WHITEPAPER

# What Competition? Your MSSP's Secret Weapon

LUCIDUM

# 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.

According to channelinsider, the global MSSP market is projected to grow at a 15.4% CAGR (compound annual growth rate) until 2030. To capture this growing and competitive market, MSSPs need to show value on day-zero (during sales demonstrations and free trials) and deliver value on day-one. But the challenges include:

- slow onboarding that can take anywhere from 30 days to 6 months and even then, might not provide an accurate view of the customer and their security posture.
- initial remediation and compliance requirements that are discovered **after** onboarding (30 days to 6-months after the contract is signed) .
- a customer that is not supportable or generating revenue for the MSSP until after onboarding and remediation are completed.
- continual manual work to audit changes to the customer environment, especially amidst emerging threats.
- missed opportunities for finding whitespaces and upselling due to tight budgets and overworked staff.

With these challenges, MSSPs can end up over-spending on onboarding and over-spending on support, which reduces margins and decreases customer confidence and NPS scores. Lucidum allows MSSPs to automatically generate a complete view of each customer's assets, users, and security posture, including inventory details (for example, data classification, application inventory, asset ownership) and security details (for example, risks, threats, and active vulnerabilities).
All on day-zero.

# Precision Quoting, Maximum Trust

With Lucidum, MSSPs automatically generate an accurate and complete view of a prospective customer's environment.

On day-zero, Lucidum empowers MSSPs to see all assets, all users, asset ownership and data ownership, data classifications, security risks, threats, vulnerabilities, and compliance misconfigurations. With this kind of visibility, Lucidum empowered MSSPs can offer precise, transparent quotes that build customer trust before a contract is ever signed.

Lucidum is agentless and ingests read-only API data from the solutions already in the customer's environment, including IT, operations, development, business, network, security, and HR solutions, and structured and unstructured data from data lakes. Lucidum uses the ingested data, ML algorithms, rules-based algorithms, texting mining, and network graph analysis to normalize data, deduplicate records, find "invisible" assets, and find relationships between assets, users, and data.

Competing and current MSSPs cannot provide a detailed, end-to-end inventory, or accurate security evaluations. However, your competitive distinction and unique value starts on day zero.

# Faster Onboarding, Maximum Margins

For MSSPs, onboarding a new customer is labor-intensive, slow, and costly. Most MSSPs onboard customers in 60-90 days. And for some large or complex customers, onboarding can take up to six months. No customers thoroughly understand their environment, and their current security team or MSSP doesn't, either.

Lucidum-empowered MSSPs reduce onboarding work to a few hours. Before a contract is signed, Lucidum-empowered MSSPs see all assets, all users, all relationships, and the current security posture of the customer, including risks, threats, vulnerabilities, and misconfigurations.

Lucidum finds all assets, users, and data, even "invisible assets" that the customer does not know about. Invisible assets are assets that are frequently overlooked by security and IT software. Invisible assets include ephemeral assets (containers, VMs), unmanaged assets (shadow IT, IoT assets, OT assets), zombie users , and non-human accounts (service accounts).

Lucidum triangulates and connects temporal values that might initially seem like mere data byproducts. By stitching together these data fragments, Lucidum identifies gaps that would otherwise be lost across different clouds, technology stacks, and user management systems.

Lucidum performs deep learning analysis to connect bits of data, such as IP addresses and user activity, from one technology set to another. This process reveals data stores, assets, and user accounts that would otherwise be overlooked.

Lucidum also leverages Network Graph Analysis to find "invisible" assets. This ML tool finds connectivity patterns and communication patterns within the network that reveal unknown assets like IoT devices and OT devices. Network Graph Analysis also finds isolated subgraphs in the network graph that frequently indicate shadow IT.

With unpleasant surprises out of the way, Lucidum-empowered MSSPs accurately plan onboarding, remediation and compliance work, and eliminate rework. This level of accuracy inspires customer trust, improves NPS, and increases margin.

# Providing a Better Customer Experience

Lucidum provides automated, real-time views of customer environments inside the MSSP's platform. 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 updates its vulnerability reference tables that include consolidated CVE data from all the major security organizations. Finally, Lucidum keeps a record of changes for each asset, user, and vulnerability.

As customer environments change and grow, Lucidum-empowered MSSPs automatically keep up with the changes, always seeing new assets, new users, new vulnerabilities, new threats, and new compliance issues. MSSP customers get seamless protection, and MSSPs get reduced workloads and increased revenue.
Lucidum-empowered MSSPs are never blind-sided by unmanaged assets, unmanaged users, or new threats and vulnerabilities.

During QBRs, Lucidum MSSPs not only demonstrate security improvements but can provide expert advice on infrastructure improvements. Lucidum MSSPs can use Lucidum dashboards (or Lucidum data in their current reporting platform) to show infrastructure and security improvements over time. In fact, Lucidum-empowered MSSPs can make these dashboards available to customers on-demand.

During QBRs, Lucidum MSSPs can show security improvements like:

- Number of CVEs discovered and their remediations.
- Number of KEVs and their remediations.
- Assets at risk and their remediations.
- Compliance violations and their remediations .
- All "invisible" assets that are now managed by IT and meet security requirements.

Lucidum MSSPs can also provide expert insights and suggest infrastructure improvements, like:

- identifying crown jewels, so the MSSP can prioritize these assets.
- Identifying idle cloud instances and possible cost savings.
- displaying a list of untagged cloud instances and suggestions for automated tagging with Lucidum.
- showing EC2 instances that are using the default security group  Lucidum-empowered MSSPs provide the vigilance that drives customer loyalty, improves NPS, and reduces churn.

# Generating Whitespace and Upselling

Lucidum-empowered MSSPs have a detailed, granular view of each customer's environment. This accurate, real-time view allows MSSPs to find whitespaces and upsell to the customer.

After ingesting read-only API data from the solutions already in the environment and applying ML algorithms to normalize data, deduplicate records, and find relationships between assets, users, and data, the transformed data is stored in the Lucidum Data Group (LDG).

The Lucidum Data Group (LDG) is the repository of deduplicated, normalized, enriched data for assets, users, and vulnerabilities. All transformed data is stored in the LDG.

Lucidum MSSPs can query the LDG to find all the assets or users where specific software or services are not running.

For example:

- As a customer adds more assets, Lucidum can find assets missing agents, create an automated action to install the agents on each asset, and bill the customer accordingly.
- As a customer adds more users, Lucidum can find users that are not using MFA, create an automated action to install the MFA software for each new user, and bill the customer accordingly.
- As a customer moves more assets to cloud-based infrastructure, the Lucidum-empowered MSSP can sell that customer more cloud management and cloud security services.
- As a customer migrates from one enterprise solution to another, the Lucidum-empowered MSSP can sell pro services to the customer. The Lucidum-empowered MSSP knows exactly which assets and users use the old system and need to migrate to the new system.

Because Lucidum includes powerful automations, Lucidum-empowered MSSPs can fill gaps with automated installations and updates, freeing up technical staff. The combination of upselling and automation leads to increased profit/loss ratios.

# Conclusion

With Lucidum, MSSPs can outclass the competition, with precise initial quotes on day-zero, dramatically reduced onboarding time, seamless protection as the customer grows, and upselling opportunities that benefit both the customer and the MSSP margins.

Lucidum allows MSSPs to leapfrog the competition by generating immediate customer value, increasing customer trust and NPS scores, and reducing churn. Find your secret weapon with Lucidum.