LMNTRIX
BE THE HUNTER | NOT THE PREY

ThinkGrid

SIEM AT THE SPEED OF LIGHT

ACTIVE DEFENSE

ZERO HYPE

ZERO FALSE POSITIVES

ZERO EXCUSES

LMNTRIX US.
333 City Blvd West. Suite 1805
Orange, CA 92868 USA
+ 1.888.958.4555

LMNTRIX HONG KONG.
Room 1102, 11/F, Kenbo Commercial Building
333-339 Queen's Road West, Sai Ying Pun. Hong Kong
+ 852.580.885.33

LMNTRIX UK.
Kemp House, 152 - 160 City Road.
London, EC1V2 NX
+ 44.808.164.9442

LMNTRIX AUSTRALIA.
Level 5. 155 Clarence St
Sydney. NSW.
+61.288.805.198

LMNTRIX SINGAPORE.
60 Kaki Bukit Place # 05-19
Eunos Techpark
+ 65.3169.0639

LMNTRIX
BE THE HUNTER | NOT THE PREY

Organizations are fighting an asymmetric battle. Adversaries are elusive, polymorphic, well-funded and able to bypass legacy security technologies to exfiltrate your most critical data. Organizations are understaffed, overwhelmed with alerts and lack the visibility and information they need to detect and investigate cyber threats.

LMNTRIX is transforming detection and incident investigation with our cloud based threat analytics platform - ThinkGrid. ThinkGrid provides enterprise-wide visibility and codified detection expertise to amplify your defense against today's most sophisticated cyber attacks.

TRADITIONAL SIEM IS NO LONGER ENOUGH

Since the early 2000s, Security Information and Event Management (SIEM) has been the go-to security model for the early detection of targeted attacks and data breaches. SIEM combines Security Information Management (the storage and analysis of log data) and Security Event Management (monitoring, correlating, and notification of security events) to help organizations deal with threat detection and response.

However, SIEMs have been unable to keep pace with the security needs of modern enterprise. As early as 2014, Gartner analyst Oliver Rochford said "Implementing SIEM continues to be fraught with difficulties, with failed and stalled deployments common."

As the volume, complexity, variety, and speed of data continues to increase, traditional SIEMs cannot keep up. Modern malware, data breaches, and security threats are incredibly complex, and they require a more proactive, agile approach to security infrastructure.

THE LMNTRIX SOLUTION TO SIEM

SIEM systems work well to defend against known threats with fixed perimeters and signature-based security. But how does this approach translate to today's cloud-focused, dynamic landscape?

Organizations still shell out more than $1.5 billion annually for SIEM services—but they are still struggling to fend off modern threats. Rule-based and signature-based security systems have failed to prevent the most serious data breaches of the last several years.

LMNTRIX uses advanced security analytics for more robust, scalable security. Security analytics uses machine data to pinpoint anomalies and view resource usage in real-time, allowing you to make fast, informed decisions about complex security threats. Machine data is helping IT teams bring better context to data and create actionable intelligence, which is crucial in the ever-evolving digital security landscape.

HIGHLIGHTS

PURPOSE-BUILT – The cloud-based platform was built by security practitioners for security practitioners

ANSWERS, NOT ALERTS – identify known and unknown threats by applying real-time threat intelligence to enterprise event streams

CODIFIED DETECTION EXPERTISE – enhance detection and investigation capabilities with codified expertise from LMNTRIX security researchers and data scientists

MACHINE LEARNING FOR THREAT DETECTION – identify unusual network activity or user behavior to pinpoint attackers before they do damage.

SUB-SECOND SEARCH – improved search time across billions of events helps security analysts proactively hunt for covert behavior on the network

RAPID DEPLOYMENT – operational in hours instead of months or years

EASILY SCALABLE – elastic, cloudbased infrastructure makes it easy for organizations to scale as business needs or seasonal requirements change

PREDICTABLE COSTS
software-as-service provides predictable operating expense for software, support, infrastructure, threat intelligence and security expertise

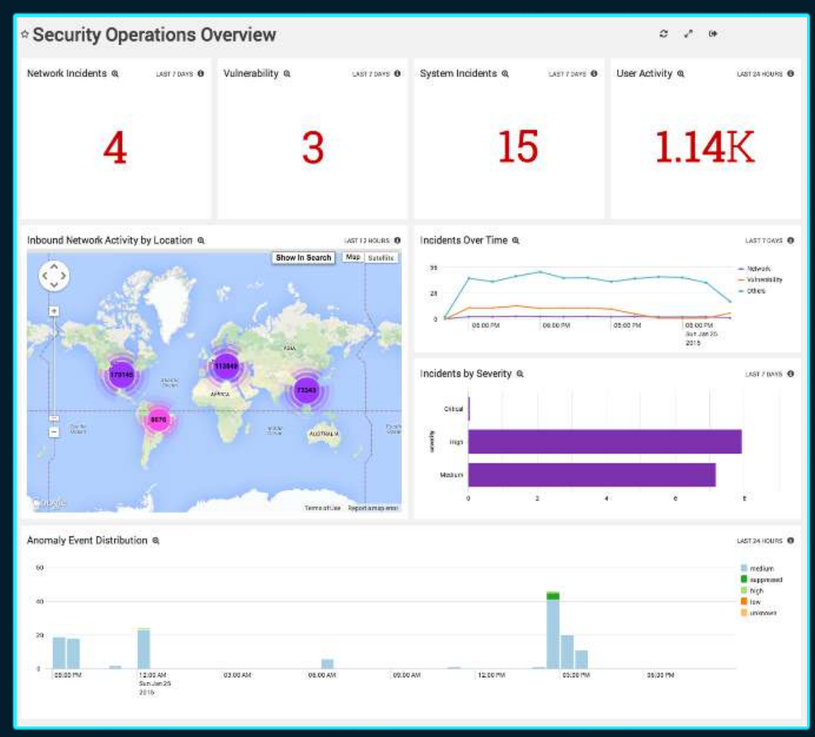
LMNTRIX
BE THE HUNTER | NOT THE PREY

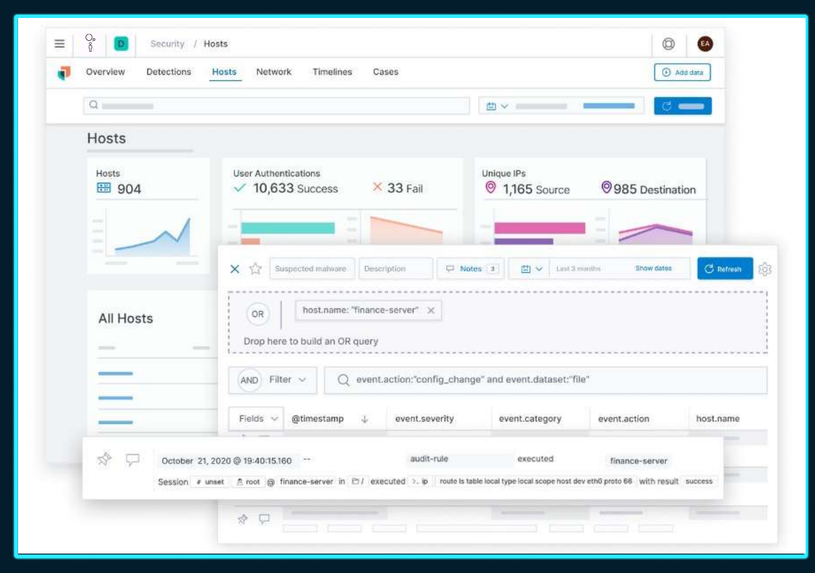
USE SECURITY ANALYTICS TO AUTOMATE THREAT DETECTION

Enterprise security teams typically use SIEM solutions to perform two main functions:

- Analyze security event data in real-time
- Collect, store, and analyze log data for incident forensics and regulatory compliance

Modern companies have transitioned to using microservices, container services, and cloud-based technology to drive innovation and continuous development. The continuous innovation model requires several layered components, including the operating system, applications, storage devices, servers, workstations, and more. Traditional SIEM architecture is not built to handle this volume and variety of data, leading to significant challenges in analyzing and reporting data. This is where ThinkGrid comes in.





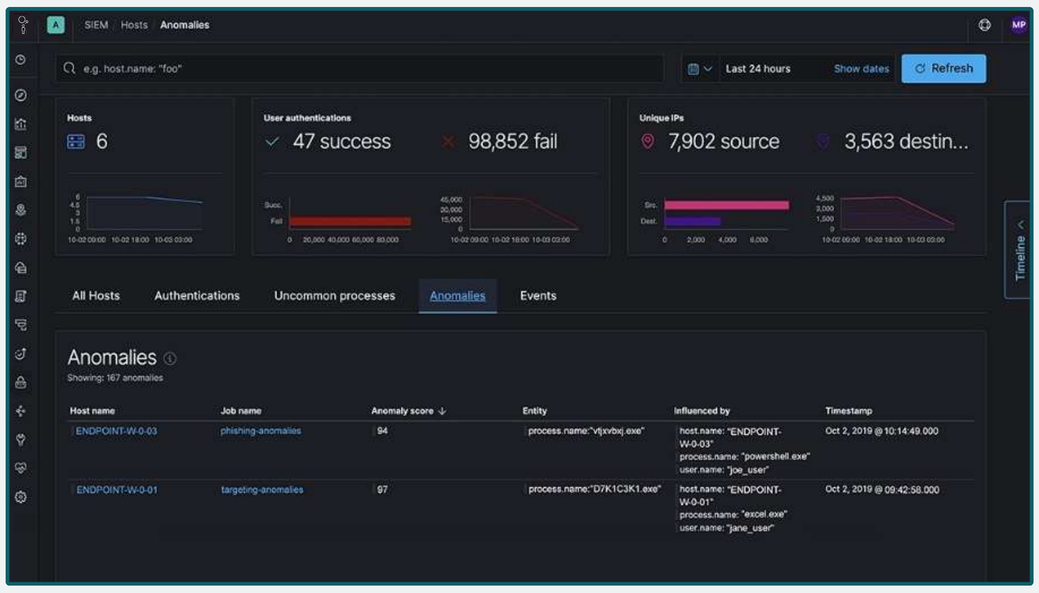
WHY CHOOSE THINKGRID FOR SECURITY ANALYTICS?

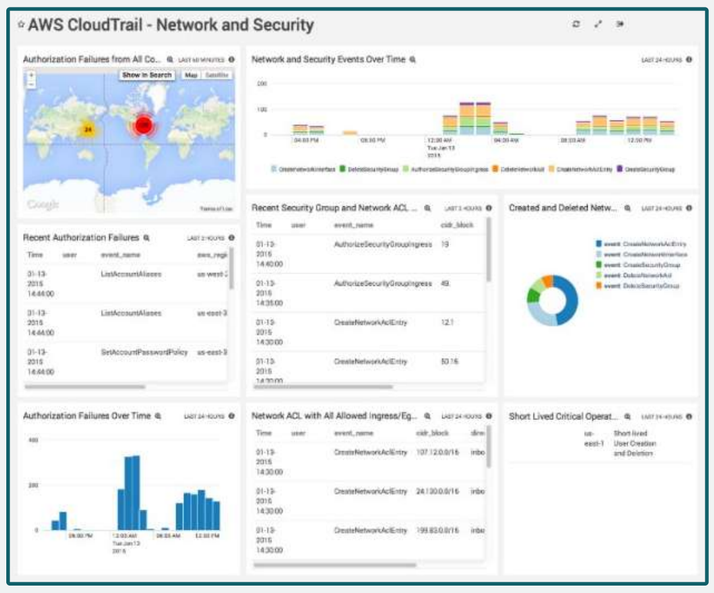
With LMNTRIX Active Defense, we don't use a SIEM to detect and respond to advanced threats. However, we do recognize the need for a SIEM to meet log management and compliance requirements and as such we offer an onsite Managed SIEM Service or a cost-effective cloud option Security-aaS to replace your SIEM – we call it ThinkGrid.

Offered as an optional extra to Active Defense, LMNTRIX ThinkGrid is the fastest and most scalable analytics based SIEM on the planet. By allowing unlimited log collection, LMNTRIX ThinkGrid is ideal for large log management and compliance use cases. ThinkGrid Onsite can be deployed on Google Cloud, Azure, AWS, OpenStack or in-house otherwise you can subscribe to ThinkGrid Cloud.

Our use of machine learning algorithms means our platform gets smarter every minute while also eliminating the need for clients to write rules or create thresholds. By analysing your data in order to find discrepancies and unorthodox behavior, our platform is able to link these anomalies together, joining the dots and uncovering the truth behind advanced threat activity. Critically, in order to ensure accuracy, our algorithms are based on your data because the only way we can know what is "abnormal", is to know what's "normal" for your organization.

While SIEM can only identify known events, ThinkGrid uses machine learning algorithms to identify abstract relationships, anomalies, and trends.





With ThinkGrid, your IT teams can:

- Match log data with threat intelligence data to identify and visualize malicious IP addresses, domain names, email addresses, URLs, MD5 hashes, and more
- Leverage real-time infrastructure monitoring to help you ward off impending threats
- Benefit from machine learning algorithms that automatically uncover unknown security events
- Protect data with end-to-end encryption and platform certifications
- Scale automatically to optimize performance
- Analyze centralized data on easy-to-read, intuitive dashboards

ThinkGrid offers behavior modeling and predictive analytics, helping you look holistically at the entire stack—without relying on rules or predefined schemas. LMNTRIX's focus on advanced security analytics allows organizations to move beyond the limitations of traditional SIEM.

THINKGRID MACHINE LEARNING USE CASES

THEAT INDICATOR CATEGORY	HELPS YOU IDENTIFY	...BY FINDING ANOMALIES IN...
Data Exfiltration	Credit card, health record theft	Firewalls, web proxies, secure gateways, DNS logs
Malware Command & Control Activity	Infected systems beaconing	Firewalls, web proxies, DNS request logs
Compromised Endpoints	Spreading malware internally	EDR/AV logs, Netflow records
Suspicious Server Behaviors	New bit torrents, chat rooms, file services	Process starts, network connects
Suspicious Account Activity	Account creation, privilege changes	Process starts, network connects
Unauthorized Login Attempts/Activity	Smart brute force attacks	Servers, directories, audit logs
Unusual IDS/IPS Events	Unusual security threats	IDS/IPS, IDP, NGFW logs
Disabled/Interrupted Logging	Attempts to hide tracks	All types of log data
Unusual Network Activity	DDoS attack, excessive DNS requests	Firewalls, web Proxies, secure web gateways, Netflow, DPI logs
Abusive/Attacking IP Address	External data scrapers, internal snoopers	Firewalls, web proxies, secure web gateways, Netflow, DPI logs

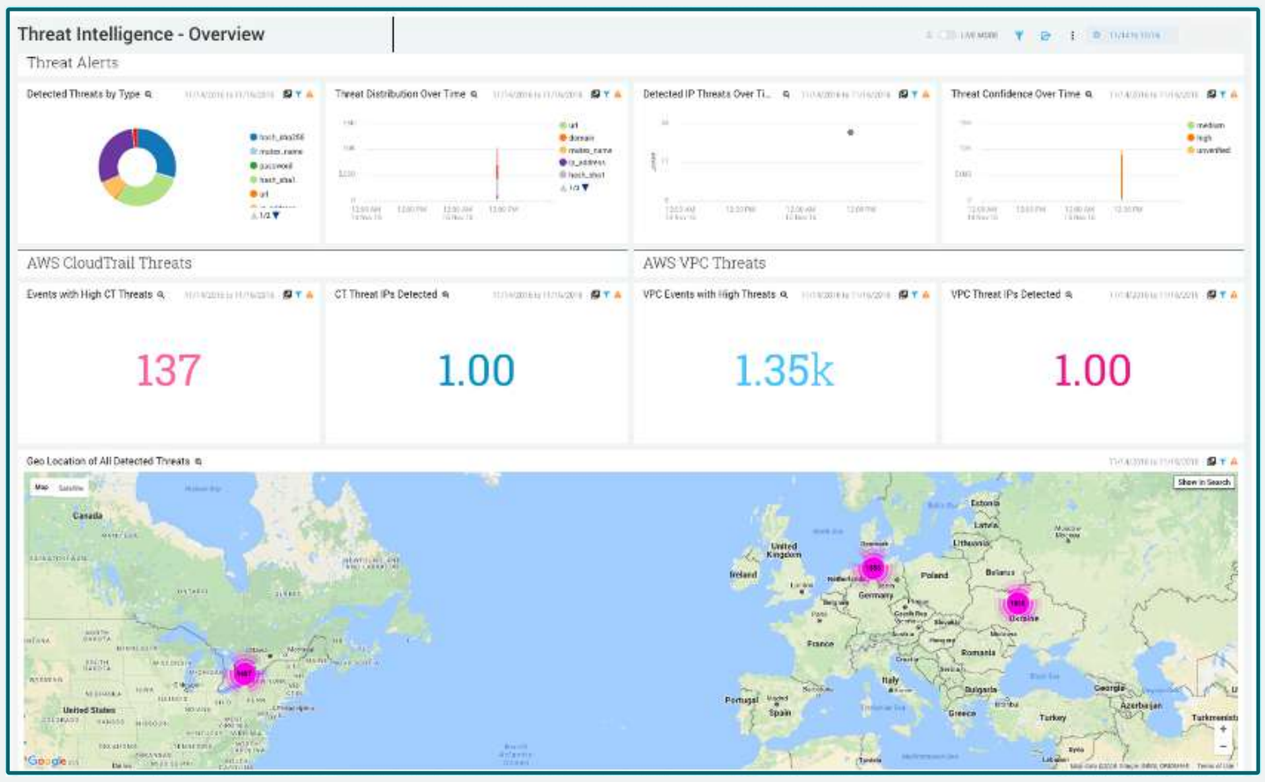
LMNTRIX
BE THE HUNTER | NOT THE PREY

IDENTIFY & PRIORITIZE THREATS TO ELIMINATE 'ALERT FATIGUE'

When the volume of modern security threats meets outdated security infrastructure, it creates "alert fatigue." With so many alerts and so much noise, how does your security team manage and prioritize their efforts?

ThinkGrid generates actionable, high-fidelity alerts through unified logs and metrics, automatically identifying and prioritizing threats—without admins setting policies or rules. ThinkGrid ingestion is data-agnostic, and customizable dashboards make it simple to drill down to individual events (and correlated events).

ThinkGrid also removes the need to invest in hardware and manpower so resources can be spent finding and resolving security issues. And because our technology was designed for cloud security, it easily scales to meet the needs of even the largest enterprises.



BUILT BY SECURITY PRACTITIONERS

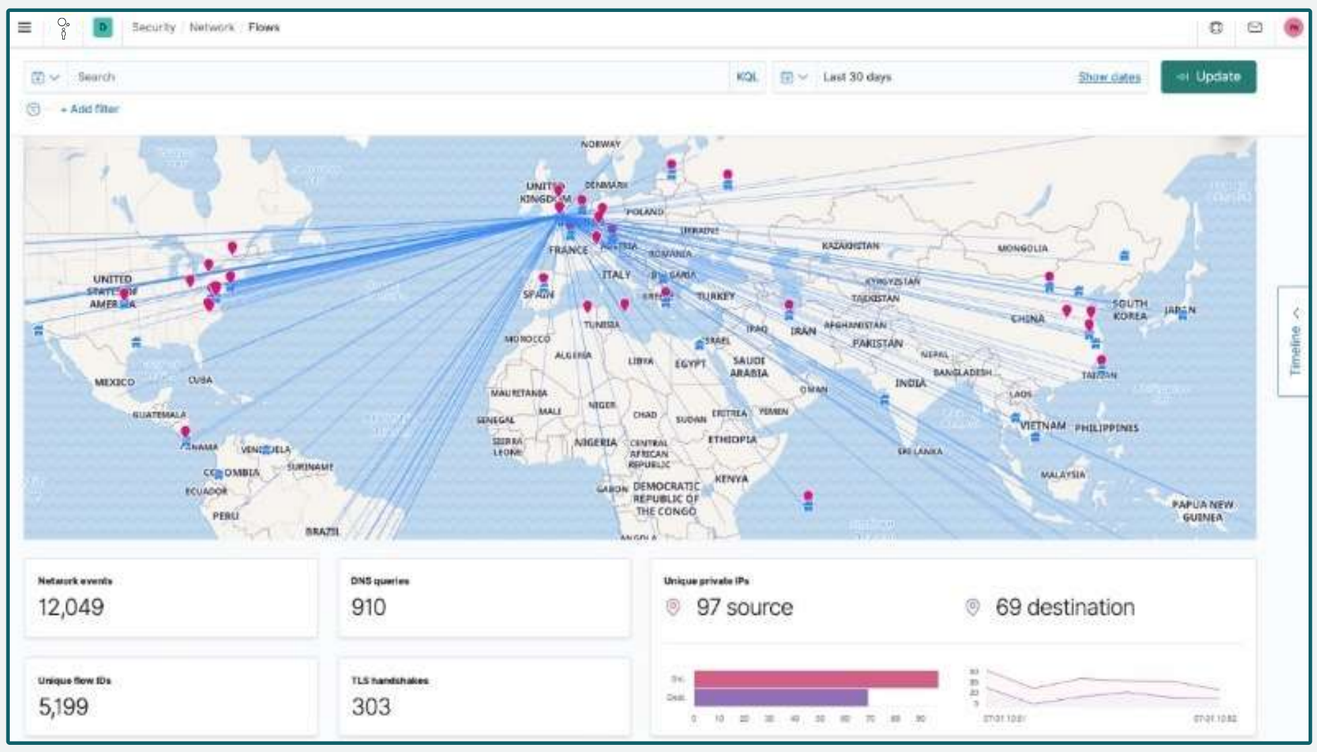
LMNTRIX built ThinkGrid from the ground up — by security practitioners, for security practitioners. ThinkGrid combines threat insights gained from responding to the worlds' most consequential breaches with big data security analytics and codified security expertise so you can quickly identify and investigate cyber threats.

ADAPTIVE DETECTION

Your adversaries are constantly changing. Your detection and investigation capabilities must evolve just as quickly. LMNTRIX has a dedicated ThinkGrid team made up of data scientists and security researchers that codify extensive front-line incident response experience into detection rules, and behavioral analytics. Within hours of discovering an emerging attack, they create new rules and perform retrospective analysis of your environment to determine the potential impact and feed these rules back into the ThinkGrid platform. Upon discovering malicious activity, ThinkGrid generates alerts enriched with supporting data, such as attacker context, to aid the investigator in validating and scoping the incident.

ENTERPRISE-WIDE VISIBILITY

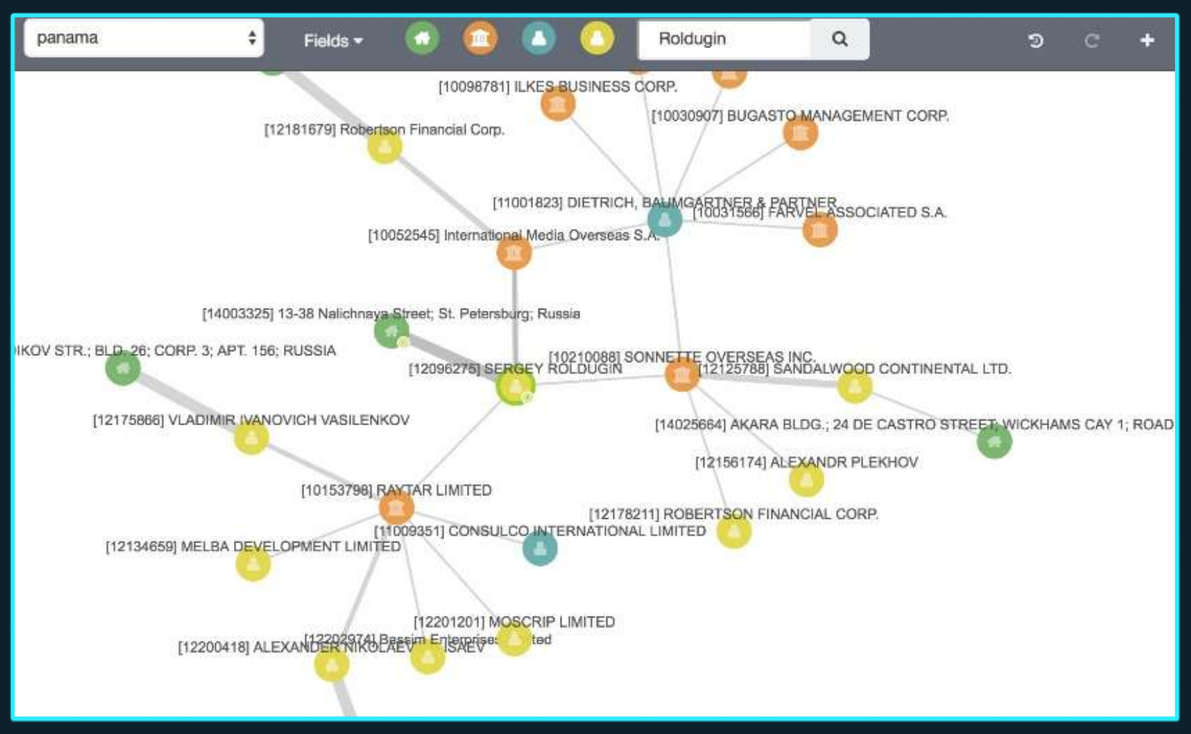
Your attackers can enter anywhere. You need visibility everywhere. ThinkGrid provides enterprise-wide visibility by aggregating alerts from the diverse range of security technologies throughout your organization. With ThinkGrid, you can centrally analyze information like logs, flows, and contextual data from across your environment — no matter how disparate your data sources. Our thin network sensors provide real-time visibility to distributed environments, aggregating events from remote locations and sending them to a centralized location for log retention, threat analysis and investigation.

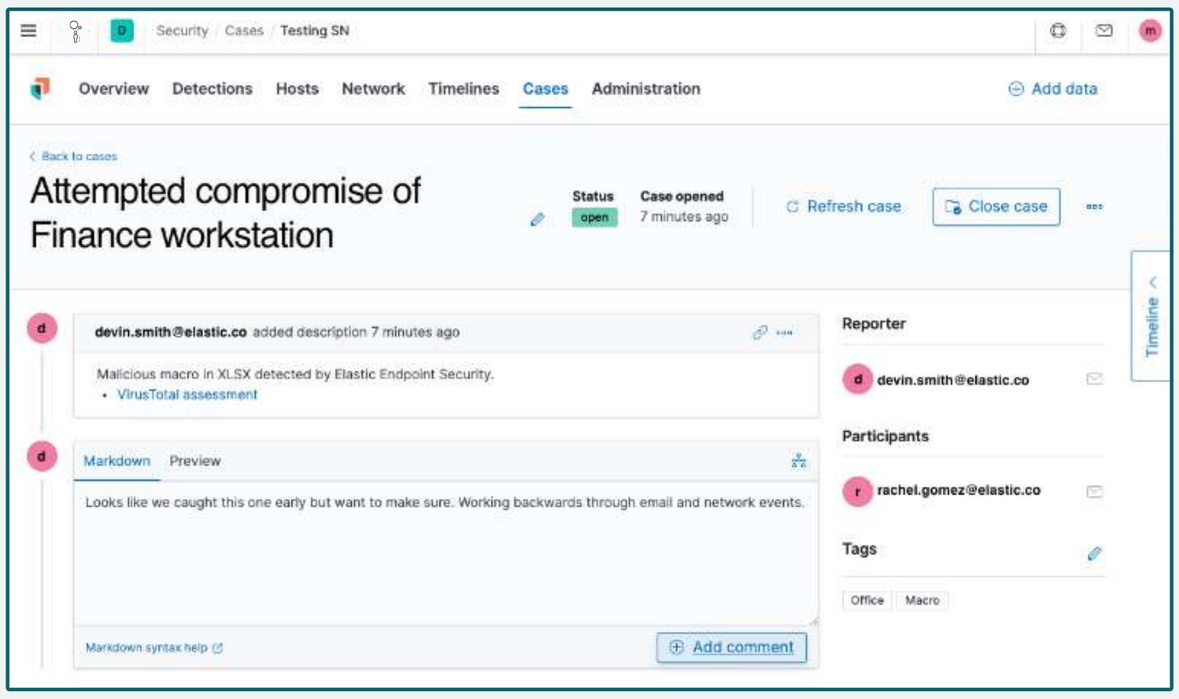


GRAPH ANALYSIS FOR THREAT ANALYSIS

Your team's ability to respond to an ever-increasing number of cyber attack is stretched to the breaking point. You need a dramatic increase in security operations productivity and effectiveness that will accelerate your incident response lifecycle.

There are potential relationships living among your logs and data; linkages between documents, IP addresses, users, people, places, preferences, products, you name it. ThinkGrid Graph Analysis offers a relationship-oriented approach to security that lets you explore the connections in your data using the relevance capabilities of ThinkGrid.



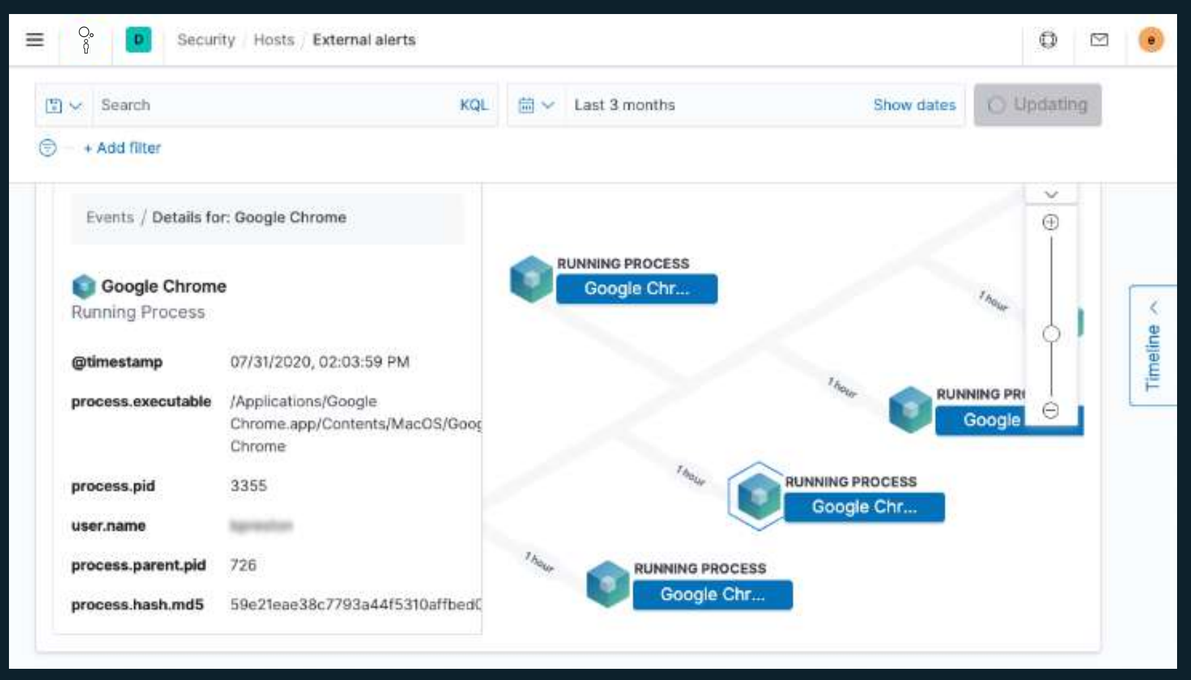


SECOPS AND THREAT HUNTING ARE TEAM SPORTS

ThinkGrid provides an interactive workspace for security teams to triage events and perform initial investigations. Monitor for threats, gather evidence on a timeline, pin and annotate relevant events, and forward potential incidents to ticketing and SOAR platforms.

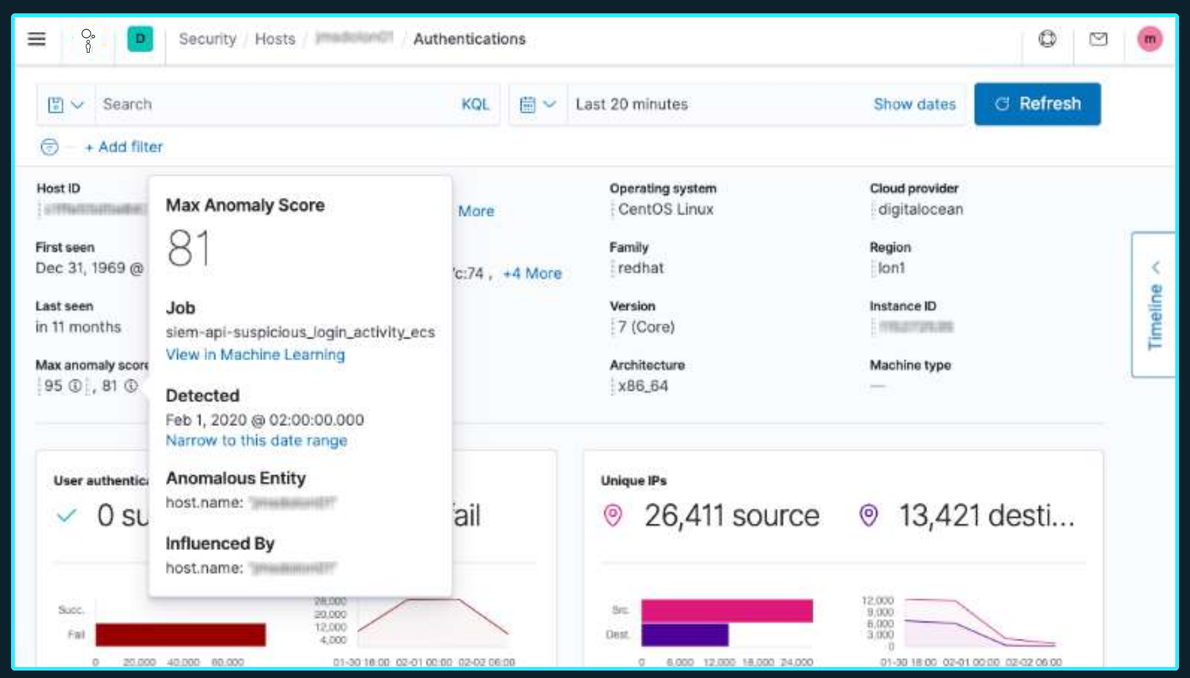
GAIN VISIBILITY INTO YOUR ENVIRONMENT

WThinkGrid allows you to view your data on interactive dashboards and maps. Perform graph-based relationship analysis. Search across information of all kinds. Do it all with the technology fast enough for the sharpest analysts.



AUTOMATE DETECTION WITH ATT&CK-ALIGNED RULES

With ThinkGrid Cloud you can continuously guard your environment with correlation rules that detect tools, tactics, and procedures indicative of potential threats. Cut to what matters with preconfigured risk and severity scores. Content is aligned with the MITRE ATT&CK knowledge base and ready for immediate implementation.



DISCOVER COVERT ACTIVITY

When an adversary evades detection, there is no evidence of compromise, no starting point for your investigation. To discover emerging attack campaigns, you must pre-emptively search for evidence of covert behavior. ThinkGrid enables nimble data exploration via sub-second search across billions of events so security analysts can proactively hunt for hidden indicators of compromise. Once identified, agile investigation tools help analysts pivot from one indicator to the next, evaluate the full context of newly discovered artifacts, reconstruct the attack storyline and ultimately limit the impact of the breach.

SIMPLIFIED DEPLOYMENT EXPEDITES TIME TO VALUE

ThinkGrid requires minimal onsite configuration, simplifying deployment and eliminating costly professional services engagements. Our elastic, cloud-based infrastructure scales seamlessly, allowing you to adapt faster as business needs or seasonal requirements change. The ThinkGrid subscription includes software, support, infrastructure, threat intelligence and codified security expertise, ensuring predictable operating expense.

FEATURES	THINKGRID ONSITE	THINKGRID CLOUD
	PLATFORM FEATURES	
Data ingest & transformation	YES	YES
Data retention	Client managed	3 months online – 9 months offline
Search & Analytics	YES	YES
Data visualization & dashboards	YES	YES
Reporting (PDF & PNG)	YES	YES
CSV Exports	YES	YES
Host security analysis	YES	YES
Network security analysis	YES	YES
Timeline event explorer	YES	YES
Case management	YES	YES
Detection engine	YES	YES
Prebuilt detection rules	YES	YES
Detection rule alerting	YES	YES
Machine learning anomaly detection	NO	YES
Prebuilt anomaly detection jobs	NO	YES
Graph analysis	NO	YES
LMNTRIX intelligence feed integration	YES	YES
Operations & management	YES	YES
Data exploration & visualization	YES	YES
Observability for unified visibility across your entire ecosystem	YES	YES
Application performance monitoring	YES	YES
Live tail for streaming logs	YES	YES
Metrics for infrastructure monitoring	YES	YES
Uptime for application & service monitoring	YES	YES
Maps for analyzing geospatial data	YES	YES
Encrypted communications	YES	YES
Role-based access control	YES	YES
Single sign-on (SAML)	NO	YES
Encryption at rest support	NO	YES
FIPS 140-2 mode		
Orchestration	NO	YES
Audit logging	NO	YES
IP filtering	NO	YES
LDAP, PKI1, Active Directory authentication	NO	YES
Single sign-on (SAML, OpenID Connect, Kerberos)	NO	YES
	OPERATIONS & SUPPORT	
Managed platform	YES	YES
Security monitoring	By client or partner	By client or partner
Support coverage	Business Hours	Business Hours
Unlimited # of incidents	YES	YES
Web, Slack and phone support	YES	YES
Emergency patches	YES	YES
Hosting	On-premise (client supplied infrastructure)	LMNTRIX Cloud (AWS)
Redundancy (clustering)	YES (client supplied infrastructure)	YES
Remote Training (1-week)	YES	YES
Hot-warm architecture, with automated index curation	YES	YES
Automated snapshots (every 30 min)	YES (client supplied infrastructure)	YES
Disaster recovery	YES (client supplied infrastructure)	YES