WHITE PAPER

Zero Pain, All Gain. Winning Customers' Hearts and Minds

LUCIDUM

NOW PART OF cyderes

Introduction

Lucidum is the industry's only comprehensive, intelligent, and efficient security data fabric pipeline that includes:

- 750+ connectors to security, IT, cloud, and other sources of data;
- Significant, user-friendly transformation machine-learning functions with five patents (four pending);
- Integrations with SIEM, Risk, Threat, Data, Ops platforms and all cloud providers;
- Set up, configuration, and integration within minutes, not weeks or months.

MSSPs face risks that affect their bottom lines. These risks include undetected security threats, incomplete asset visibility, poor or failed service delivery, and ensuring customers comply with ever-changing regulations.

When an MSSP cannot address 100% of security threats, cannot see and monitor 100% of a customer's environment, or fails to deliver outstanding service, customers become dissatisfied. Unhappy customers reduce NPS (net promoter score), search for another MSSP (churn), and can harm an MSSP's reputation. All of this negatively affects margin, reputation, and profitability.

Lucidum MSSPs eliminate these risks and create happy, loyal customers and improved NPS.

MSSPs' Worst Fears with Their Customers

As security providers, one of the top risks to an MSSP is **missing a security threat or inadequately responding to a security threat** in a customer's environment. As cyber threats increase in number and sophistication, this risk becomes the top-priority to both MSSPs and their customers. If an MSSP fails to detect and mitigate a threat, customers lose trust in the MSSP, the MSSP's reputation is damaged, and customers can potentially leave the MSSP.

Incomplete asset visibility is another risk for MSSPs. Ephemeral assets (containers, serverless functions, Infrastructure as Code), virtual machines, unmanaged assets (IoT/OT devices and development and testing environments), zombie users, and non-human accounts create blind spots for MSSPs. If an MSSP cannot see an asset, user, or application, an MSSP cannot protect that environment, but the customer still blames them. These unknown and unmanaged assets increase the attack surface, do not comply with security policies and compliance policies, and increase the risk of unauthorized access and data leaks.

Most MSSPs promise SLAs (service-level agreements), a service contract between the MSSP and the customer. SLAs can include Time to Onboard, Time to Notify for Zero-Day Vulnerabilities, Mean Time to Quarantine (MTTQ), and Mean Time to Resolution (MTTR). When an MSSP **fails to meet SLAs,** the MSSP loses customer trust and usually must pay a financial penalty (reduced fee or service credits to affected customers).

Regulations and laws that protect privacy, data, and financial information continue to proliferate. Customers look to MSSPs to help them comply with laws and regulations, for example HIPAA, PCI DSS, FISMA, Sarbanes-Oxley, and GDPR. **Non-compliance or faulty compliance** is a risk for MSSPs. Non-compliance or faulty compliance can result in legal and financial penalties for the customer and the MSSP.

The Cost of These Problems

When an MSSP does not detect and mitigate security threats, has incomplete asset visibility, has poor or failed service delivery, or fails to ensure compliance with regulations, the MSSP suffers financial losses, damage to their reputation, and declining net promoter score (NPS).

There are two ways an MSSP can suffer financial losses due to risks: direct loss and churn. When an MSSP fails to ensure compliance for one or more customers, the MSSP and its customers are subject to fines and legal repercussions. When an MSSP cannot deliver asset visibility, security management, SLAs, or compliance, customers lose trust in the MSSP. This lost trust can also lead to customer churn.

MSSPs that do not mitigate risks (undetected security threats, incomplete asset visibility, failed SLAs, and failed compliance) also suffer damage to their reputations. Dissatisfied customers can leave negative online reviews, spread negative word-of-mouth, and make it more difficult for MSSPs to acquire new customers and grow existing customers.

When dissatisfied customers leave negative online reviews and spread negative word-of-mouth, net promoter score (NPS) decreases. Many MSSPs use net promoter score (NPS) to measure customer experience and predict business growth. MSSPs that do not rectify risks create unhappy customers. Unhappy customers become detractors and hurt an MSSP's NPS. Low NPS scores harm business growth and profitability.

How Lucidum Dissolves These Issues

Lucidum MSSPs diminish and mitigate both customer and business risk.

Lucidum is agentless and ingests read-only API data from IT, operations, development, business, network, security, and HR solutions, and structured and unstructured data from data lakes. Lucidum uses ingested data, ML algorithms, rules-based algorithms, texting mining, and network graph analysis to normalize data, deduplicate records, and find relationships between assets, users, and data. Integrating data from over 700 sources and using patented AI and ML, Lucidum allows MSSPs to **see all assets, all users, all data, all relationships, and the current security posture of the customer, including risks, threats, vulnerabilities, and misconfigurations.**

Lucidum allows MSSPs to dynamically update this inventory data as the customer's environment changes. With no blind spots, no unknown devices, no shadow IT, Lucidum helps MSSPs provide 100% security coverage. Lucidum performs ingestion and applies ML algorithms to ingested data at least once a day and more frequently if required. Lucidum then updates asset records and user records that have changed (delta). Lucidum also updates the vulnerability reference tables that include consolidated CVE data from all the major security organizations. Lucidum also keeps a record of changes for each asset, user, and vulnerability. Users can view this record of changes.

LUCIDUM

Lucidum ingests data from IT, operations, development, business, network, security, HR solutions, and data lakes. The more data Lucidum ingests, the better the security insights. Lucidum then uses the ingested data, ML algorithms, rules-based algorithms, text mining, and network graph analysis to populate security data for each asset and user. For example, Lucidum finds CVE data about assets by ingesting data from endpoint software and vulnerability software. After ingestion, Lucidum uses ML to triangulate and build relationships between all the ingested data. Lucidum uses the results of ingestion and ML to enrich data for assets, users, and vulnerabilities. MSSPs that use Lucidum can take advantage of full visibility of assets, users, and data to continually determine where vulnerabilities and known exploited vulnerabilities exist, find unexpected configuration changes, find unprotected or unauthorized users, and find risks throughout the environment. Lucidum MSSPs **monitor security risks and quickly respond to emerging threats and vulnerabilities on each and every system** and identity in the customer's environment.

Lucidum MSSPs automatically prioritize and fulfill compliance tasks. With Lucidum, MSSPs automatically monitor compliance requirements like endpoint protection, MFA, IAM, Privileged Access Management (PAM), VPNs, patch management, backups, anti-virus solutions, firewalls, encrypted and unencrypted storage, data governance, and configuration changes. Because Lucidum ingests all the data from your environment and uses ML to infer relationships and enrich records, Lucidum MSSPs can automatically find devices that do not meet compliance requirements. Lucidum also includes a feature called Actions. Actions are no-code automations that automate compliance tasks. MSSPs can use Lucidum to **automatically monitor all compliance requirements and to automate remediation tasks,** allowing technical staff to concentrate on value-added work while adhering to regulations.

MSSPs that use Lucidum will gain operational efficiency by automatically auditing assets, users, and security posture. Lucidum also allows MSSPs to automate security tasks, like installations, updates, patching, quarantining assets, starting and stopping assets, launching vulnerability scans, editing AD properties, creating tickets, and sending data to external systems like Slack, Jira, and SIEMS and SOARs Lucidum includes Actions, no-code automations that use webhooks and APIs.

LUCIDUM

These automations improve resource allocation and productivity. With Lucidum, MSSPs can improve SLAs like Time to Onboard, Time to Notify for Zero-Day Vulnerabilities, MTTQ (mean time to quarantine), and MTTR (mean time to resolution). Lucidum provides a detailed view of each customers environment that helps MSSPs quickly onboard new customers, immediately identify assets at risk for zero-day vulnerabilities, and immediately identify assets and users that require quarantine. Lucidum's powerful automations allow MSSPs to automatically respond to security threats, reducing MTTR.

When MSSPs have full visibility into a customer's environment, full visibility into a customer's security posture, and automations that aid compliance and SLAs, customers have increased satisfaction, and MSSPs foster long-term relationships with customers.

Direct and Effective Client Success with Lucidum

Lucidum MSSPs not only mitigate risk but also build strong, positive relationships with customers.

MSSPs that use Lucidum deliver superior service, with quicker onboarding, proactive monitoring and remediation, and hardened SLAs. Superior service creates satisfied customers.

Lucidum's patented Risk Score System is customized to each customer's unique needs, to help MSSP technical staff prioritize tasks that are most important to the customer. Lucidum uses externally valid data and ML to measure risks for assets, users, and data. Lucidum then populates risk fields for assets (Risk Factors, Risk Score, Risk Ranking and Risk Level), for users (Risk Score, Risk Ranking, and Risk Level) and for data (Data Risk). Lucidum MSSPs can use patented SmartLabels, centrally managed, variable-driven, dynamic tagging and transformations, to further customize risk measurements and priorities.

Lucidum MSSPs provide a customized experience for each customer during status updates and regular business reviews. During QBRs (quarterly business reviews), Lucidum MSSPs can present hundreds of data points showing improvements made in the last 90 days. MSSPs can also use Lucidum dashboards (or display Lucidum data in their preferred reporting application) to provide insight into the customer's current security posture and make strategic recommendations to the customer.

LUCIDUM

This opens new revenue and engagement opportunities to recommend services, security maturation, and cross-sell. MSSPs make Lucidum dashboards available to customers on-demand with their own branding.

With Lucidum, MSSPs offer superior services, provide measurable improvements to the customers' security posture, and offer security thought-leadership for their customers. The superior service and transparent communication lead to higher customer retention, enhanced reputation, and business growth.

Conclusion

Lucidum helps MSSPs mitigate both customer and business risk, delivering superior and competitive service that their customers and prospects desire.

MSSPs that use Lucidum automatically monitor security risks and quickly respond to emerging threats and vulnerabilities. Lucidum MSSPs see all assets, all users, all data, all relationships, and the current security posture of the customer, including risks, threats, vulnerabilities, and misconfigurations. This view is updated automatically as the customer's environment changes.

Lucidum helps MSSPs improve SLAs like time to onboard, time to notify for zero-day vulnerabilities, MTTQ, and MTTR. And Lucidum's automations help MSSPs achieve operational efficiency that leads to superior service. Lucidum MSSPs automate compliance audits and automate remediation tasks.

Lucidum MSSPs provide a superior, customized experience for each customer.

Get the competitive edge that 100% visibility, unmatched coverage, improved SLAs, and automated compliance provides. Contact Lucidum to schedule a demo today.

LUCIDUM