Sharelock Identity Security Platform Essential

Welcome to the Sharelock Identity Security Platform Essentials document, your comprehensive guide to understanding the core features and capabilities of our advanced security solution. In today's ever-evolving threat landscape, organizations face unprecedented challenges in protecting their digital identities and sensitive data. At Sharelock, we recognize the gravity of these challenges and are committed to providing robust, innovative solutions to address them.

This document serves as your gateway to unlocking the full potential of the Sharelock Identity Security Platform. From identity protection to threat detection and response, our platform offers a comprehensive suite of features designed to safeguard your organization's most valuable assets.

As you navigate through the intricacies of the Sharelock Identity Security Platform, you'll gain insights into how our solution sets itself apart from the competition. We take pride in not only delivering state-of-the-art technology

but also in our unwavering dedication to customer success, industry-leading expertise, and relentless pursuit of innovation. With Sharelock, you can trust that you're not just investing in a product, but in a strategic partner committed to your organization's security and success.

Whether you're an IT security professional tasked with fortifying your organization's defenses or a business leader seeking to mitigate risks and ensure compliance, this document is your comprehensive resource for understanding the capabilities and benefits of the Sharelock Identity Security Platform.

Clarify the Terms

In response to the escalating threat landscape surrounding identity and access management (IAM) infrastructure, industry leaders such as Gartner and KuppingerCole have introduced the concept of Identity Threat Detection and Response (ITDR). This approach encompasses a suite of tools and practices aimed at defending identity systems against sophisticated attacks and efficiently remediating any compromises.

However, the broad categorization of all identity security aspects under ITDR can lead to confusion in the market. To provide clarity and precision, it's beneficial to segment these aspects into two distinct classes of protections: Prevention and Posture Management, and Threat Detection and Response. This segmentation enables organizations to understand and address their security needs more effectively.

Prevention and Posture Management form a foundational aspect of any robust security strategy, focusing on proactively identifying and mitigating risks to an organization's identities. This proactive stance involves surfacing potential vulnerabilities to the administrative team and implementing measures to fortify the organization's defenses.

Within the realm of Identity Threat Detection and Response (ITDR), this proactive stance is embodied in the Identity Security Posture Management (ISPM) module. ISPM plays a pivotal role in analyzing an organization's identity landscape to uncover security risks stemming from improper posture. This includes identifying ghost or orphan accounts, evaluating the usage of Multi-Factor Authentication (MFA), and scrutinizing other aspects of identity management, but unfortunately this is not enough.

We can say that ISPM operates within the paradigm of "shift left" security, emphasizing the early identification and mitigation of security concerns. Unlike real-time threat detection, which often relies on sophisticated machine learning algorithms for immediate threat discovery, shift left security primarily leverages analytics and preventive measures to mitigate

risks. ISPM distinguishes itself by focusing on practical risk analysis and posture management, prioritizing actionable insights over complex ML algorithms. In selecting an identity security product, it's essential to consider its ability to deliver on both fronts. A product that offers a balanced combination of Prevention and Posture Management, and Threat Detection and Response capabilities provides organizations with the flexibility and agility to adapt to evolving threat landscapes while maintaining robust security postures. By prioritizing this balance, organizations can effectively safeguard their identities and data assets against increasingly sophisticated threats.

An essential aspect of understanding identity security is recognizing that the "I" in ITDR stands for Identity, not just Account. An Identity encompasses the entirety of a user's digital presence and can include multiple accounts, roles, and entitlements. Protecting identities requires a holistic view that goes beyond individual account protection and considers the intricate relationships and attributes associated with each identity.

Sharelock offers native integration with leading Identity Management and Governance (IMG) products, including OneIdentity, SailPoint, IBM IGI, and others. This integration empowers Sharelock ITDR to leverage the extensive repository of identity data managed by these solutions, providing unparalleled visibility into the organization's identity landscape.

By seamlessly connecting with IMG solutions, Sharelock ISP gains access to a wealth of identity attributes, relationships, roles, and entitlements stored within these platforms. This deep integration enables Sharelock to go beyond simple account-level visibility and delve into the complex network of identity relationships across the organization.

With Sharelock ITDR, organizations can enhance their identity security posture by leveraging comprehensive identity insights to detect, investigate, and respond to identity-related threats effectively. By embracing this holistic approach to identity security, organizations can better protect their digital identities and safeguard their critical assets against evolving threats.

The Sharelock Platform Infrastructure

Platform Security with Sharelock CWP Integration:
Sharelock ITDR operates on a robust Kubernetes-based infrastructure, ensuring scalability, reliability, and security at every level of operation. One of its standout features lies in its unparalleled platform security, safeguarded by the integrated Sharelock Cloud Workload Protection (CWP) module.

Scalability and flexibility:

Scalability is a critical requirement for modern identity security solutions, especially in environments handling millions of events per day and requiring real-time processing. Sharelock meets this demand by leveraging Kubernetes, a powerful container orchestration platform known for its ability to scale effortlessly and handle high volumes of data with ease. By harnessing the power of Kubernetes, Sharelock ensures that organizations can process millions of events per day while maintaining optimal performance and reliability. This scalability allows Sharelock to effectively analyze vast amounts of data in real-time, enabling proactive threat detection and response across the entire identity landscape.

Furthermore, Sharelock's seamless integration with both on-premises and cloud environments is a testament to its versatility and adaptability. Organizations can deploy Sharelock in any environment without the need for extensive modifications or adjustments, ensuring a smooth transition to identity security solutions offered as a service.

In essence, Sharelock's scalability and flexibility make it an ideal choice for organizations seeking robust identity security solutions capable of meeting the demands of today's dynamic threat landscape. Whether deployed on-premises or in the cloud, Sharelock delivers unparalleled performance and reliability, empowering organizations to safeguard their digital identities with confidence.

Self-Protecting Mechanism:

Unlike conventional approaches that rely solely on external security

measures, Sharelock ITDR implements a self-protecting mechanism to fortify its underlying infrastructure. This proactive approach is pivotal as any compromise to the infrastructure could potentially jeopardize the entire identity security framework.

Continuous Inspection and Threat Detection:

Sharelock ITDR employs a comprehensive approach to security, continuously inspecting Kubernetes workloads and pods for any signs of compromise or misconfiguration. By leveraging the advanced capabilities of the Sharelock CWP module, the platform identifies and mitigates potential threats in real-time.

Behavioral Runtime Protection:

A key highlight of Sharelock ITDR's platform security is its behavioral runtime protection mechanism. This innovative feature utilizes sophisticated techniques, such as eBPF (Extended Berkeley Packet Filter), to monitor syscalls and network activity at the kernel level. By analyzing patterns of behavior, the system can swiftly detect and respond to any deviations that may indicate the presence of a threat.

Unmatched Threat Identification:

Unmatched Threat Identification: The integration of Sharelock CWP with Kubernetes empowers Sharelock ITDR to deliver unmatched threat identification capabilities. By combining proactive self-protection measures with real-time threat detection, the platform sets a new standard for security within the ITDR landscape.

Unique Value Proposition:

Sharelock ITDR's platform security feature represents a paradigm shift in identity threat detection and response. With its proactive approach to infrastructure protection and advanced threat identification capabilities, Sharelock ITDR stands out as a leader in safeguarding digital identities and infrastructure against evolving threats.

Sharelock ISPM - The preventive landscape

Native Integration with IAM/AM/PAM: Sharelock stands out by seamlessly integrating not only with Access Management (AM) solutions but also with leading Identity Management and Governance (IMG) products like OneIdentity, SailPoint, IBM IGI, and others. This integration grants Sharelock ITDR access to a vast repository of identity data managed by these solutions, offering unparalleled visibility into the organization's identity landscape. By tapping into IMG solutions, Sharelock ITDR goes beyond simple account-level visibility to explore the intricate web of identity relationships, roles, and entitlements across the organization.

In order to delineate Sharelock's preventive measures, let's categorize the areas:

- **Risky Accounts (Orphan, Dormant, Ghost)**
- **Privileged Accounts (Administrative and Service)**
- **Should Be vs As Is**
- **Multi-Factor Authentication (MFA)**
- **Policy Deviation**

Risky Accounts

Each account/identity in Sharelock is associated with a specific risk, determined by its classification and behavior over time. Certain accounts receive heightened attention, including orphan, dormant, and ghost accounts, all deemed inherently risky.
Orphan accounts are active but not linked to any user or identity, while dormant accounts have had no activity for an extended period. Ghost accounts, created directly on a target/application, remain uncontrolled due to the lack of two-way synchronization. Sharelock constantly highlights these high-risk accounts on its console and notifies managers through a specific playbook task.

Privileged Accounts

Administrative accounts, typically managed by a Privileged Access Management (PAM) system, require temporary grants for system operation. Sharelock monitors administrative activity associated with these accounts through PAM system audit logs, adjusting the risk level based on target activity and any behavioral anomalies observed during global administration tasks. Any high-risk accounts are promptly flagged for security managers' attention.

Service accounts facilitate machine-to-machine interactions and usually do not permit interactive logins. However, in cases where standard logins are necessary, Sharelock detects anomalous behavior, marking such accounts as high risk. For instance, if a service account exhibits interactive login behavior, it is considered a threat. Sharelock's behavioral analysis is critical in identifying potential misuse of service accounts, such as in data exfiltration cases via modified batch scripts.

As Is vs Should Be

Sharelock offers a compliance analysis on the Identity base through the correlation of access clusters. This involves two fundamental analyses: Should Be and As Is.

Should Be Analysis: This analysis intelligently groups classes of users/accounts with similar access bases, creating clusters based on the access policies defined by the Identity and Access Management (IAM) systems. It identifies patterns in access requirements and clusters users/accounts accordingly.

As Is Analysis: Similar to Should Be analysis, As Is analysis creates clusters of users/accounts based on their access behavior. It considers the access granted and the behavior associated with that access, providing a comprehensive view of user/account behavior.

The Should Be and As Is clusters are compared, and deviations or outliers are flagged with an Incompliant Score. These scores indicate areas where the actual access patterns deviate from the organization's expected or desired access policies.

This analysis is conducted automatically periodically, ensuring continuous monitoring of identity compliance. Users/accounts with high Incompliant

scores are promptly identified and brought to the attention of their respective owners through specific tasks in the playbook. This proactive approach enables organizations to address compliance issues promptly and maintain a secure and compliant identity infrastructure.

MFA Monitoring and Analysis

- **MFA Adoption Monitoring:** Sharelock offers a centralized dashboard designed to monitor the adoption of Multi-Factor Authentication (MFA) solutions across organizations, spanning multiple Access Managers and IAM products. This dashboard provides a comprehensive overview of the organization's overall status of MFA deployment. It synthesizes crucial information, including enrolled factors and devices, into an easily digestible format. Additionally, the Sharelock dashboard offers detailed insights into various metrics related to MFA adoption, facilitating trend analysis over time. This functionality enables organizations to track the progress of MFA implementation and identify areas for improvement.

- **MFA Usage Monitoring:** Sharelock can effectively track the usage of Multi-Factor Authentication (MFA) through its seamless integration with access audit logs via APIs, such as Okta, Active Directory (AD), and OneLogin, among others. By leveraging these integrations, Sharelock captures comprehensive data on users' actual MFA usage, including each MFA step performed. Additionally, Sharelock enriches this data with contextual information such as geolocation and device details. This enriched data is presented through intuitive visualizations and trends over time within the Sharelock platform. Security experts can utilize this information to gain insights into the current utilization of MFA across the organization, enabling them to make informed decisions and adjustments as necessary.

Policies Deviation

An important aspect to highlight is that certain activities, although they may initially seem like policy deviations, hold significant security implications. Sharelock prioritizes the identification and management of suspicious or potentially malicious activities, treating them as emerging or confirmed threats while simultaneously flagging them as policy deviations in the

background. These activities are swiftly addressed through specific Tasks and Automated Security Logic (TASL) within Sharelock's playbook, ensuring they are promptly brought to the attention of the relevant stakeholders.

Some common examples of such activities include:

- Creation of new users/accounts outside the provisioning process.
- Deletion of users/accounts outside of the provisioning process.
- Bulk creation or deletion of users/accounts.
- Creation of new applications outside of the provisioning process.
- Malicious modification of email forwarding policies.
- Malicious alteration of SharePoint file access permissions.
- Unauthorized editing of Azure Information Protection (AIP) sensitivity labels.

By proactively identifying and responding to these activities, Sharelock mitigates potential security risks and helps maintain the integrity of the organization's identity and access management framework.
Ultimately, it is worth mentioning that Sharelock ITDR introduces advanced capabilities that transcend conventional identity discovery and visibility functions. Unlike traditional solutions, Sharelock ITDR's integration with Identity Management and Governance (IMG) systems is bi-directional, enabling organizations to orchestrate recertification campaigns based on holistic Identity Risk assessment rather than focusing solely on individual accounts. This bi-directional connection empowers organizations to enforce recertification processes aligned with the Minimum Privilege principle. This ensures that users possess only the necessary access rights, thereby reducing the risk of overprovisioning. Moreover, Sharelock ITDR leverages real-time behavior analysis to provide recommendations for identity attribute modifications, further fortifying the organization's security posture and compliance efforts.

Sharelock Detection - Model and features

Why Sharelock needs historical data to perform behavioural analysis? Imagine a jewelry store, where the behavior of visitors is scrutinized to detect any potential threats or anomalies. In one scenario, an armed individual attempts to enter the store, brandishing a weapon—a clear and overtly anomalous behavior signaling an imminent attack. This type of behavior is relatively straightforward to identify and categorize, akin to recognizing a known threat based on predefined patterns or rules.

However, consider another scenario where a well-dressed gentleman enters the store, appearing like any other ordinary customer. Unbeknownst to the staff, this individual engages in subtle actions, such as surreptitiously swapping a genuine jewel with a counterfeit one. Unlike the overtly armed attacker, this behavior is much more nuanced and sophisticated, requiring a keen analytical eye to detect. Identifying anomalies in this scenario necessitates a deeper understanding of normal customer behavior and the ability to discern subtle deviations or irregularities.

In essence, these scenarios illustrate two distinct types of behavioral analysis: the first involves recognizing overt and easily identifiable anomalies, akin to spotting a threat in plain sight, while the second requires a more nuanced approach, leveraging historical data and sophisticated algorithms to detect subtle deviations from expected behavior. A robust behavioral analysis solution must be capable of handling both types of anomalies, from the glaringly obvious to the intricately concealed, to effectively safeguard against a wide range of threats.

This is why Sharelock, relying solely on machine learning algorithms, requires access to historical data to effectively perform behavioral analysis. The creation of accurate and effective baselines necessitates the accumulation of historical data spanning from a minimum of several weeks to three to four months. Any claim suggesting behavioral detection without the need for historical data likely pertains to a behavioral analysis of the first type—focused on recognizing overt anomalies based on predefined patterns or

rules. However, for a more sophisticated and nuanced understanding of behavior, especially in detecting subtle deviations or irregularities, historical data and machine learning algorithms are essential. By leveraging historical data, Sharelock can develop comprehensive behavioral baselines that enable the detection of even the most intricately concealed threats.

In the acronym ITDR, the "I" stands unequivocally for Identity. However, it's a term often misconstrued, sometimes interchangeably with Access. While safeguarding access is undeniably pivotal, it merely represents the first line of defense—a barrier that determined threat actors often breach. But does that leave us defenseless? Far from it. Rather, it signals a shift in strategy. We're no longer contending with a blunt force approach but rather pursuing a much subtler adversary, akin to hunting a cunning thief rather than an assailant wielding a weapon. This analogy underscores the necessity for a nuanced and adaptive approach—one that goes beyond merely fortifying access points to encompass the intricate realm of identity security.

Sharelock's conceptual model for detection revolves around the notion of IoBs (Indicators of Behavior), mirroring the concept of IoCs (Indicators of Compromise). IoBs serve as flags for anomalies compared to the "normal" behavior of users, accounts, or entities within the system. Here, "normal" behavior is defined by historical data specific to the observed phenomenon. Each IoB comprises a subject (user, account, entity) whose anomalies are under scrutiny, along with a direct object representing the action being analyzed. For instance, if an account is the subject and a SharePoint folder the direct object, every access action to that folder is monitored. By learning the typical access patterns, Sharelock can flag anomalies in real-time access to the folder.

One intriguing aspect of Sharelock's IoBs is the ability to freely interchange subject and direct object. For example, the folder can become the subject, allowing the system to learn how different accounts access it, thereby identifying anomalies in folder access patterns. Additionally, two other entities play roles in IoBs: the algorithm defining the anomaly type (e.g., frequency anomaly, novelty anomaly) and the type of baseline for

comparison (global, personal, or cluster).
Consider the scenario of monitoring login actions for all company accounts. Each account serves as a subject, with "login" as the object complement, employing a personal baseline for anomaly comparison and a specified algorithm (e.g., frequency). Given the potentially vast number of accounts (tens of thousands), this approach generates a corresponding number of baselines for comparison.

This flexible and nuanced approach to behavior monitoring enables Sharelock to detect anomalies effectively across diverse scenarios, empowering organizations to proactively mitigate security threats. Sharelock offers a range of content packs, each containing pre-configured IoBs tailored to protect both access and corporate applications such as MS 365, MS Azure, Octa, OneLogin, PAM, SAP, SharePoint, and more. These content packs provide a ready-made set of IoBs, streamlining the implementation process. However, Sharelock also allows users to configure custom IoBs directly from the graphical interface, enabling the creation of IoBs for specific needs, even for legacy applications.

An IoB acts as a metaphorical laser beam within the detection framework, representing a potent tool for strengthening security defenses. As the number of IoBs increases, so too does the network of protective barriers, bolstering the organization's resilience against threats. Managing millions of behavioral baselines within large enterprises necessitates highly efficient discovery algorithms capable of swiftly building baselines and enabling real-time monitoring during runtime processing. Sharelock's ability to achieve this feat, leveraging years of research and development to develop advanced discovery algorithms, underscores its innovative edge in the realm of threat detection and response.

Indeed, Sharelock's algorithms represent a pinnacle of efficiency and real-time processing capability. The ability to reconstruct millions of behavioral baselines using historical data in a matter of hours stands as a testament to Sharelock's innovative research and development efforts. This rapid baseline reconstruction ensures that organizations can adapt swiftly to evolving

threats and maintain robust security postures in dynamic environments. Such innovative prowess underscores Sharelock's commitment to delivering cutting-edge solutions for threat detection and response.

In the realm of threat detection based on behavioral machine learning, the ability to classify unstructured data represents a significant leap forward. While clustered peers of subjects based on attributes can aid in anomaly detection, the true innovation lies in the classification of unstructured data for behavioral clusters. In many security infrastructures, structured data and logs serve as the primary source of information. However, vast amounts of unstructured data within organizational frameworks remain largely untapped, despite holding immense potential.

Consider the example of access to company files and folders. Effectively categorizing this unstructured data could provide valuable insights into account and identity behaviors crucial for threat detection. Although advanced semantic understanding technologies like Large Language Models (LLMs) offer promise, integrating real-time unstructured data classification into security systems requires significant innovation.

Sharelock has emerged as a leader in this regard, bridging the gap by implementing practical methods for classifying unstructured data within its ITDR framework and leveraging it in real-time processing. This innovative approach enables organizations to harness the full potential of unstructured data for enhancing threat detection and response capabilities.

Ultimately, the efficacy of a detection security system hinges on two critical factors: its sensitivity and its capacity to minimize false positives. Sensitivity measures the system's ability to accurately detect genuine threats, while false positive reduction focuses on mitigating erroneous alerts. In traditional threat detection systems, heightened sensitivity often correlates with a rise in false positives, leading to alert fatigue and diminished attention. Therefore, striking a balance between sensitivity and false positive reduction is paramount. An effective security system must maintain high sensitivity while concurrently minimizing false positives to ensure accurate threat

detection without inundating operators with irrelevant alerts. Here is where we spent much effort and many field test. It would be interesting to give the result of the last test conducted few months ago.

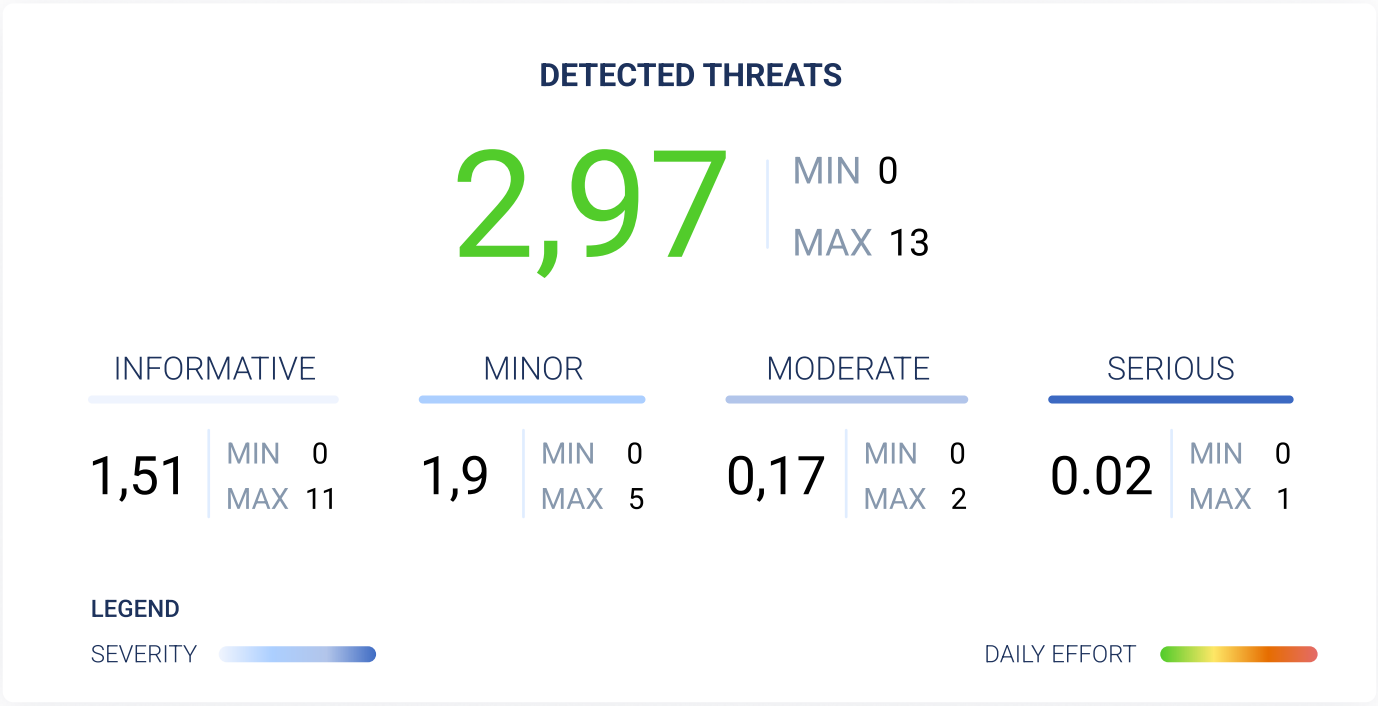
System data:

Customer:	Large European Telco
Number of Identities:	58,000
Application under protection:	Office 365 (with all tenant), ERP, CRM
Number of IoBs:	124
Number of Behavior Baseline:	1,253,000
Training period:	3 Months
Real Time Processing Period:	2 Months
Total Number Of Events:	1.35 Billion

Result:

Daily average of detected threats

The data relates to the period 01/10/2023 - 31/12/2023



Overall, the results of the field test indicate that Sharelock ITDR has achieved a commendable balance between sensitivity and false positive reduction. The system's capability to accurately detect and prioritize threats while minimizing false positives reflects its efficacy in enhancing cybersecurity posture and mitigating security risks effectively.

Consequently, these achievements can be considered as a testament to the system's reliability and effectiveness in real-world deployment scenarios.

Sharelock - Threat Response

Investigation is a critical aspect of understanding and mitigating potential identity threats within an organization's security framework. It involves analyzing detected activities to uncover the scope, method, and impact of potential threats to identity integrity. This process requires correlating data from various sources to gain comprehensive insights into the nature of the threat and to identify affected systems or data.
Sharelock's innovation in the realm of identity security aimed to transition from a rule-based approach to a more agile, rule-free environment. However, this transition is still a work in progress, particularly in the investigation domain.

Currently, Sharelock’s Threat Modeler relies on rule-based mechanisms to correlate anomalies detected by IoBs. These anomalies are then mapped onto recognized threat tactics, highlighting their severity to the security team. This categorization aligns with the six-stage severity kill chain and is mapped onto MITRE techniques and tactics for standardized terminology. In the Sharelock Identity Security Platform, the concept of threat is separate from the notification alert. Once detected, the threat has its life cycle and remains active until the remediation playbook is completed or an operator closes it manually. For each subsequent anomaly that the system encounters relating to that particular attack pattern, the security analysts will be notified if and only if the situation worsens, therefore if the total risk of the threat increases, or if a minor stage is moved to a major one. This mechanism is to

avoid overloading the work of security operators but to alert them only when strictly necessary.

Looking ahead, Sharelock is poised to introduce generative AI for fast and automated investigation of discovered threats. Leveraging local Large Language Models (LLMs), we aim to tackle the complexity of cyber threats by enabling detailed and timely investigations into individual or clustered anomalies. The generative AI will come into play post-anomaly detection, conducting contextualized investigations efficiently. It will analyze the context of suspicious activities, distinguishing between internal user behavior, external hostile activity, and anomalies within the infrastructure. Automating the threat hunting, investigation, and response processes offers significant advantages. It dramatically accelerates threat response times, minimizing the delay between detection and mitigation. Additionally, it enhances the accuracy of investigations by reducing false positives, ensuring that only genuine threats are addressed promptly and effectively.

Sharelock ITDR includes a playbook to play appropriate actions on a threat.

The features of the playbook within the Sharelock platform include:

- **Predefined Response Actions:** The playbook is equipped with predefined response actions tailored for various security incidents.
- **Manual and Automatic Response Capabilities:** Users can choose between manual and automatic responses, providing flexibility in how incidents are managed.
- **Streamlined Incident Response Processes:** The playbook is designed to streamline incident response, helping to reduce response times and minimize potential damage.

The detailed features of the playbook provided by Sharelock go beyond predefined response actions for various security incidents. Here are some of the key elements of Sharelock's responsive playbook:

- **Automatic and Manual Response Options:** The system can employ a mix of automatic and manual responses to remediate detected threats, thus providing flexibility in incident response.

- **Comprehensive Response Mechanisms:** Various actions can be triggered in response to threats, including but not limited to:
  - Push notifications, emails, or SMS to account owners for identity confirmation.
  - Additional audits to investigate threats.
  - Risk-based recertification campaigns for user access rights.
  - Disconnecting users from current sessions.
  - Revoking access rights.
  - Resetting passwords.
  - Activating multi-factor authentication.
  - Notifying the Security Operations Center (SoC) team.
  - Disabling accounts involved in the threat.

- **Custom IAM Workflow Automation:** The playbook can automatically trigger custom Identity and Access Management (IAM) workflows, either with or without a manual approval step, to block or unlock a user depending on the situation.

- **Integration with Incident Management Systems:** It may also integrate with incident management systems such as Jira or ServiceNow for automated incident reporting and can alert other systems or services about a threat via real-time threat alerts using webhooks.
  Centralized Log Management: Sharelock's playbook has capabilities for security event forwarding via Syslog to SIEM systems for centralized logging and threat analysis.

These detailed features ensure that the Sharelock's playbook is not only responsive but also robust and capable of a wide range of responses tailored to the nature and severity of the security incidents detected by the system.
Of course no specific innovativeness is into the playbook. Just completeness of the product and again the strict integration with the IAM system.

Sharelock

CONTACT US

learn.sharelock.ai | www.sharelock.ai | info@sharelock.ai