Whitepaper

The Proactive Advantage: Mastering Cybersecurity with Observability

Author

Sanjeev Mehrotra

Executive Summary

Traditionally, enterprise infrastructure was on-premise, with all applications and underlying infrastructure under direct control. However, with increased digital transformation and exponential adoption of cloud infrastructure and native apps, there has been a paradigm shift in cybersecurity measures. While a simple log collection and correlation through a traditional SIEM solution was effective in a data center-led environment, a more robust analytics platform providing granular visibility is key to staying ahead in today’s world.

Hence, observability in cybersecurity has become an essential aspect that gives a comprehensive visibility into the state of internal systems, including complex networks, applications, and infrastructure, through the analysis of logs, metrics, and traces. It ensures the reliability and security of applications and infrastructure, providing a clear picture of what is happening within the environment.

This whitepaper provides a comprehensive guide, covering the core components, critical use cases, and strategic business benefits of adopting security observability.

Introduction

Reportedly, Global 2000 companies lose nearly 9% of their profits to unplanned downtime, totaling billions annually. The second-highest cost comes from regulatory fines. These incidents are often born from a common failure: an inability to see and understand what is happening across the enterprise network in real-time. This is the critical visibility gap that modern security observability is designed to bridge.

Unlike traditional security monitoring, which relies on pre-defined thresholds and alerts, observability in cybersecurity offers deep visibility into the present and past states of your entire network. It focuses on collecting and correlating data from various sources, from cloud infrastructure to on-premise applications, to gain actionable insights into vulnerabilities, anomalous behavior, and active threats. The goal is to gain deep visibility across your IT environment to manage security threats proactively.

The Challenge of Modern IT Complexity

Modern enterprises typically operate hybrid cloud environments, with some applications running on-premise and others in public clouds.
Many organizations have adopted a multi-cloud strategy with applications spanning multiple public cloud providers and geographies. This increases complexity, making complete visibility harder to achieve. At the same time, global regulatory and data privacy requirements force organizations to safeguard personal data and to verify that third-party partners handle that data appropriately. Cloud computing, microservices architectures, and the Internet of Things create a vast, interconnected ecosystem that traditional security measures struggle to protect.
This is where security observability becomes crucial.

It provides a unified, data-rich view of the entire IT infrastructure, which helps organizations to:

- Detect and respond to threats in real-time.
- Identify vulnerabilities and misconfigurations before they can be exploited.
- Establish baselines of normal system behavior to spot anomalies instantly.
- Dramatically improve incident response times and effectiveness.
- Continuously enhance security posture and reduce overall risk.

Ultimately, implementing security observability allows an enterprise to make the crucial shift from a reactive to a proactive security stance. This holistic view is essential for preventing costly breaches, maintaining customer trust, ensuring compliance, and protecting the organization's brand and bottom line.

Key Aspects of Security Observability

For effective implementation of security observability in an organization, the following processes must work together to provide a comprehensive, unified view of an organization's security posture:

1) **Data Collection:** The foundation of observability is collecting data from across the IT infrastructure. Sources include:

   - Metrics on system performance and resource utilization
   - Traces of transactions and user activities
   - Telemetry data from security controls and endpoints

2) **Data Analysis:** Raw data is transformed into actionable intelligence through sophisticated analysis. This involves:

   - Real-time processing of massive data volumes
   - Correlating events across different systems and controls
   - Using AI and ML algorithms to detect anomalies
   - Recognizing patterns to identify potential threats

3) **Contextual Intelligence:** To make informed decisions, the observability data should be enriched with contextual information, such as:

    - Threat intelligence feeds from both internal and external sources
    - Up-to-date asset inventory and configuration data
    - User and Entity Behavior Analytics (UEBA)
    - Business priorities and risk assessments

4) **Dashboard Visualization:** Complex security data is made clear and accessible through visualization tools that provide:

    - Interactive dashboards presenting critical trends and anomalies
    - Customizable reports tailored for different stakeholders (e.g., CISO, IT security)
    - Real-time alerts and notifications to guide security analysts' response plans

5) **Automation:** Observability platforms should integrate with workloads (on-premises and cloud), network, and endpoints to enable rapid, automated response, and reduce analyst fatigue. This includes:

    - Continuous monitoring and testing of security controls across diverse tools and technologies
    - Orchestration of incident responses through automated playbooks
    - Using AI/ML to analyze patterns and predict future threats

By integrating these five processes, an organization can build a robust security observability framework that provides the deep insights needed to protect the enterprise effectively, with a shorter Mean Time to Resolution (MTTR) and human intervention.

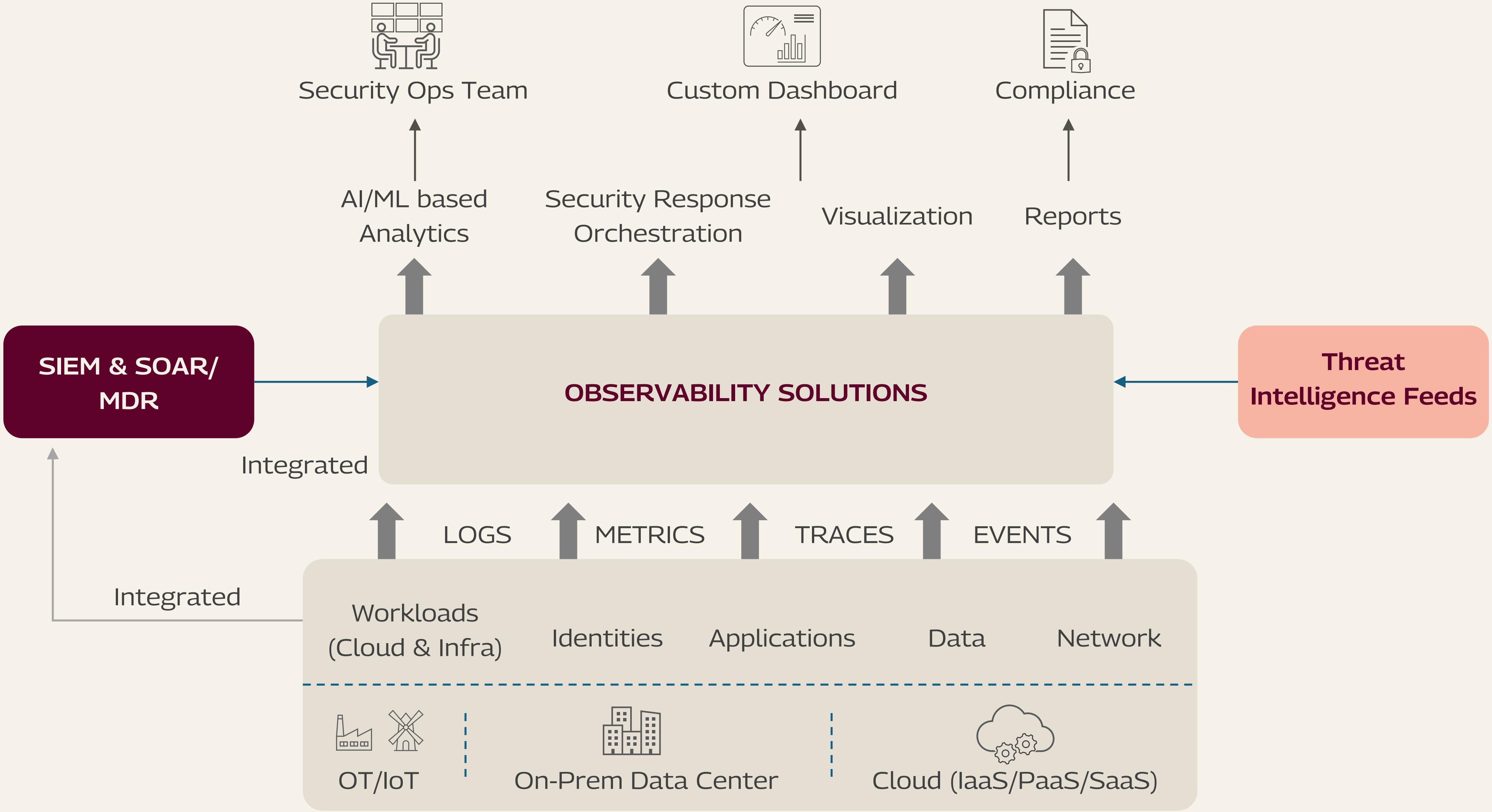

Figure 1: Observability Solution Architecture

Security Observability in Action

The actual value of security observability is realized when applied to the most pressing security challenges facing modern enterprises. It moves beyond a theoretical concept to deliver tangible improvements across a wide range of critical functions, including:

1) Threat Detection and Response

- Identify and investigate suspicious activities across the entire IT estate in real-time
- Correlate events across systems to uncover complex attack patterns
- Automate initial response actions to immediately contain threats

2) Vulnerability Management:

- Continuously monitor systems for emerging vulnerabilities and misconfigurations
- Prioritize remediation efforts based on business risk and potential impact
- Track the effectiveness of patching and mitigation strategies

3) Continuous Compliance Monitoring:

- Ensure adherence to regulatory requirements like GDPR, HIPAA, and PCI DSS
- Automatically generate audit trails and compliance reports
- Detect and alert on potential compliance violations in real-time to prevent penalties

4) Cloud Security:

- Monitor hybrid and multi-cloud environments for unauthorized access, data exposure, and misconfigurations
- Ensure consistent security policy enforcement across hybrid and cloud-native infrastructures
- Track resource usage and configuration changes to prevent shadow IT and cost overruns

5) Zero-Trust Implementation:

- Enable continuous verification of user and device trust before granting access to data or applications
- Enforce least-privilege access by actively monitoring sessions for anomalous behavior
- Support micro-segmentation by monitoring all network traffic, both north-south (to/from the data center) and east-west (within it)

6) DevSecOps Integration:

- Identify and remediate vulnerabilities in the software development lifecycle (SDLC)
- Detect and investigate API abuse and abnormal usage patterns
- Monitor application performance and behavior for potential security issues within the CI/CD pipeline

7) IoT and Edge Computing Security:

- Gain complete visibility into all connected IoT and Industrial IoT (IIoT) devices and environments
- Monitor edge networks for anomalous traffic and potential compromises

From Business Risk to Strategic Advantage

Security observability is a strategic enabler that directly addresses critical business challenges hampering growth and increasing risk in today's digital landscape. It achieves this by turning fundamental operational hurdles into sources of strength and resilience:

- **Taming IT Complexity:** With IT environments becoming more complex, traditional security approaches struggle to keep pace. Security observability provides a unified view of the entire infrastructure, enabling effective management and security of this complexity, turning a major vulnerability into a manageable asset.
- **Amplifying Team Expertise:** Amid a persistent cybersecurity skills gap, many organizations struggle to find and retain qualified security professionals. Security observability tools can address this challenge by automating routine tasks and delivering actionable insights, thereby reducing the monitoring team's dependency.
- **Outpacing Evolving Threats:** Cyber threats evolve faster than manual defenses can adapt. Security observability enables organizations to detect and respond to new and emerging threats with greater speed and precision.
- **Regulatory Compliance Requirements:** Meeting regulatory requirements and industry standards is a constant hurdle. Observability simplifies this by providing the continuous monitoring, automated audit trails, and comprehensive reports needed to demonstrate compliance and pass internal and external audits with confidence.

Delivering Measurable Security Outcomes

By shifting from a reactive to a proactive posture, security observability delivers significant, measurable benefits across the organization:

- **Enhanced Incident Response:** Reduces Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) by providing precise, context-rich data and minimizing false positives across all infrastructure components (network, workloads, and endpoints)

- **Significant Cost Savings:** Prevents costly security breaches, reduces fines associated with non-compliance, and lowers operational overhead through better resource allocation and less manual effort

- **Improved Operational Resilience:** Increases system uptime and availability by preventing security incidents that cause unplanned downtime, directly supporting business continuity

- **Reduced Business Risk:** Hardens the overall security posture, demonstrably decreasing the likelihood and impact of successful data breaches or cyber-attacks

- **Accelerated Business Growth:** Enables faster time-to-market for new products and services while strengthening customer trust and satisfaction

The Future of Security Observability

The field of security observability is rapidly evolving, driven by key technological advancements and new security paradigms:

- **Smarter Detection with AI/ML:** Predict threats with advanced AI algorithms that go beyond simple pattern recognition to automate complex analysis and surface stealthy attack patterns in large datasets
- **Deeper Cloud-Native Integration:** Provide deeper, specialized insights into ephemeral environments like containers and serverless functions to enhance observability as cloud adoption accelerates
- **Convergence with XDR:** Unify observability feeds with Extended Detection and Response (XDR) platforms to create a single, end-to-end security view from endpoint to cloud
- **Automated Threat Detection and Remediation:** Orchestrate detection and remediation workflows, to neutralise threats faster and with reduced manual effort
- **Privacy-Preserving Analytics:** Incorporate privacy-preserving analytics techniques to balance security insights with regulatory and data-protection requirements

Conclusion

In an era defined by sprawling, complex IT environments, security observability provides the only way to achieve true clarity and control over an organization's security landscape.

By transforming raw data into actionable intelligence, observability empowers every level of the business. For security engineers, this translates to faster threat detection and a dramatic reduction in incident response times. For CXOs, it provides a clear, data-driven view of the organization's security posture, ensuring compliance and reducing overall business risk.

Ultimately, proactively managing security threats is not just about protection—it is about maintaining trust, enabling innovation, and ensuring business resilience. Security observability is the key to achieving that goal.

Endnotes

.conf24: Splunk Report Shows Downtime Costs Global 2000 Companies $400B Annually. (n.d.). Splunk.

https://www.splunk.com/en_us/newsroom/press-releases/2024/conf24-splunk-report-shows-downtime-costs...

About the Author

Sanjeev Mehrotra is a dynamic technology leader with over 28 years of experience in driving digital security transformations for global enterprises. As the Global Head of Cybersecurity at Tech Mahindra, Sanjeev leads the vision, strategy, and execution of the company's cybersecurity portfolio, helping organizations build resilient, threat-aware environments in an increasingly complex digital world.

Prior to joining Tech Mahindra, Sanjeev spent over a decade and half at HCL, where he held key leadership positions and was instrumental in scaling the organization's global cybersecurity practice. His deep industry knowledge spans multiple sectors, including BFSI, healthcare, manufacturing, and telecom.

Sanjeev holds a management degree from the Institute of Management Technology (IMT) and a technical foundation built on years of hands-on experience in enterprise IT and security.

Based in Noida, India, Sanjeev plays a pivotal role in shaping Tech Mahindra's cybersecurity strategies, ensuring the delivery of cutting-edge solutions that help clients navigate the complex and ever-evolving digital landscape.

Sanjeev Mehrotra

Global Head - Cybersecurity,
Tech Mahindra

About **Tech Mahindra**

Tech Mahindra (NSE: TECHM) offers technology consulting and digital solutions to global enterprises across industries, enabling transformative scale at unparalleled speed. With 152,000+ professionals across 90+ countries helping 1100+ clients, Tech Mahindra provides a full spectrum of services including consulting, information technology, enterprise applications, business process services, engineering services, network services, customer experience & design, AI & analytics, and cloud & infrastructure services. It is the first Indian company in the world to have been awarded the Sustainable Markets Initiative's Terra Carta Seal, which recognizes global companies that are actively leading the charge to create a climate and nature-positive future. Tech Mahindra is part of the Mahindra Group, founded in 1945, one of the largest and most admired multinational federation of companies. For more information on how TechM can partner with you to meet your Scale at Speed™ imperatives, please visit https://www.techmahindra.com/.

TECH
mahindra

www.techmahindra.com
www.linkedin.com/company/tech-mahindra
www.x.com/Tech_Mahindra

Copyright © Tech Mahindra Ltd 2025. All Rights Reserved.

Disclaimer: Brand names, logos, taglines, service marks, tradenames and trademarks used herein remain the property of their respective owners. Any unauthorized use or distribution of this content is strictly prohibited. The information in this document is provided on "as is" basis and Tech Mahindra Ltd. makes no representations or warranties, express or implied, as to the accuracy, completeness or reliability of the information provided in this document. This document is for general informational purposes only and is not intended to be a substitute for detailed research or professional advice and does not constitute an offer, solicitation, or recommendation to buy or sell any product, service or solution. Tech Mahindra Ltd. shall not be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. Information in this document is subject to change without notice.