Baseline Cybersecurity for the Australian Mining Industry

German Virtual Business Delegation to Australia

Online Conference with Focus on Mining Industry

October 20th 2020

DETACK

Structure

1. About Detack GmbH
2. Baseline Cyber Security (I) with COSMO*: Problem → Solution → Results → Feedback

   Case study: LEAG (Lausitz Energie Bergbau AG, coal mining, ~52 mil tonnes /y 2019)
3. Baseline Cyber Security (II) Password Analytics for critical infrastructure with EPAS**: Problem → Solution → Results

   Examples: Evonik Industries (speciality chemicals, €14 bn t/o) and Emirates Global Aluminium (bauxite mining, aluminium industry, $6 bn t/o)

* Continuous Object-based Security Management Operations

** Enterprise Password Assessment Solution

FACTS

- Privately held (2000~), founded in Bochum, Germany
- Ludwigsburg, Germany (2005~)
- R&D Arm: Praetors AG, Beckenried, Switzerland (2010~)
- Expertise: High-end IT security services & solutions
- Product portfolio: Cybersecurity consulting and solutions, R&D
- Business split: 75% solutions, 25% services
- Industry concentration to date: Finance, insurance, industry, energy…and growing
- We are here because we believe that our solutions – baseline IT object security and secure passwords – can help the Australian mining corporations to achieve compliance and increase their cybersecurity resilience

DETACK

2000
Founded

IT Security
Services
Consulting

2011 COSMO
2013 EPAS
Launch

EPAS
Patented
30+ Countries

Baseline Cyber Security (I) with COSMO

Case Study:

LEAG, a brand of Lausitz Energie Bergbau AG

©LEAG: https://www.leag.de/en/business-fields/mining/

- Lignite mining in the four opencast mines in the region Lusatia, Germany (second largest lignite district in Germany)
- Refining the run-of-mine lignite in the industrial park “Black Pump”
- The opencast mines of LEAG produced around 52 million tonnes of lignite in 2019
- LEAG promotes that “future-oriented energy technologies in the fields of renewables, storage and sector coupling and new energy and industrial services for the market to be developed by LEAG”
- More: https://www.leag.de/en/business-fields/mining/

The Requirement

- Lausitz Energie Bergbau AG (LEAG) baseline security must satisfy requirements dictated by industry regulations as well as internal and group policies.

- **Baseline security is the achievement of an adequate and appropriate level of security for IT systems; appropriate means that the industrial risk level / criticality must be always taken into account.**

- Very complex systems, made of various, often legacy, components must have a minimal cybersecurity level, i.e. reach the baseline.

- Each IT component must be verified on a regular basis, intervals depending on criticality, and remediated if non-compliant with the baseline security requirements.

- The process must be auditable and trackable down to the individual person who performs the verification and remediation.

- There must be no gaps in any industrial control zone; gaps would render the entire effort useless.

- Reporting and visualization of the current status, as well as the time-base evolution of each component security must be available for internal use and for external regulatory bodies.

The Challenges

- **No automation**: Because of the zoning model used in such environments, even basic automated endpoint security controls tend to fail, especially for the critical automation / closed loop systems which are located in isolated segments; there are many critical components that do not speak TCP/IP, and even when they do they are isolated, unreachable. That means people are needed.

- **No personnel**: Human assisted controls are also difficult and expensive to implement, as there are many distinct, specialized systems, often legacy, that require specialized personnel, and because of the typical plant / installation size, a lot of such personnel; it is hard to get 20-50 expensive cybersecurity specialists in the middle of nowhere and make them stay there.

- **No clear definitions**: Regulations are often confusing, regulators are influenced by the tech marketing hypes of the day, resulting in changing requirements and inconsistent remediation recommendations. Internal security control definitions are as good as the people doing them; even when they are stellar, they are often not updated for years, while the cybersecurity threats change daily.

- **Not enough coverage**: Efforts usually manage to reduce the risk in isolated areas, but because of limited personnel resources, we are left with large zones insufficiently covered, and this makes the entire effort futile. It simply takes too long to solve the problem.

The Solution

- ✓ The **internal policies**, **external regulations**, and any other **compliance requirements** are distilled into a consistent and technically viable cybersecurity concept that clearly defines the baseline requirements.

- ✓ All components are stored as **objects** in an inventory list, together with their **security classification** (i.e. malfunction can cause loss of life or injury, or just financial loss, or environmental impact, etc.), **industrial security zone**.

- ✓ The objects are assigned **properties**, such as O/S, vendor software, functions, etc., properties which are then reused for other objects once defined.

- ✓ Each property is mapped to a **template** which defines the infosec requirements and each requirement has a corresponding **checklist** which can be used by non-IT personnel.

- ✓ The **non-IT personnel** downloads selected checklists as **tasks** whenever they happen to have network coverage, then use the to **verify and remediate** the components under their supervision, over a number of days; once ready, the results are uploaded into the central database and the status of the objects updates.

- ✓ Updates in requirements or new threats are **automatically applied** to all objects and results in new checklists

The Result

- ✓ With COSMO we have created a **toolset**, that also incorporates the required infosec intelligence, to enable non-specialized personnel to verify and enforce baseline security controls across the entire environment, without leaving any gaps.

- ✓ That means that **existing personnel**, with basic computer knowledge, can perform all verification and remediation tasks to reach and confirm the baseline security level. A small team, local or remote, of highly competent cybersecurity specialists manages, controls, and updates the entire system.

- ✓ COSMO does **not touch** existing systems, requires **no permanent connectivity**, and runs on independent, rugged mobile devices that any employee can carry around: phone, tablet, laptop, including BYO.

- ✓ The personnel – typically non-IT engineers – use the mobile devices, even in areas with no Wi-Fi / mobile coverage, to **check and correct the security controls** at the same time and in a manner similar to inspecting any other type of machinery.

- ✓ The baseline security requirements have been reached since 2015, they are **constantly monitored and corrected**, and the regulators and management are happy. No big cybersecurity team has been hired, no intrusive software tools have been added to the operational technology network, no infrastructure changes have been performed.

The Feedback

Q: How important is software COSMO for the IT activities of LEAG?

A: Very important: the software defines the requirements for IT systems in the productive area of use in the future.

Q: How important is the COSMO software for protecting the LEAG IT infrastructure?

A: Important: the software serves as an addition to the IT security concept of LEAG.

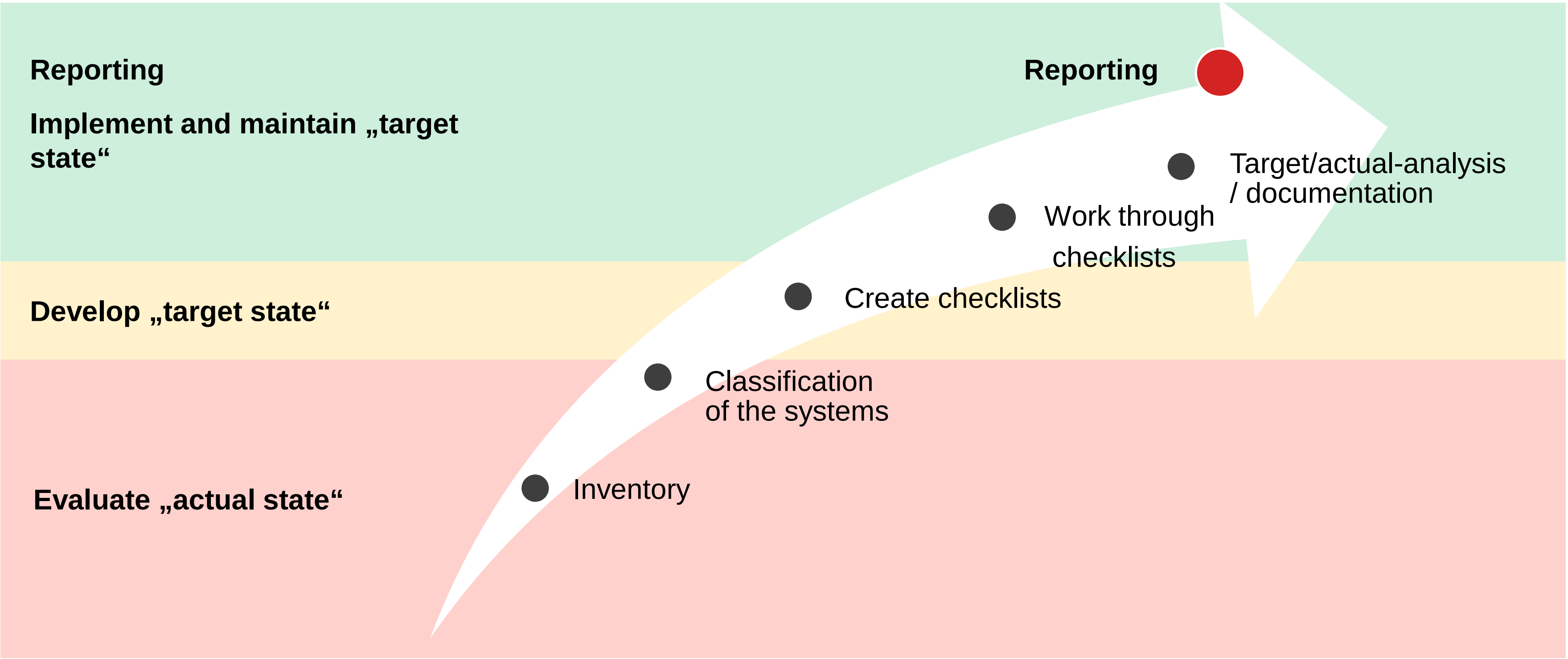
Q: How important is the COSMO software for avoiding exploitable IT security gaps in the LEAG IT system?

A: Important: the software supports the configuration of the IT systems, but does not replace the technical competence of the user.

Q: How important is the COSMO software for the fulfilment of the necessary IT security guidelines / compliance?

A: Important: the software serves as an addition to the IT security concept, but cannot independently guarantee complete protection of the infrastructure. (IP concept, network architecture, patch management, ...).

COSMO – Continuous Object-based Security Management Operations



Reporting

Implement and maintain „target state“

Develop „target state“

Evaluate „actual state“

Reporting
Target/actual-analysis / documentation
Work through checklists
Create checklists
Classification of the systems
Inventory

Baseline Cyber Security (II) with EPAS

Examples:

Evonik Industries
Emirates Global Aluminium

©Evonik: https://corporate.evonik.de/de/presse/fotos-videos/

©EGA: https://www.ega.ae/en/about-us/operations/guinea-alumina-corporation

- Reference customers for the EPAS solution for password analytics and baseline password security enforcement
- Evonik: One of the largest speciality chemicals companies in the world. Evonik Industries employs about 37,000 people and carries out activities in more than 100 countries. Revenue of €14+ billion.
- EGA: EGA is an aluminium conglomerate with interests in bauxite/alumina (Guinea) and primary aluminium smelting (United Arab Emirates). They employ about 7,000 people. Revenue of $6+ billion.
- More: https://www.detack.com/en/epas#epas-cl

The Problem

- Both **compliance** with regulations and the need to protect against **cybersecurity threats** require a form of provable **strong user authentication**. This is the most basic requirement in any organization, including the critical infrastructure and the industrial sectors.

- The most widely used authentication mechanism is the password. All enterprises and organizations use passwords for user authentication, especially for employees.

- Major security breaches have exploited **bad password choices**.

- Password policies (requirements for length, special characters, digits, etc.) fail to provide the expected security.

- Alternatives (multi-factor authentication, biometrics) have failed to take root and are often expensive.

- Much needed password quality assurance has traditionally been considered impossible for privacy and legal reasons.

- Passwords are likely to remain **the most used authentication method**.

Passwords – What is dead may never die

- **“Gates predicts death of the password”**
  cnet.com, February 2004
- **“Goodbye, Passwords. You Aren’t a Good Defence.”**
  New York Times, August 2008
- **“ Replace Passwords NOW .”**
  Every biometrics solution provider

→ Why are we still using passwords to authenticate ourselves in 90% of the cases?

- Passwords are simple, universal, accepted and often insecure.

- Big brother can easily have our fingerprints, our tokens, our phones, but not our passwords.

- The replacement of passwords as primary authentication method has constantly been predicted to be 5 years in the future for the past 15 years.

- What can we do now and today to secure passwords in our enterprises?

The Solution

Presenter claims to solve once and for all the password problem, we are all ears and full of hope. Then we hear "we are going to replace your passwords with our product", where said product is MFA, biometrics, cloud safe, etc. Utter disappointment, it was a trick again ... this time we have real thing ☺

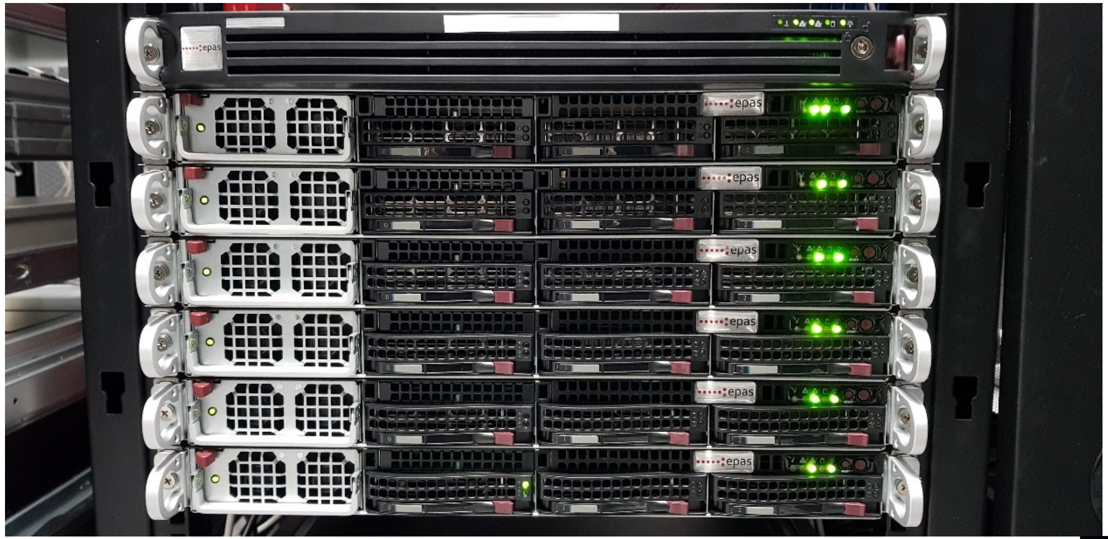
- EPAS is a **fully automated**, appliance based solution, that provides two main features: password **quality assessments** and password **quality enforcement**. It provides **proof of compliance** without requiring switching to new, alternative authentication technologies.

- It is fully **compliant** with all **legal requirements** and regional or enterprise **privacy regulations** – installed in more than 30 countries with no privacy related issues – and is used as both an audit tool to generate **metrics** and **KPIs**, as well as an on-going authentication QA and control solution.

- EPAS verifies and enforces various infosec compliance and control rules, such as detection and use prevention of **already exposed credentials**, weak or **predictable passwords**, passwords **shared by multiple users**, and about anything else one can think of about password security, with detailed reporting, historical data analysis, and remediation progress reports.

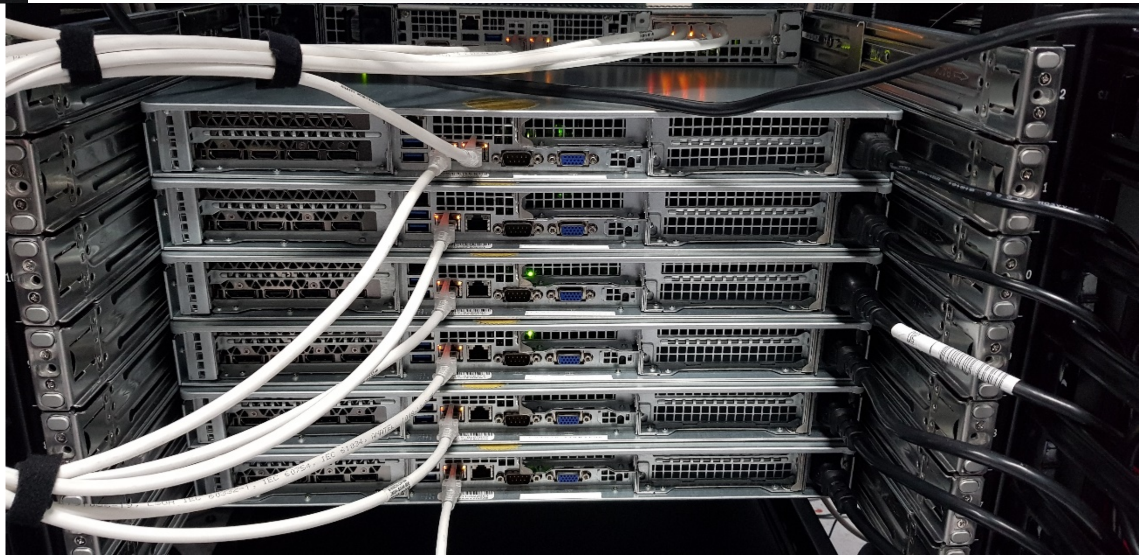
- It supports all kinds if enterprise systems, from A/D to mainframes to IoT and PLC devices, and is centralized – i.e. a central instance with satellite components serve multiple countries, data centres, plants, and installations.

EPAS: Customer Deployment Example (East Asia)



- ❑ Satellite / remote data centres in Hong Kong, Japan, Philippines, Malaysia, Indonesia, Vietnam
- ❑ Agent unit connections via either private links or VPN
- ❑ No personnel required at the remote sites

- ❑ EPAS Central Installation in a Singapore data centre
- ❑ Core installation operations from Mumbai, India
- ❑ 24/7 Operations



The Results

- ✓ Emirates Global Aluminium has been using EPAS Audit for the past five years to successfully measure, monitor, and remediate password security issues, as well as staying compliant with the relevant requirements for their particular industrial sector.

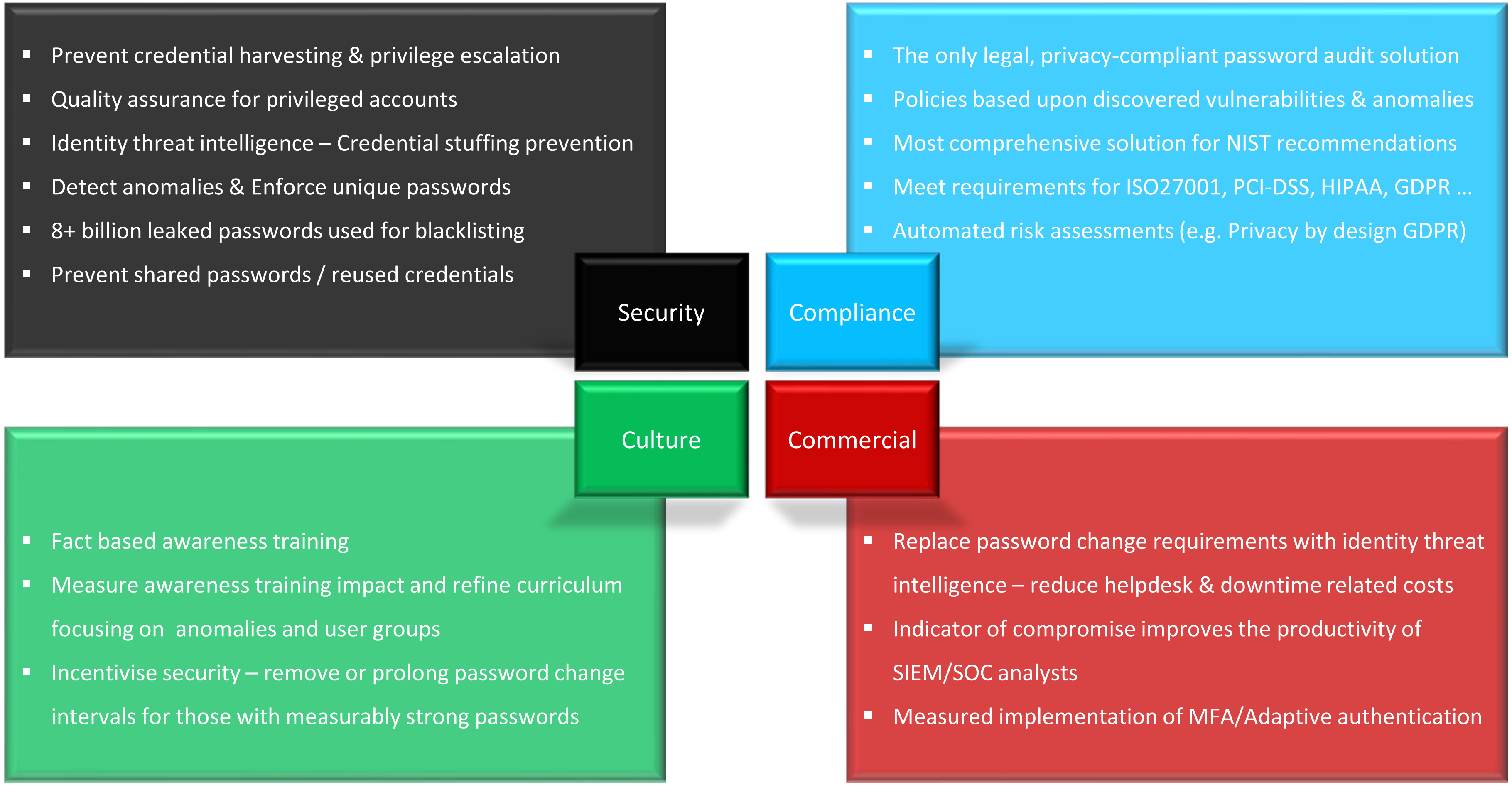
- ✓ Evonik Industries has been using both EPAS Audit and EPAS Enforcer for the past three years for detecting password relates security issues, as well as enforcing the password strength dictated by the baseline security requirements of the chemical industry.

Why password analytics is a critical component of the baseline cybersecurity for mining industry:
Managing and controlling access to IT/OT information and resources → 2 components besides regulations

1. Physical access: considering the surface of a typical site, hardware and software components will be within reach of opportunistic or targeted attacks. Access control and authentication are the first line of defence.

2. Logical access to computer networks: the increase in using automated and connected OT in mining industry create multiple new entry points for cyber criminals; critical OT systems are connected with office networks involving various types of users (suppliers, contractors etc.). Secure authentication is essential, not only for the perimeter, but at all layers, in order to prevent attacks or block them before reaching critical OT systems.

Drivers for Password Analytics and Quality Assurance



Security

- Prevent credential harvesting & privilege escalation
- Quality assurance for privileged accounts
- Identity threat intelligence – Credential stuffing prevention
- Detect anomalies & Enforce unique passwords
- 8+ billion leaked passwords used for blacklisting
- Prevent shared passwords / reused credentials

Compliance

- The only legal, privacy-compliant password audit solution
- Policies based upon discovered vulnerabilities & anomalies
- Most comprehensive solution for NIST recommendations
- Meet requirements for ISO27001, PCI-DSS, HIPAA, GDPR …
- Automated risk assessments (e.g. Privacy by design GDPR)

Culture

- Fact based awareness training
- Measure awareness training impact and refine curriculum focusing on anomalies and user groups
- Incentivise security – remove or prolong password change intervals for those with measurably strong passwords

Commercial

- Replace password change requirements with identity threat intelligence – reduce helpdesk & downtime related costs
- Indicator of compromise improves the productivity of SIEM/SOC analysts
- Measured implementation of MFA/Adaptive authentication

Thank you for your attention!

Questions?

SecurITy
made
in
Germany

Trust Seal
www.teletrust.de/itsmig

Contact:
Costin Enache, MD
costin@detack.de