REVERSINGLABS

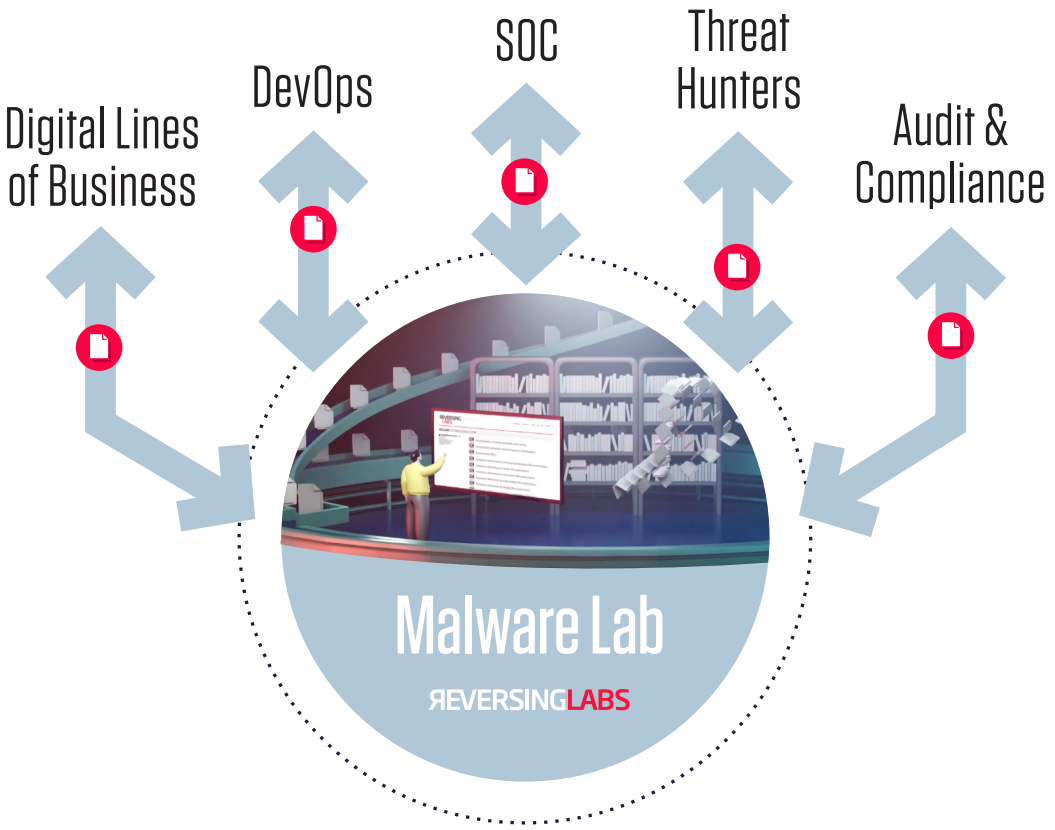
SOLUTION BRIEF

ReversingLabs Solution for Implementing a Malware Lab

BRINGING TRUST TO YOUR DIGITAL BUSINESS

As digital business and remote work become the new normal, organizations recognize their increasing exposures to cyberattacks and the need to refactor their security strategies accordingly. In response to this new landscape several key factors are influencing the demand for an inhouse Malware Lab, including sophisticated targeted attacks, expanding digital risks, reactive security practices, etc.

The context for the "Malware Lab" has been around for some time, and while there have been many names that have influenced its evolution, "Dirty Lab" and Threat Detection Engineering come to mind, the objective remains the same- gain better insight to cyber risk across the entire organization and bolster defenses based on threat actor behaviors through malware research.



For high-risk enterprises, a more formal and productive Malware Lab has begun to appear as part of their strategic initiatives focused on maturing their security programs by:

- Solving the cybersecurity talent gap through tools consolidation and automation, and providing exceptional global and local threat intelligence.
- Refocusing security teams on understanding their adversaries before they attack by integrating threat hunting services across locally seen evidence as well as globally sourced threat intelligence.
- Providing support to the broader digital lines of business to better defend against new threat vectors as exposures increase.

CISOs have voiced the following factors in prioritizing a Malware Lab as part of their ongoing transition and pursuing a more threat-focused information security approach focused on the following:

- **Understanding their adversaries**, their attack behaviors and corresponding IOCs. This critical threat intelligence supports establishing a proactive posture and being able to take actions based on what's likely to hit them based on current trends.
- **Establishing a "center of excellence"** which provides automated reverse engineering to understand what might happen should malware enter their organization, proactively position against these attacks, and aggressive hunt threats that may already exist within our environment.
- **Evolving their detection and response capabilities** beyond curating 3rd-party Threat Intelligence Feeds, and deploying controls more efficiently and effectively. With more actionable intelligence, they can prepare for adversaries' attacks, and know what to expect should these attacks roll out in order to prepare their controls and defenses in advance.
- **Becoming predictive in their security strategy**, and embracing a proactive philosophy to understand their risks in the context of threats- they want to know what's going to happen to them, what are likely adversary capabilities, how do they attack, and what are they attacking. By understanding whether there is an opportunity for them, they can adjust their infrastructure accordingly.

Challenges

The harsh reality is that many organizational groups and security teams are responding *from behind*. The fact of the matter is that security alerts and potentially malicious files either go undetected, or are not identified, triaged and analyzed due to an overwhelming backlog and lack of resources. The 2020 Cisco CISO Benchmark Study highlighted that just under 48% of alerts were investigated- the lowest level in over four years. This rather significant gap is challenging not only the security teams, but the risk & compliance staff and C-suite as well.

Some of the challenges facing malware analysts and researchers include:

TOO MANY ANALYSIS TOOLS, MANUAL PROCESSES, AND AD-HOC WORKFLOWS

- **Open-source tools are NOT enough**
  - Managing open source analysis tools and associated manual processes, ad hoc workflows, and disparate data is cost prohibitive.
- **Dynamic analysis alone is NOT enough**
  - Existing file analysis solutions are not scalable and become cost prohibitive in addressing the increasing demands for file analysis and investigation, and supporting deeper malware research and threat hunting.
  - Existing file analysis solutions such as AV/NGAV and Sandboxes fail to address the increasing complexity and size of contemporary malware i.e. destructive objects.
- **Black-box convictions are NOT enough**
  - Security vendors lacking the breadth of analysis simply render vague threat findings with no transparency about how they came to their conclusions which result in the need for ongoing investigation and ultimately inaction which fails security operations.

INCREASING NEED TO UNDERSTAND NOT ONLY WHAT HAS HAPPENED, BUT WHAT MIGHT HAPPEN

- **Reacting to Alerts is NOT enough**
  - By the time the SOC is engaged, it's likely an attack has already begun to unfold and the risk of downtime and data loss is measurable. Getting to more proactive postures requires understanding your adversaries in advance, knowing who's out there, what their capabilities are, what types of organizations they are attacking, how they are attacking these organizations, and what they go after when they attack.
- **File analysis for the SOC is NOT enough**
  - As new digital business processes are established, new digital content is created, and security risk levels increase. Failing to inspect this content before it enters the organization introduces uncertainty, and for malware detected, understanding potential adversary behaviors enables security to bolster defensive postures.
- **Global intelligence is NOT enough**
  - Targeted attacks, derived through extensive recon and stealthy infiltration, typically look to exploit a specific industry or organization. These attacks are crafted to exploit specific weaknesses, and focus on specific objectives or assets. Local threat analysis, and the appropriate expertise and infrastructure to support extended research and hunting is necessary to apply new intelligence to bolster defensive positions.

INCREASING DEMAND FOR CONTINUOUS CONTENT VERIFICATION AND INSPECTION

- **Third-party trust is NOT enough**
  - The exchange of information is still a fundamental part of digital business, however it's not enough to blindly "trust" digital content from your partners and customers. Uncertainty regarding third-party risk requires continuous monitoring to reliably achieve business objectives.

Solution

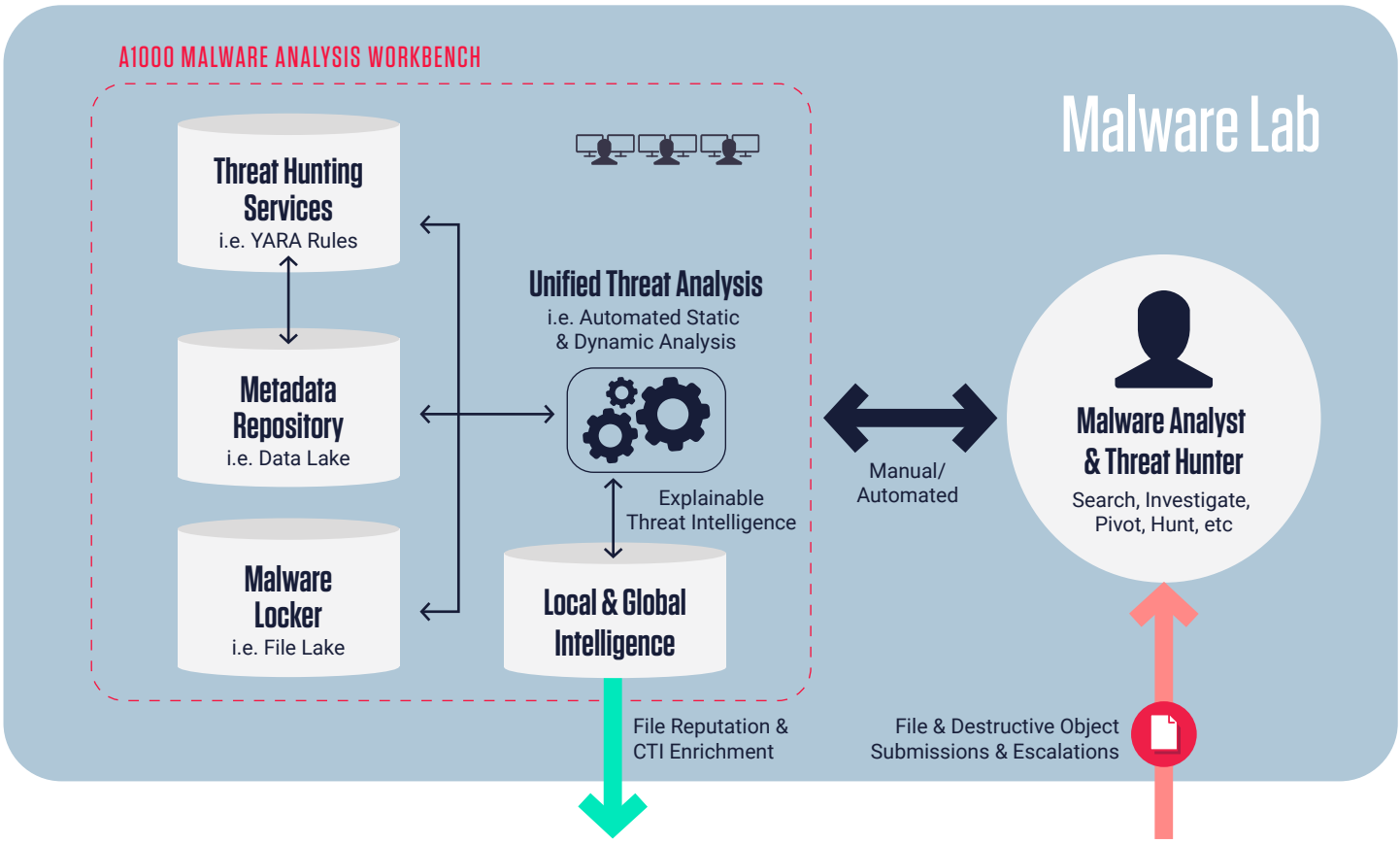
The ReveringLabs Malware Lab provides a commercially supported turnkey solution, that meets the demanding requirements of enterprises in need of automating threat analysis and gathering more actionable intelligence about malware behaviors for use in not only triage and response, but in threat hunting as well as serving other analysis requirements of the business outside the SOC.

The Malware Lab achieves the following objectives:

- Creates a specialized security service that analyzes binary content, investigates complex threats, shares intelligence, and reduces cyber risks by serving all lines of the digital business as a distinct center of excellence.
- Centralizes analysis, research and hunting activities outside the production network to streamline escalation processes, speed detection and response, bring visibility to potential malware exposures, upskill security and operational staff, and hunt threats across the enterprise.
- Consolidates and optimizes file analysis tools to improve accuracy, efficiency, automation, and overall effectiveness.
- Extends Explainable Threat Intelligence and MITRE ATT&CK attributes into security analytics and operations to better inform all stakeholders.

The Malware Lab accomplishes the following:

- **Unify Threat Analysis** tools and optimize file analysis to improve accuracy, efficiency, automation, and overall effectiveness.
- **Centralize investigation, research and hunting** activities to provide extended visibility into malware exposure, speed detection and response, upskill staff, and hunt threats across the enterprise.
- **Streamline escalation processes** by creating a specialized security service group that shares intelligence, reduces cyber risks and serves all lines of digital business as a center of excellence.
- **Develop local intelligence** (internal to an organization) about files and exploits within the infrastructure, allowing security teams better understand their attackers and assess the effectiveness of existing security controls.



Components of a Malware Lab:

- **Unified Threat Analysis Engine and Console:** ReversingLabs Titanium Platform powers the malware lab, enabling threat analysts, researchers and hunters to work from a unified threat analysis workbench comprised of capabilities including automated static analysis and dynamic analysis (i.e. sandboxing technologies) as well as analysis results from other key indicator sources within the platform including network (URI/URL, IP, Domain) and certificate trust chains. By consolidating these capabilities into a single automated analysis solution with a well structured data schema and common console for investigating samples, managing workflows, and hunting threats, Malware Analysis Teams have seen 3x improvement in productivity.

	Point Solutions (e.g. Open Source or Home-grown Tools)	ReversingLabs Titanium Platform Unified Threat Analysis		Legacy Sandbox Solutions
	Manual Static Analysis	Automated Static Analysis	Dynamic Analysis	Dynamic Analysis
Legacy Sandbox Solutions				
Unpacking Support				
Performance				
Scalability				
Intelligence - Indicators, etc				
MITRE ATT&CK Support				
Unified, Single Schema				
Commercially Supported				

- **Comprehensive Threat Intelligence Repository:** Provides a definitive repository of local, as well as relevant global, intelligence that can be leveraged for enriching existing security controls and infrastructure with more explainable threat intelligence on malware.
- **Malware "Sample Locker" or File Lake (e.g. S3):** Stores files in a secure, private location, with restrictive access controls, and these archived samples are available for future research and training. Within the Lab a detailed manifest of security context is maintained for navigating the archived content.
- **Metadata Repository or Data Lake (e.g. Splunk, Elastic, Hadoop):** Continuously monitors for threats, and hunts retrospectively by applying YARA rulesets in search of indicators of interest across the metadata that is extracted from all files decomposed and analyzed locally or sourced globally.
- **YARA Rule Repository:** Consolidates rulesets for use in optimizing detection and threat hunting.

Benefits

The Malware Lab enables enterprises to mature their security organization and play a more strategic role in securing their digital transformation.

- **Technology**
  - **Upgrade and consolidate tools** by unifying the necessary technologies into a common operational console with a normalized, single data schema that helps analysts understand malware behaviors, classify attacks, hunt for new threats, and proactively prepare your security controls and defenses in advance of projected attacks.
  - **Centralize visibility** into attack malware by providing a complete solution that factors in not only the analysis and engineering requirements, but also the applicable infrastructure to support analysis, hunting and continuous monitoring.
  - **Enable early warning** capabilities by centralizing current and historical data, and enabling predictive insights to potential threats.

- **People**
  - **Create a Center of Excellence** by consolidating malware analysis and threat hunting expertise, and the practices to support security operations.
  - **Optimize skills utilization and training** by leveraging better proximity to resources and expanded visibility into threat intelligence and associated best practices.
- **Process & Organizational**
  - **Centralize escalation point** to optimize business and security workflows, thereby reducing detection and response times and the business' overall risk exposure.
  - **Create a universal service team** for the business which supports the consolidation of metrics and risk analysis.
  - **Streamline auditing response** by leveraging a single repository for investigative results across the enterprise, provides an enterprise-wide perspective on risk supported by explainable threat intelligence and classification transparency.

Case Study

Large international financial services organization

- **Their Challenge**
  To provide a safe environment to submit, analyze, detonate, store, and report on file samples submitted to their Malware Research Team and gain insights to new and emerging threats as well as alert on changes in disposition.
- **ReversingLabs Solution**
  The ReversingLabs Malware Lab provided the core analysis and detection technologies to process files and render verdicts at tremendous speed and scale, with additional investigative and hunting resources to deeply understand malware tailored to their organizations infrastructure.
- **Benefit/Value Realized**
  By establishing a dedicated and specialized set of security tools and skills resulted in faster queue processing, more actionable intelligence through extensive indicators and MITRE ATT&CK mappings, reduced response times, and greater insights to potential risks achieved through threat hunting and gaining visibility into potential attacker behaviors which supported reinforcing defenses for more proactive postures.

REVERSINGLABS
Worldwide Sales : +1.617.250.7518
sales@reversinglabs.com