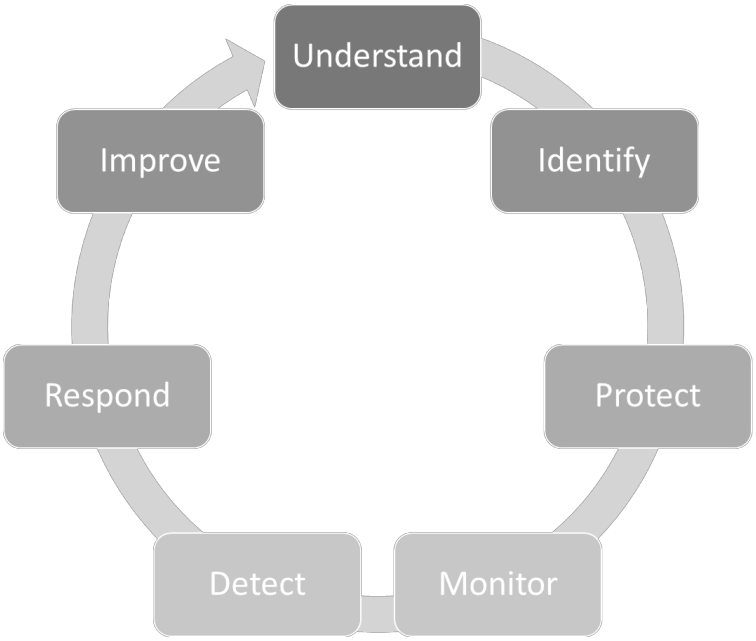

Fig. 3: The Privilege Management Cycle.

Major questions organizations should raise for themselves are:

- Do we know about all our privileged accounts?
- Do we protect all privileged accounts?
- Do we manage all privileged accounts?

If the answer to any single of these questions is “no”, organizations should start defining their Privilege Account Management strategy and implementation.

4 Elements of a Privilege Account Management Solution

Privilege Account Management is not about a single technical approach. Consistently managing privileged accounts across their entire lifecycle and covering all use cases for protecting privileged accounts requires implementing a number of capabilities in a coordinated and integrated manner.

While there is a multitude of terms vendors use for Privilege Account Management, there are a limited number of technical core elements that make up comprehensive Privilege Management solutions.

Privilege Management starts with Shared Account Password Management, but goes well beyond

As illustrated in figure 1, two main technologies address on the one hand the Shared Account Password Management and, on the other hand, Session Management. However, both key disciplines consist of a variety of capabilities, and are complemented by other technologies.

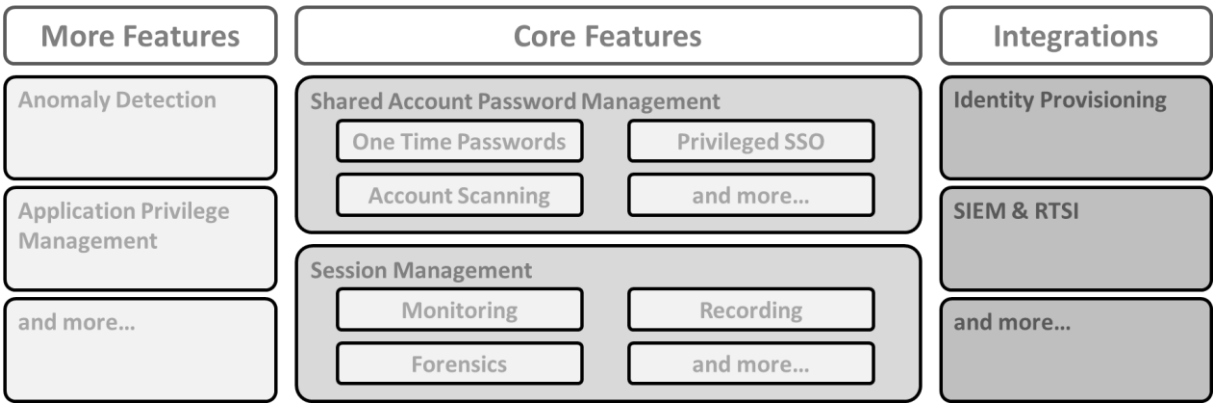

Fig. 4: Building Blocks of Privilege Management.

Shared Account Password Management is not only about one time passwords for accessing shared accounts, but also about Single Sign-On to multiple accounts a person is regularly using; detection and management of privileged accounts in distributed environments; integration with Identity Provisioning solutions for management of the ownership of shared accounts; and strong authentication support for accessing the Privilege Management solution itself.

Session Management includes capabilities such as Session Monitoring, Session Recording, and the ability to intercept sessions. Furthermore, there are a multitude of technical challenges, ranging from analyzing sessions using graphical user interfaces to covering specifics of complex server infrastructures using jump hosts or managing SSH keys for these sessions as well.

Aside from the core feature set, there are other areas. An increasingly popular field is anomaly detection, which can be addressed specifically for privileged accounts or more generally for all users. Another capability is Application Privilege Management, supporting both externalization of credentials in applications and scripts from code, and secure use of credentials in application-to-application communication.

Anyway, implementing Privilege Account Management capabilities commonly happens in a phased approach, supported by setting up the guidelines and organization. Selecting the right tool is about finding a solution that has sufficient functional breadth and depth while also supporting flexible integration with other elements of the IT infrastructure such as Identity Provisioning, SIEM (Security Information and Event Management), or RTSI (Real Time Security Intelligence). Furthermore, Privilege Management is no longer for a few users, but increasingly for the masses. Thus, these tools must support simple roll-out, given that administrators, operators, and privileged non-IT users across the organization might need to use at least some features of these tools.

5 The Thycotic approach to Privilege Account Management

Thycotic is one of the leading vendors in the Privilege Account Management market. The company's Secret Server product combines a strong feature set with a rapid deployment approach and an easy-to-use interface, supporting Privilege Management as a widespread activity not being limited to few administrators.

Thycotic is a US-based vendor in the Privilege Account Management market. The company started with providing solutions in the field of Windows Server management. From there, their Secret Server product – the key product of Thycotic – evolved towards a comprehensive Privilege Management solution covering a wide variety of target systems. While the product still runs on Windows Servers and makes use of capabilities provided by the Microsoft Server platform, it supports a range of target systems, including network devices, Unix, Linux, and hypervisors as target systems.

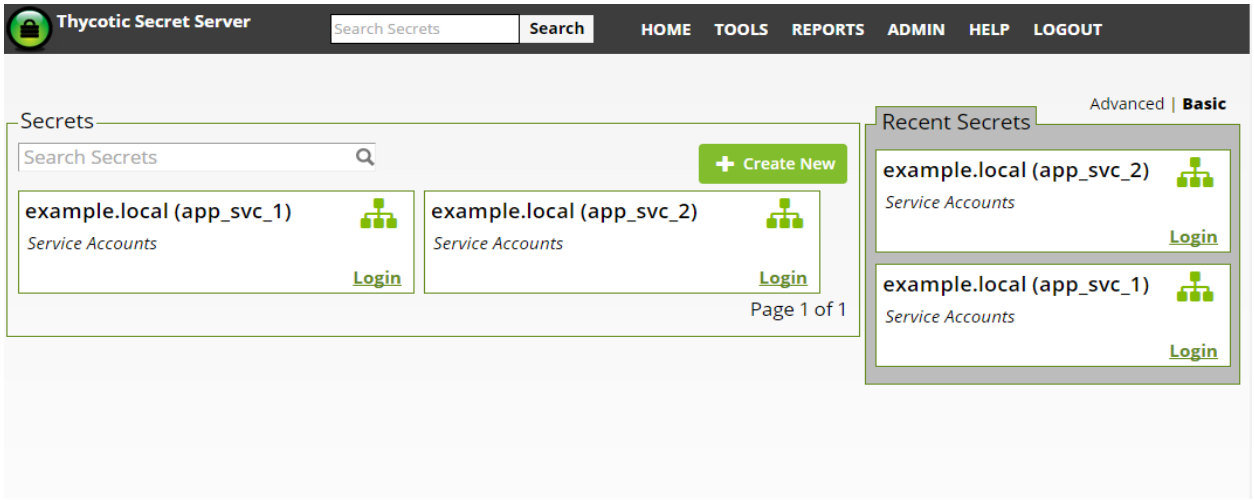

Fig. 5: Thycotic combines a comprehensive feature set with an easy-to-use user interface.

Thycotic has lean and rapid-to-deploy solutions in its DNA

Thycotic, in contrast to several other vendors, has been focusing on rapid and simple deployment and an easy-to-use user interface from the very beginning. One reason for that is the sales model that Thycotic had implemented initially: Thycotic focused on direct telephone and Internet based sales instead of traditional field sales either through their own sales teams or partners. In such a model, an

approach that is lean regarding required professional services efforts and support is mandatory. With today's shift of Privilege Account Management from being merely an administrative tool for a very limited user population to a far broader range of use cases, Thycotic benefits from that "lean DNA". Furthermore, with Privilege Account Management becoming a challenge for virtually any organization, it has to be simple enough also for small and mid-sized organizations.

Nowadays, Thycotic continues with its traditional sales approach while complementing it rapidly growing partner infrastructure on a global scale, including some global consultancies being part of the partner ecosystem.

Having a lean approach (and, notably, competitive pricing) does not mean a lean feature set. From its roots in the Windows ecosystem, Thycotic Secret Server has grown to a product supporting enterprise requirements, including sophisticated support for globally dispersed environments, high availability, and failover in its latest release.

"Our IT administrators were able to get up to speed with Secret Server within minutes and our control over data security was improved immediately. By adopting a tool that manages our sensitive credentials for us, we no longer face the inefficiencies that can plague an organization as big as ours." (Michael Boeglin, Director of Global Infrastructure, International Rescue Committee)

Thycotic Secret Server supports the major areas of Privilege Management, including Shared Account Password Management, Session Management, Behavioral Analytics, and Application Identity Management. The product delivers a baseline feature set in all areas, with specific strengths in the core domain of Shared Account Password Management. Here, it supports discovery capabilities across not only Windows but also e.g. Unix and Linux systems. Furthermore, Thycotic Secret Server has extensive support for managed devices.

A specific strength is the broad set of APIs plus support for Microsoft PowerShell. The latter allows for managing target systems via custom PowerShell scripts, thus providing a lean and efficient way for rapidly adding integration for specific managed devices. Overall, Thycotic Secret Server has successfully matured from a Windows-centric entry-level solution for Privilege Management into an enterprise solution, while still emphasizing the strength of being a lean and rapid-to-deploy solution.

"We can't say enough about the Secret Server product and its ability to integrate with just about anything. With the use of APIs, scripting and automating is much, much easier now!" (Josh Shoefield, Senior Systems Engineer at Availity, an industry-leading, HITRUST-certified health care information technology company)

From the KuppingerCole perspective, Thycotic Secret Server is a clear pick for further evaluation when selecting a Privilege Management solution. It is of particular interest when competitive pricing, rapid deployment, and short time to value are required, while also supporting a variety of complex and specialized enterprise use cases.

6 Action Plan for Privilege Account Management

Privilege Management is a key activity in mitigating Information Security risks and increasing cyber-attack resilience. Thus it is not only about deploying a tool but also understanding the risks and implementing guidelines and organization alongside tool deployment.

As with any investment, management will question the value of setting up a Privilege Account Management infrastructure. While the threats by both internal and external attackers are obvious, a key success factor is concretely identifying and indicating the risks for not having a Privilege Management solution in place. These include data theft and leakage, violation of contracts with large customers, and violations of regulatory compliance requirements, to name just a few. Defining such risks not only demonstrates the need for investing in Privilege Management but also allows for measuring the success of a Privilege Management program.

> *„Auditors identifying the lack of Privilege Account Management immediately alarmed our C-level" (CISO, European Consumer Goods Company)*

Alongside selecting and implementing the tool(s), Privilege Account Management requires four other main elements:

- **Guidelines** for Privilege Management, from golden rules to concrete policies
- An **organizational structure** covering the entire breadth of privilege management use cases, beyond a certain technical domain
- The **people** running the Privilege Management environment, analyzing events, and responding to these
- The **interfaces** to other elements of the IT and in particular Information Security infrastructure, e.g. for further analysis of events or integration of shared account lifecycles with the user lifecycles managed by Identity Provisioning tools

The Privilege Account Management Cycle depicted in figure 3 is the starting point for an action plan which should result in both a functional tool as well as the necessary surrounding elements.

7 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

Kuppinger Cole Ltd.
Sonnenberger Str. 16
65193 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com