integrating

cutting-edge security technologies

the case for SIEM & PAM

logpoint
SIEM.
But different.

CYBERARK

Atos

Introduction

A changing threat landscape

The majority of organizations have basic security practices in place, such as firewalls, antivirus, patching processes, etc. This enables them to protect against most traditional threats. But what happens with the ones that slip through or when the threat landscape changes?

Historically, organizations have looked at security as point-solutions, in which you apply a certain technology in a certain place to solve a specific issue. This allows for rapid solutions to very specific problems and quick implementation of new services. Utilizing point-solutions to solve today's challenges is increasingly proving inadequate.

Instead of building a centralized model for authentication, authorization or tracking behavior and threats, most organizations delegate access to specific people within the organization and rely on a framework of trust. Often, these users have very wide access rights.

The actions taken by users and incidents created in these different tools are not collected, analyzed and evaluated in a broad view. As a result, things creep through the cracks.

A framework of trust

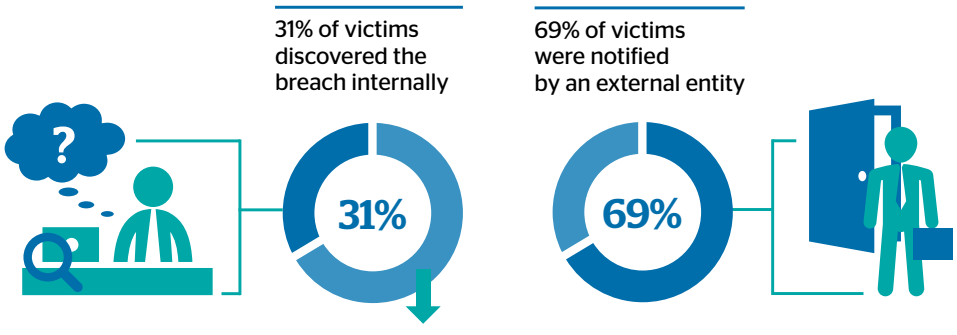
The framework of trust further places a burden onto the administrator. When something goes wrong, the focus naturally moves to the person with the privileges. Not to the incidents generated by the system, not to the actions performed or the manager assigning the privileges to the administrator.

A superior partnership

In order to address the above issues in a superior way, CyberArk, LogPoint and Atos entered a partnership. The partnership enables us to deliver integrated IT security solutions based on state of the art technology where business continuity is in focus.

"We help you understand your risk exposure and build your cyber security strategy."

Figure 1: How Compromises Are Detected



Down from 37% in 2012

*In 2014 we again experience an increase of companies that did not detect internally that they had been compromised- in 2012 = 37%, 2013 = 33 %, 2014 = 31%

The Kill Chain

Focus of the Kill Chain & the attacker

The Cyber Kill Chain is frequently used to describe the nature of cyber-attacks as well as the structure of an intrusion. Focus of the Kill Chain is on detecting ongoing attacks and changes in user- and computer behavior that indicate a breach. The Kill Chain establishes that regardless of whether organizations are dealing with an external or internal threat agent. One of the first steps is reconnaissance, where an intruder propagates the network and gathers information on accounts.

The next step is lateral movements inside the network, which occur when sufficient information has been gathered on relevant accounts to start exporting data or as jump point to compromise additional systems. This can take hours, weeks or months after first entering the network. This is the approach followed by most attack patterns. Intruders continue to move inside the network until they reach their desired destination, which in most cases are the servers and the domain controllers.

PAM & SIEM - working together

Privileged Account Management (PAM) can help prevent and detect this form of attack and the lateral movement is able to feed a Security Information & Event Management (SIEM) solution with enriched information on such activities.

Overall, an external attack with a breach of the perimeter can be detected with a SIEM solution, whereas an internal attack in which a user escalates privileges with a PAM solution is detected by the inherent functionality of the PAM solution. The lateral movement and in part the reconnaissance areas can be detected with a SIEM. The movement can be detected when the SIEM evaluates the logs and patterns of traffic that are being generated by the network nodes.

Once the intruder has reached the target within the network exploitation, escalation of privileges is required before data can be exfiltrated. Here PAM and SIEM can work together to identify the breach.

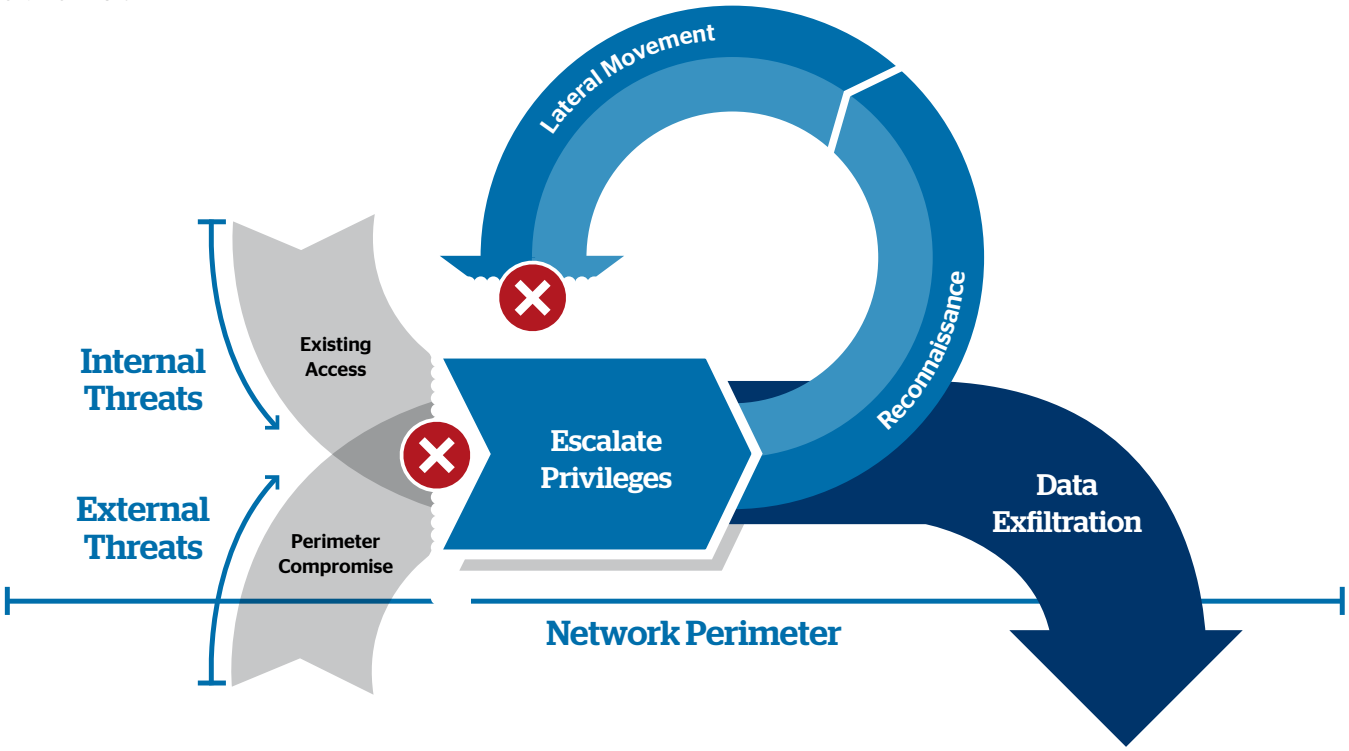
A Common Point of Entry

It is important to continuously monitor environments that are at risk for compromise. Attackers follow the path of least resistance, so pick solutions that support the varied components in your most at-risk environments. Targeted attacks may pick widely used operating systems or third party applications as their entry point. These attacks always involve privilege escalation, mitigated by employing CyberArk.

Once an attacker has an entry to the network, the attacker will move laterally in the network and identify the target of interest. This lateral movement can be detected by LogPoint. In essence the escalation, lateral movement and exfiltration can be identified by combining the technologies of LogPoint and CyberArk.

Overall, data exfiltration can be detected by using heuristics models in both PAM and SIEM by inspecting the flow of data moving out of the enterprise networks. Alerts will trigger if certain systems start communicating massive amounts of data to unusual destinations and when users start behaving differently than their colleagues, for instance moving sensitive data to removable media.

Figure 2: The Kill Chain



The LogPoint & CyberArk integration

Privileged Account Management

Full Visibility on Permissions
The use of the generic privileged accounts is created to be personally identifiable, which raises the value of a LogPoint implementation to an even higher level.

Operations Efficiency
The time spent on the administration of priviledged accounts is minimized and polices around these accounts are enforced by the system.

Authorisation Workflow
A full audit trail on usage of priviledged accounts provides the knowledge about every session and when and why this took place in addition to what happened during the session.

Security Information & Event Management

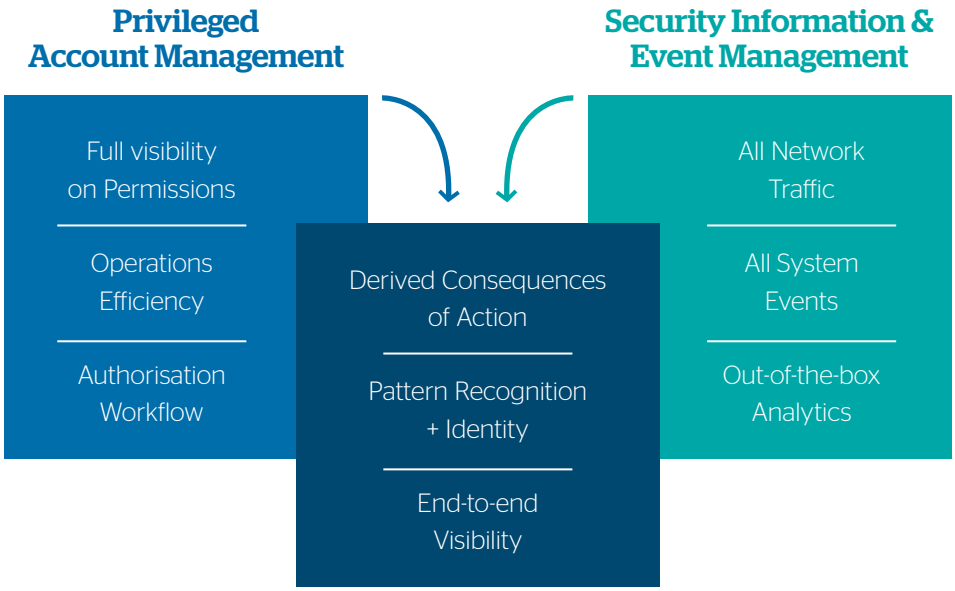
All Network traffic
Collecting flow information, logs from routers and firewalls, LogPoint can analyze patterns of activity and behaviors. With advanced analytics and correlations LogPoint can track malwares lateral movement in the network.

All System Events
All actions, changes and states on systems will be logged by applications and operating systems. This allows analysts and operators to quickly gauge and assess impacts and threats as they occur on their systems.

Out-of-the-box analytics
With ingested data from the network and the systems communicating over the network the final step is simply to use analytics. All practical use cases are supported out of the box with the easy addition of further analytics components.

"Protect your business from the inside with state of the art technology."

Figure 3: Benefits of the Logpoint & CyberArk integration



Output of integration between CyberArk and LogPoint

By integrating LogPoint & CyberArk you achieve a number of benefits

Derived Consequences of Actions
The combination of LogPoint and CyberArk provides the analyst with a tool chest that provides transparency above and beyond what can be achieved through manual processes and reviews.

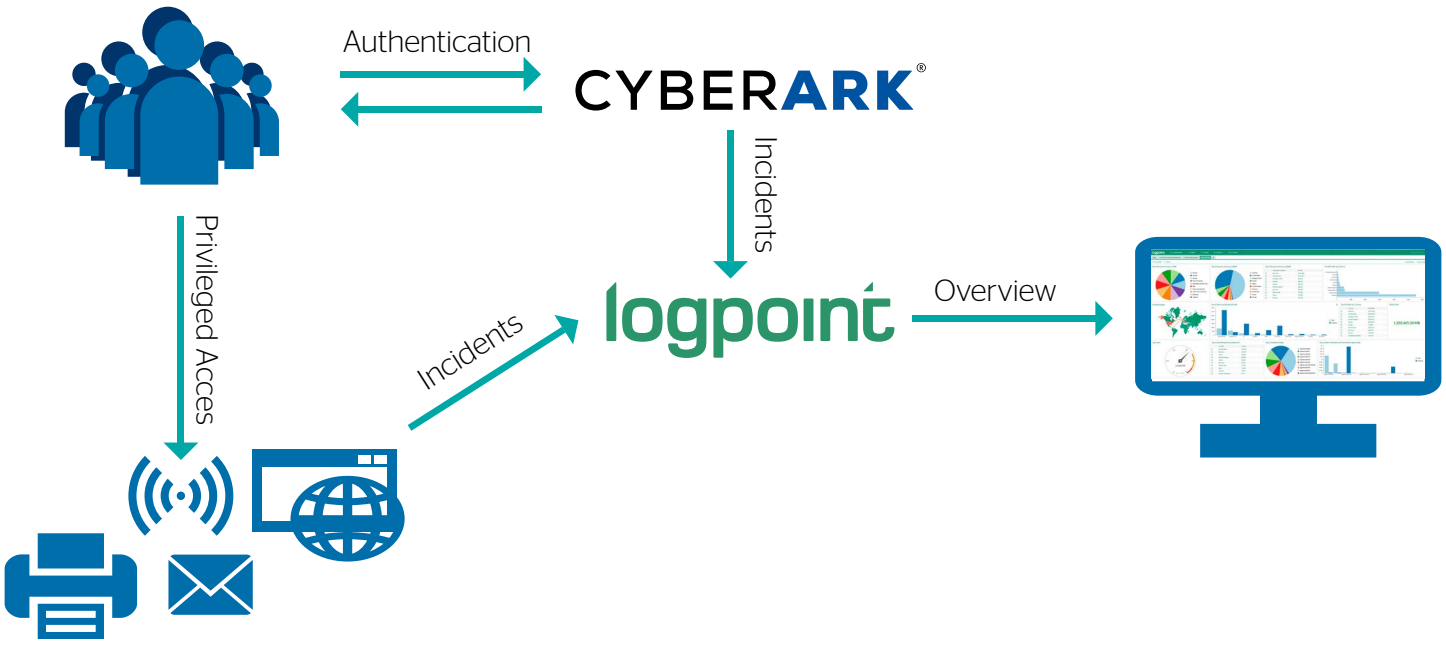
This is archived by combining knowledge about why actions were performed with the associated changes and consequences of these actions.

Pattern Recognition + Identity
With advanced pattern recognition and a clear insight into who and why an access was granted and utilized, insider threats can be tracked, dissected and stopped before data leaves the perimeter.

End-to-End Visibility
The insight gathered from systems, networks and the human aspect is the end-to-end visibility that most organizations with increasing complexities in their networks are seeking.

"Control and monitor privileged accounts and collect information on system changes and actions to minimize the risk of insider threats."

Figure 4: Integration between LogPoint & CyberArk



Atos' role

In the partnership with CyberArk and LogPoint

Atos' role is to ensure implementations where the business value is optimized from a client perspective.

This involves addressing the famous triangle where People, Processes and Technology all are taken into account (figure 6). The human firewall is as important as a piece of technology. In figure 5 you can see some of the typical areas within IT security where we are supporting our clients in successfully improving their level with regards to IT security.

Atos as advisor and executor

Our broad range of competencies and industry knowledge enables us to act in relation to customers' needs, while also reacting to changes that occur during projects.

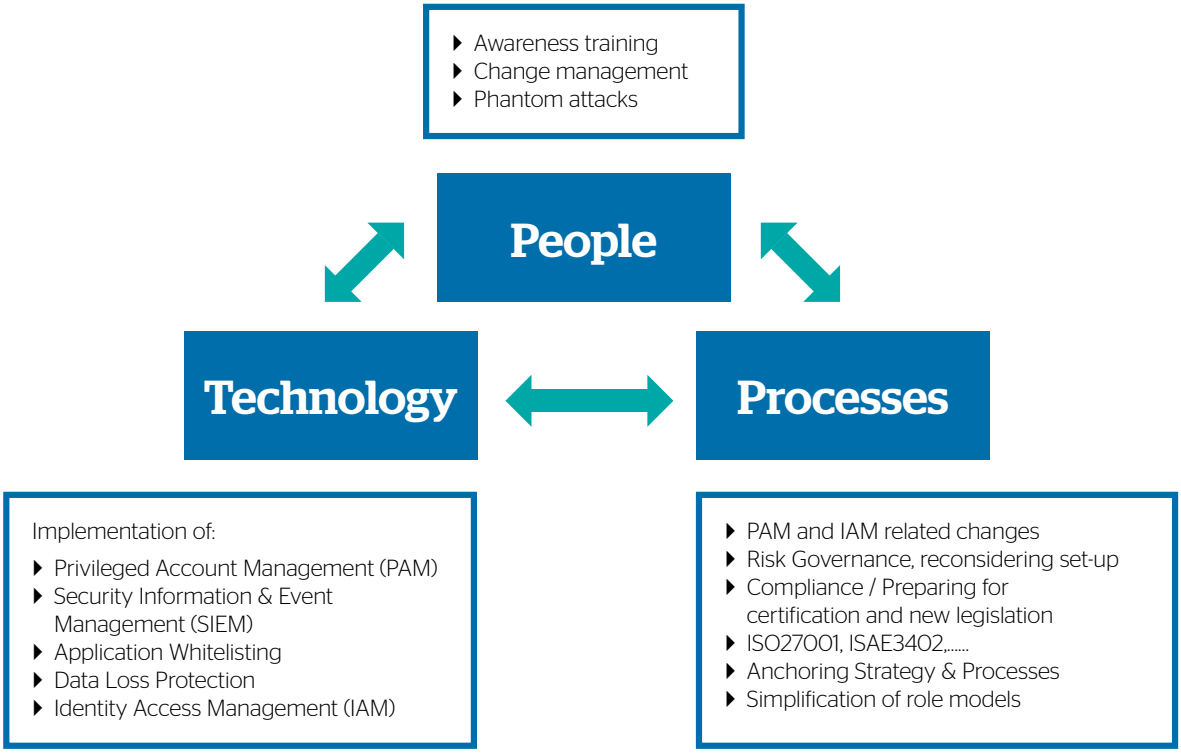
Our role in relation to this is often acting as both advisor and executor. After the commissioning we continuously support and operate the solution in order to optimize this in relation to the current threat landscape.

Olympic IT security

Our experience covers a wide variety of services to customers on a global and local scale. One of the most well-known, and in many ways challenging within the IT security area is our role as worldwide IT supplier at the Olympic Games.

Figure 5: Atos three cyber-security portfolio areas

Figure 6: How Atos supports clients with IT security



About LogPoint and CyberArk

About LogPoint

LogPoint delivers cutting edge features in the SIEM market space. The solution monitors the key system objects and components found in any organisation, including network equipment, servers, applications and databases. The solution provides a simple, transparent view into business events and allows businesses and government agencies to proactively safeguard digital assets, achieve compliance, and manage risk.

Contact one of our consultants for more information at email: info@logpoint.com
phone: +4570606100
homepage: www.logpoint.com

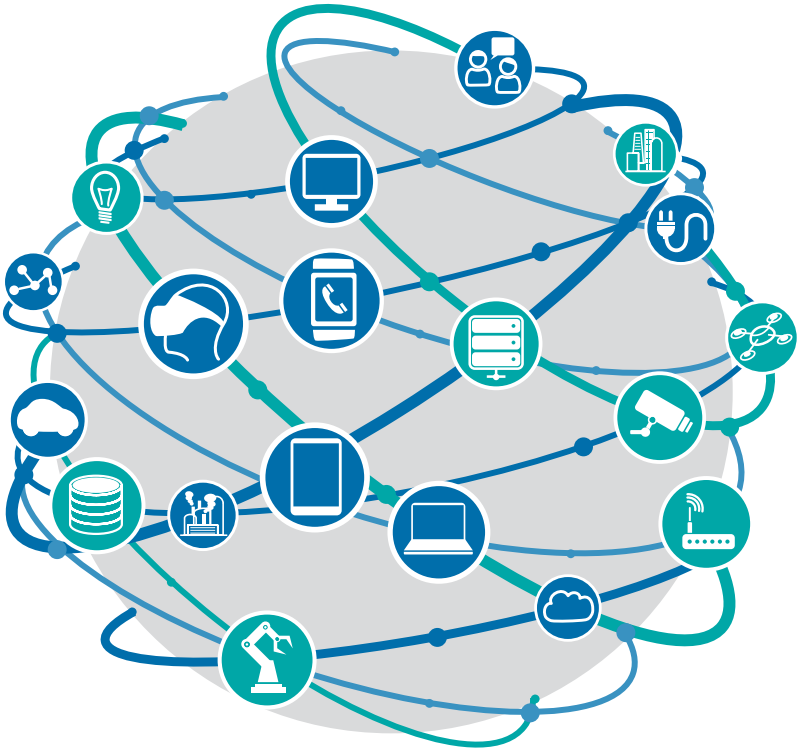
logpoint
SIEM.
But different.

About CyberArk

CyberArk is the only security company laser-focused on striking down targeted cyber threats, those that make their way inside to attack the heart of the enterprise. CyberArk's security solutions master high-stakes compliance and audit requirements while arming businesses to protect what matters most.

Contact one of our consultants for more information at email: info@cyberark.com
phone: +33 (0) 1 70 15 07 74
homepage: www.cyberark.com

CYBERARK®



About Atos

Atos SE (Societas Europaea) is a leader in digital services with 2014 pro forma annual revenue of circa € 11 billion and 93,000 employees in 72 countries. Serving a global client base, the Group provides Consulting & Systems Integration services, Managed Services & BPO, Cloud operations, Big Data & Cyber-security solutions, as well as transactional services through Worldline, the European leader in the payments and transactional services industry. With its deep technology expertise and industry knowledge, the Group works with clients across different business sectors: Defense, Financial Services, Health, Manufacturing, Media, Utilities, Public sector, Retail, Telecommunications, and Transportation.

Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and is listed on the Euronext Paris market. Atos operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, and Worldline.

Change to: For more information,
visit atos.net or contact Torben Krog at:
email: torben.krog@atos.net
phone: +45 23 70 46 77