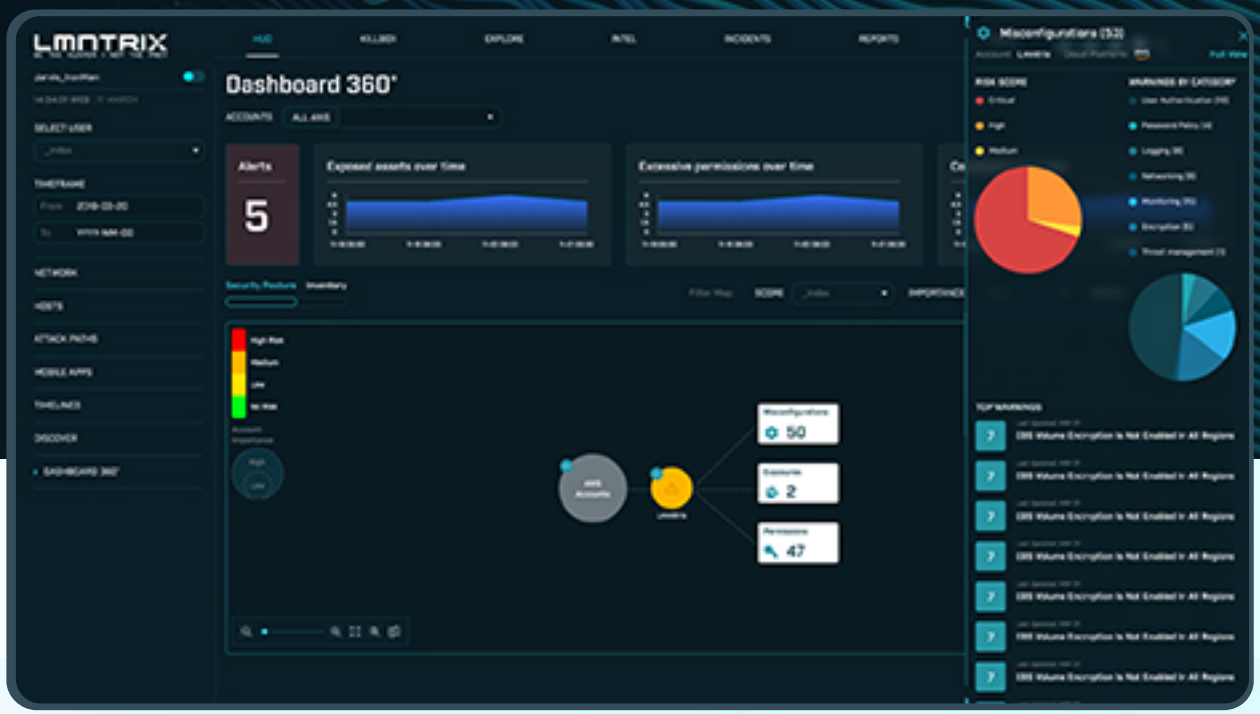
LMNTRIX

BE THE HUNTER | NOT THE PREY

LMNTRIX CLOUD XDR



LMNTRIX XDR Cloud Delivers Multi-Vector Managed Detection and Response for Multi-Cloud Workloads

Security Operations Center (SOC) and Cloud SecOps teams are overwhelmed with investigating and closing every "alert", most of which are not actual threats or incidents. LMNTRIX XDR CLOUD **contextualizes the cloud, application, and** user behavior in your environment and creates an attack storyline to identify actual threats. By focusing on actual threats in the runtime, LMNTRIX improves productivity and morale of the SOC and reduces business risk

The LMNTRIX XDR Cloud combines Cloud Security Posture **Management (CSPM) with Identity** Threat Detection and Response (ITDR) and our runtime unique Cloud Threat Detection and Response (CDR) to monitor and analyze all threat vectors including excess privileges and identity **risks, exposed assets, and** behavioral anomalies to identify and respond to real-time risk.

Reduce the cloud attack surface by understanding all permissions and their use so unused permissions can be safely eliminated without impacting productivity

Respond to actual incidents with contextualized models built to alert on atypical behaviors for your specific cloud, application, and users.

Centralized runtime analysis and observability identifies risky behaviors to stop threats before they become a newsworthy incident

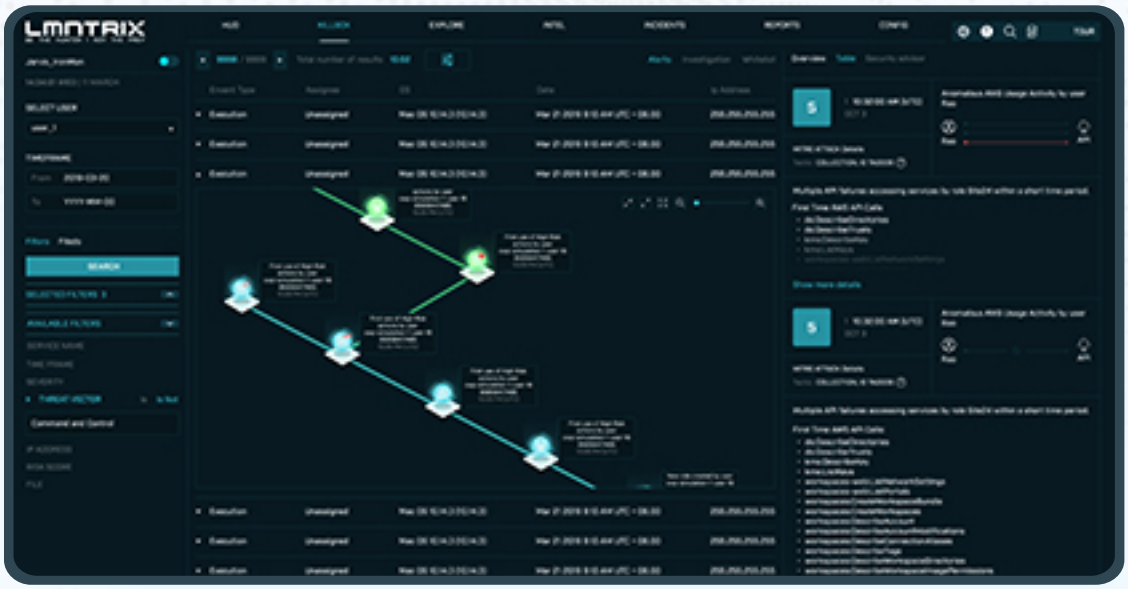
Resolve issues fast with a full understanding of exactly how threat actors penetrated the environment with attack sequences

Support internal and external compliance initiatives with automated review

Identify privilege escalation and other malicious uses of unsuspecting identities

Runtime Observability

While most cloud security tools analyze static points in time, the LMNTRIX XDR Cloud continuously monitors and analyzes configurations, permissions, and behavior in the environment providing constant vigilance and real-time observability. Particularly important for addressing misconfigurations that may take time to address or simply cannot be addressed without taking down the environment, this level of monitoring reduces the misconfiguration risks your organization is forced to tolerate.



Identifying real alerts with MBIs and the Attack Sequence and eliminate Alert Fatigue

LMNTRIX leverages malicious behavior indicators (MBIs) sequenced together to indicate an actual threat. MBIs are behaviors and activities that are detected from the metadata and logs we collect from the cloud environment. Over a period of time, a string of MBIs can reveal an attack sequence. Our Machine Learning (ML) will score these activities and create alerts for the LMNTRIX team to investigate and validate

The MBIs are sequenced into a storyline, which is then scored. The sequence is continuously evaluated as new MBIs are added to the sequence and scored. Once the score of the sequence is higher than 7, you get a realert and you know you need to investigate. This ensures you respond to the riskiest alerts first.

The LMNTRIX XDR attack sequence provides a complete overview to your team of how the attacker got in and then moved around the organization. Your team, regardless of experience level, can easily identify the vulnerabilities and take steps to close these gaps in real-time.

THE LMNTRIX XDR AI and ML are different, really.

LMNTRIX leverages advanced machine learning (ML) techniques and artificial intelligence (AI) to build models for ongoing behavioral analysis of the runtime for more accurate threat detection. Models are trained and tuned every day on customer data at a global level. The output of the models are reviewed by security experts to ensure models are accurate. For more information, check out our blog, "The Science Behind Our Security".

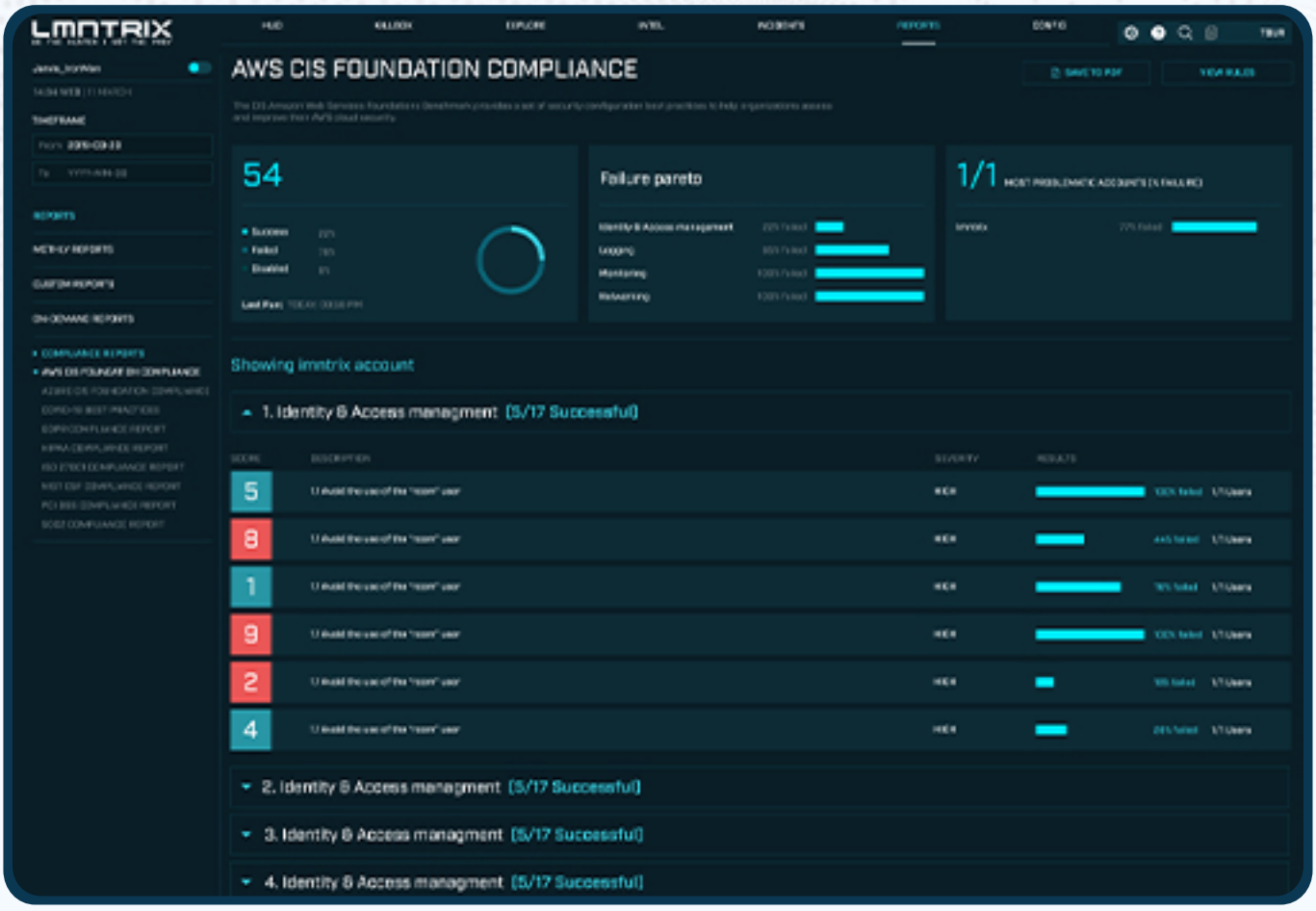
Eliminating Excessive Permissions

Access to cloud resources is granted through permissions and in order to ensure employee productivity is not impacted, many cloud teams will grant permissions broadly. Employees may only use one or two of these permissions to access the information they need, meaning the other permissions assigned to them are unused. This expands the attack surface and provides additional tools for hackers to use to penetrate your cloud. LMNTRIX XDR CLOUD automatically detects all the permissions that are assigned to users/groups/roles and analyzes their usage. This information is presented to your team so they can revoke permissions if needed and reduce the attack surface.

Effectively Implement Security Best Practices

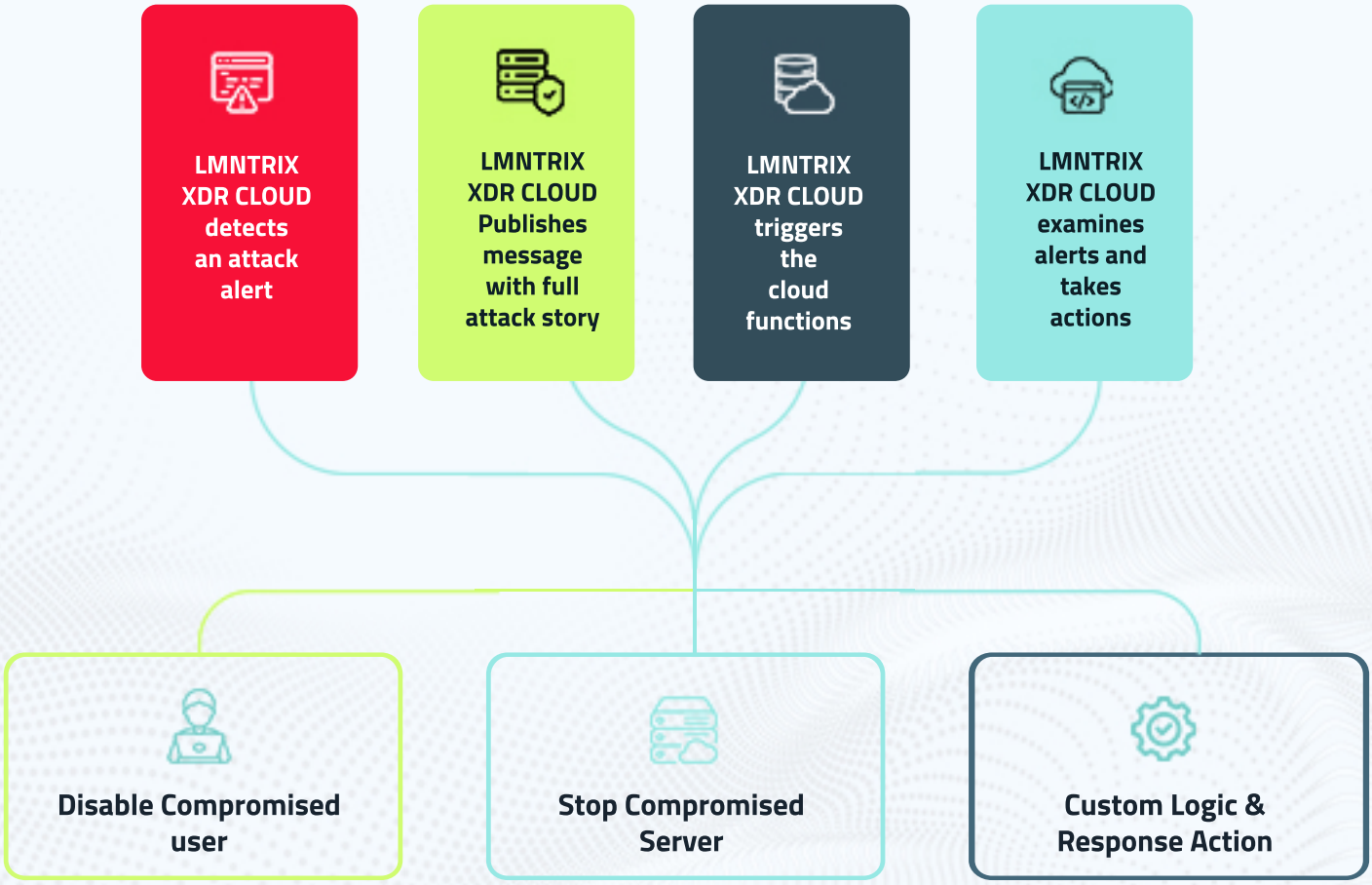
Managing security processes to ensure that your cloud security framework adheres to best practices is not an easy task. LMNTRIX helps ensure compliance with one-click reporting across a variety of common industry standards, with detailed visual reports on where you are successful and where you need to do some work. An additional layer of protection is delivered with custom governance enforcement via a query language for custom rules.

LMNTRIX's XDR Cloud continuously monitors and alerts on potentially dangerous misconfigurations such as public exposure of assets,authentication misconfigurations, password policy, logging, networking, monitoring, and encryption. Alerts deliver granular details including the affected assets, users, and the compliance rules being violated.



User-Defined Automated Response

Automated response within LMNTRIX XDR CLOUD addresses compliance/governance issues (aka misconfigurations), public exposures, and realert. You define rules within the LMNTRIX XDR CLOUD platform and only execute them if all the criteria are met.



Security analysts create remediation rules with specific configurations to resolve various issues such as public exposures or misconfigurations. Auto-remediation is an optional capability, and is rule based allowing you to decide if and when to execute remediation actions.

A Complete Picture of Cloud Risk

LMNTRIX XDR CLOUD takes a comprehensive approach to threat detection and response. It analyzes the configuration of your environment and all enabled permissions to fully assess the attack surface. It then analyzes the runtime within the environment, so your team can see which misconfigurations orpermissions are compromised and are being exploited – shutting down these vulnerabilities is where your team needs to start. This is the level of security analysis that LMNTRIX XDR CLOUD provides. Understanding where your vulnerabilities are, clarifies how and when your vulnerabilities are being exploited.

LMNTRIX XDR CLOUD not only provides a complete analysis of static configurations, it reveals risky behavior in the runtime so you can stop attacks in their tracks fast. AI and ML driven models create the right context for your business for your cloud, applications, and users, so that alerts are actual threats and not just anomalies or one-offs. The overall productivity of the team is greatly improved as they are focusing on real alerts, and not chasing random activities