DATA PROTECTION AWARENESS

SESSION1 28-01-2023

About The Presenter.

Managing Director Profile: Obed Makoti

An innovative, analytical, and entrepreneurial professional with extensive consulting, project management, business, and product development experience within the ICT industry, dealing with private and public enterprise, and Telecommunications clients. A professional with a sound track-record initiating and driving projects and ICT strategies that successfully direct business operations, people and ventures across multiple industries and business functions.

Qualifications:

B Com Information Systems & Statistics

BSC Applied Sciences Hons (Industrial Systems)

Professional Certificates:

- Certified Information Systems Security Professional
- ITIL v 4 (Exam Preparation)
- IBM Cybersecurity Analyst Professional
- Information Systems Auditing, Controls and Assurance
- Scrum Master Certification
- Agile Project Management
- PMI Approved Project Management
- Advanced Diploma in Project Management
- Diploma in Data Analytics
- SUSE Intermediate and Technical Sales Specialist
- Salesforce Trailhead RANGER

1.	QUESTION: How hackers learn about you and why Legal Practices are such desirable targets. RESPONSE: Tips for protecting your Legal Practice’s data.
2.	QUESTION: Is the size of the Legal Practice a factor for it to be in danger of attackers? RESPONSE: Tips on managing your Legal Practice’s IT infrastructure.
3.	3LM CYBER PROTECTION SHOW CASE AND DEMONSTRATIONS OF DIFFERENT TECHNOLOGIES.
4.	QUESTION: How Cybercriminals choose their targets, does your Legal Practice fit the ideal victim profile. RESPONSE: Tips for combating attacks.
5.	QUESTION: Using ethical hacking to improve your Legal Practice’s data protection. RESPONSE: Tips on enhancing your Legal Practice's resilience.
6.	QUESTION: Why it is imperative for Legal Practice to have a Cyber-Response Plan? RESPONSE: Tips on drafting a Cyber-Response plan.

DO’s AND DONT’s.

In all our sessions:

We don’t speak the language of technical people	We speak the language business leaders
CYBER SECURITY	**DATA PROTECTION**
Cyber relates to virtual or not existing physically.	Physical protection of your information.
❖ It is external to the practice.	❖ It is internal to the practice.
❖ Something else is in-control.	❖ You are in-control.
❖ Technology is involved.	❖ Hygiene is involved.
❖ Resolved by super intelligence people.	❖ Resolved by mere mortals with awareness.

DO’s AND DONT’s.

In all our sessions:

We don’t speak the language of cyber criminals

RANSOMWARE

Malicious attack aimed at extorting money from victims.

- ❖ Usually a result of known vulnerabilities.
- ❖ At the mercy of the perpetrator.
- ❖ Wait for the attacker to strike.

We speak the language of decision makers

RESILIENCE

To withstand and recover quickly from difficulties.

- ❖ Identified potential risks to the practice.
- ❖ Planning and executing risk mitigations.
- ❖ Continuously monitor emerging risks.

DATA PROTECTION

DATA PROTECTION IS ABOUT MAINTAINING THE FOLLOWING:

- ❖ Confidentiality of data.
- ❖ Integrity of data.
- ❖ Availability of data.

So! we can therefore conclude that, anybody who compromises any of the above can be classified as:

a HACKER.

Also be mindful of the fact that not all HACKERS are criminals.

HOW HACKERS LEARN ABOUT YOU

AND

TIPS ON PROTECTING YOUR DATA.

THROUGH YOUR RELATIONSHIPS AND CONNECTIONS.

EMPLOYEES

PARTNERS

FAMILY

SUPPLIERS

CUSTOMERS

TIP: Apply Zero Trust policies (Trust no one and constantly verify). Implement and train your connections on your policies.

REVEALING TOO MUCH ON SOCIAL MEDIA.

- Allows hackers to find out more about your personal life than you may want them to.
- All your “likes” and “emojis” can be aggregated together to paint a fairly clear picture of who you are and what you are into.

TIP: Always sanitize what you are putting out there. Think twice before you click and think again.

YOUR PRACTICE WEBSITE.

- The marketing's objective is to get clients, data protection's objective is to keep your data safe.
- These two objectives are often at odds with one another.

TIP: Try not to include things like list of clients, attorneys' emails addresses.

YOUR PROFILE PICTURES.

- AI and ML technologies are capable of associating pictures on different social media platforms and link them to one person.
- That headshot picture also identifies you to bad actors, and provides them with a picture they can scrape and use to impersonate you.

TIP: Use different profile pictures on different platforms. Whenever possible, don’t use photos of you or people you know in profile pictures.

PUBLIC Wi-Fi.

- ❖ Hackers can see everything you are doing when on public Wi-Fi.
- ❖ Even worse, open Wi-Fi settings, may allow anyone who’s connected to it to gain admin access to the router, leading to:
  - ✓ Man-in-the-middle attacks.
  - ✓ Network snooping.
  - ✓ Malware distribution.

TIP: Use your 3G or 4G data when away from the home or office.

USER IDs AND MULTIPLE CREDIT CARDS ON ONLINE STORES.

- Many online stores will require your credit card information for fast and efficient checkouts.
- If a that particular website gets hacked, your personal credit card information will be obtained.

TIP: Use a payment service such as PayPal to protect your personal information. If not, limit your online purchases to one credit card account.

WHY IS LEGAL PRACTICE’S DATA SUCH A DESIRABLE TARGET.

LEGAL PRACTICES ARE HONEY POTS OF DATA.

GOVERNMENTS
SECRETS

CORPORATES'
INFORMATION

INDIVIDUALS'
INFORMATION

VARIETY OF
AGREEMENTS

TRADE
SECRETS

TRUST
ACCOUNTS

And legal practices' security is usually not as good as that of corporations, governments and individuals whose data they have.

LEGAL PRACTICES RELY ON SHADOW IT.

- IT devices (BYOD), software and services outside the ownership or control of the legal practice.

ADD SHADOW POLICIES TO THE MIX.

- Those rogue or at times non-existent policies that are never reviewed or approved.

Because, it is simple and convenient for those who have access to data to put it where they want and use it as they wish even if that may not be authorized.

LEGAL PRACTICES LACK IT HYGIENE.

- Backup systems.
- Patch software.
- Endpoint detection and response tools.
- Up-to-date antivirus software.
- Business grade email addresses.
- Encryption of data and devices.
- Management of lost or stolen devices.

Unfortunately for small legal practices, it is costly to properly manage IT hygiene (especially for just 1 - 5 devices). *The above are policy based*.

HERE HOW 3LM PROJECTS CAN OVERCOME YOUR LEGAL PRACTICE'S ISSUES OF:

❖ SHADOW IT.

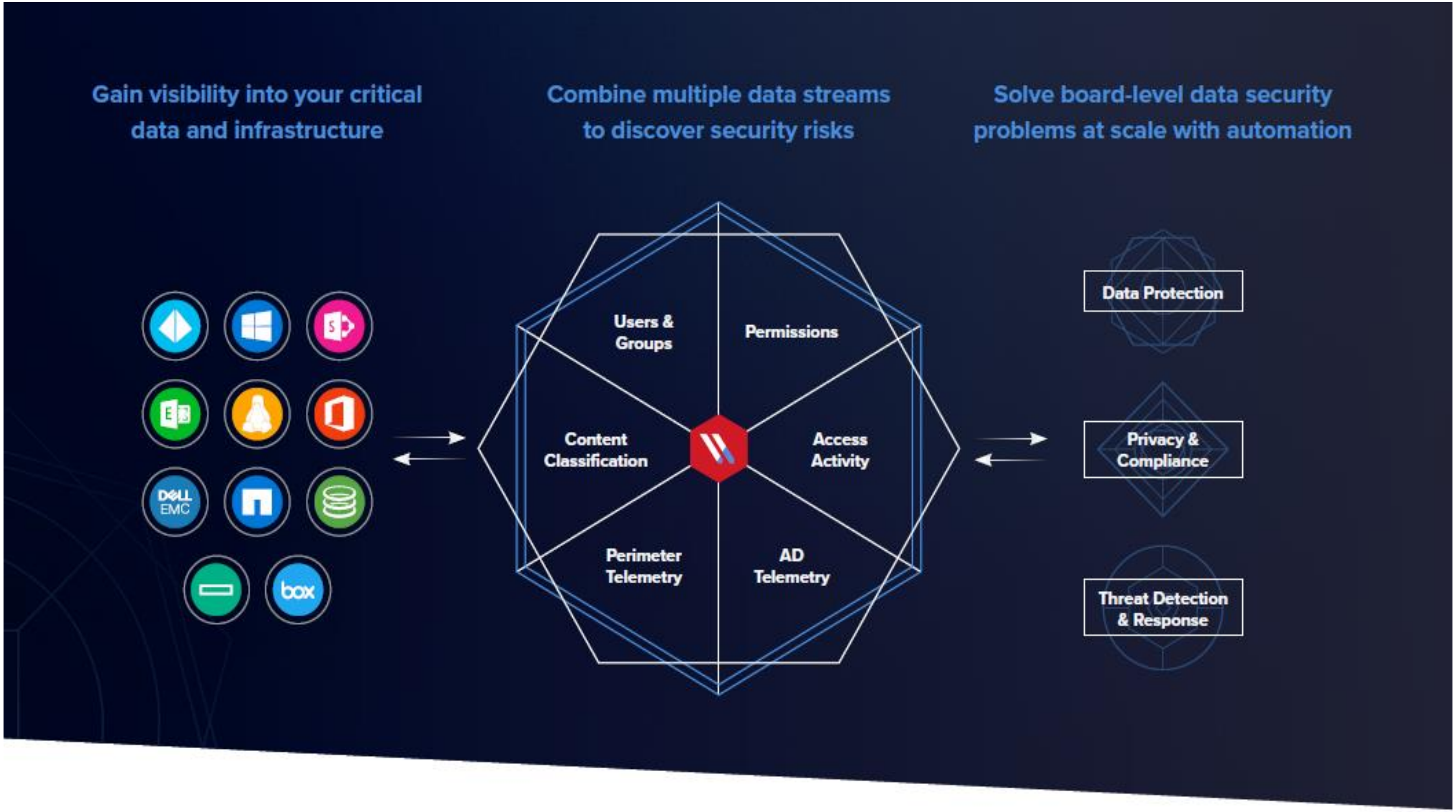
❖ SHADOW POLICIES.

A ZERO-TOUCH, AUTOMATED IT OPERATION DESIGNED TO ENFORCE POLICY COMPLIANCE, IT HYGIENE AND DATA PROTECTION ON ALL ENDPOINT DEVICES.

Our Data Protection Approach.

- Take a data-first approach to cybersecurity by focusing on threats to your sensitive data on your endpoints.
- Remotely monitor your risk levels, and enforce security standards and policies at endpoints level.
- Take appropriate action at endpoints level to protect data, maintain its integrity and prove compliance from anywhere.
- Secure device lifecycle with zero-touch automated endpoint resilience, and always-on visibility and control.

Data First Approach.

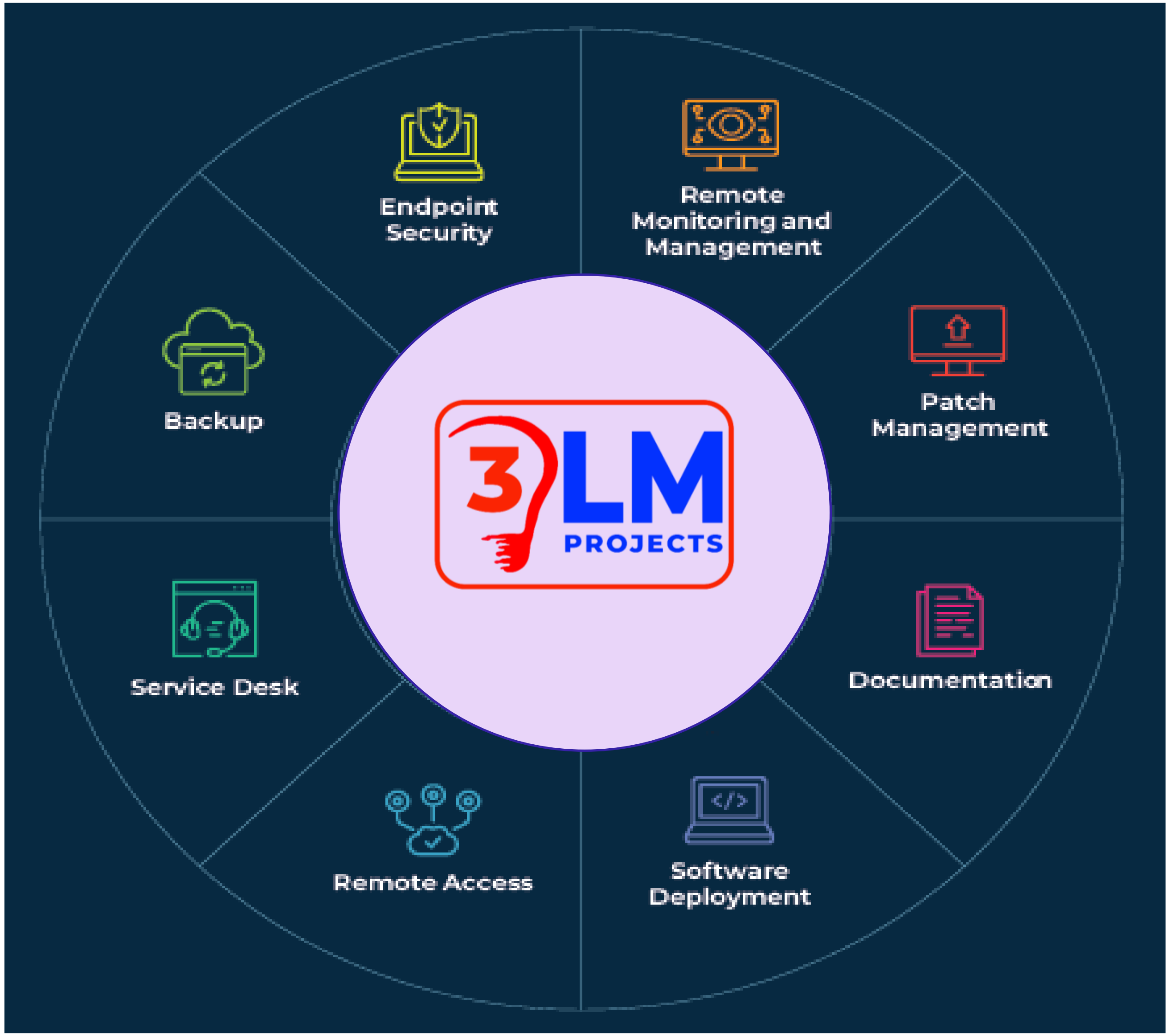


Gain visibility into your critical data and infrastructure

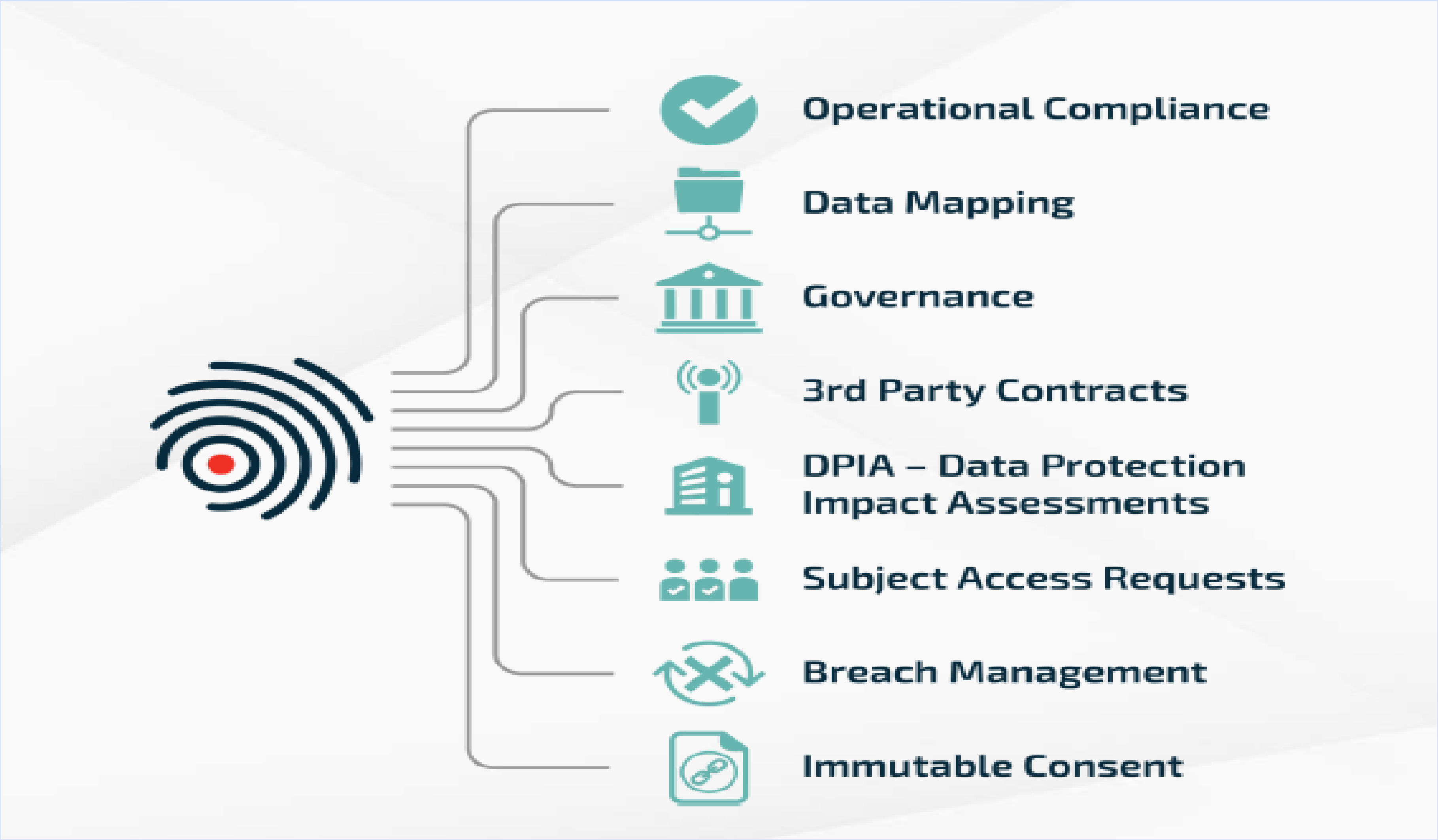
Combine multiple data streams to discover security risks

Solve board-level data security problems at scale with automation

Data Protection.



Privacy and Compliance.



Operational Compliance

Data Mapping

Governance

3rd Party Contracts

DPIA – Data Protection Impact Assessments

Subject Access Requests

Breach Management

Immutable Consent

Threat Detection and Responses.

Geo Locate
Locate a device as soon as it is lost or stolen, then take action to prevent a data breach.

End Sessions
Logout of all sessions, the device is rebooted, access to accounts are blocked.

Forced Reset
Lock devices remotely and request supervisor password.

Geo-Fencing
Lock a device if it leaves the specified area, and unlock when it re-enters the area.

Device Freeze
Remotely defined PIN code to unlock the hard drive, rendering the hardware useless to a thief.

End-of-life Wipe
Perform end-of-life wipes with compliance certificate.

IT Service Hygiene.

Monthly

- Clear event logs
- Rebuild performance
- Disk defrag

Weekly

- Empty recycle bin
- Force reboot
- Start system services

Daily

- Run system cleanup
- Delete Temp files
- Fix system errors

Zero-Touch 3LM Operations Platform.

Endpoint Protection

Reduce your attack surface, stop threats, and respond quickly to security incidents.

DriveStrike

Data Protection

We find, monitor, and protect sensitive data on premises and in the cloud.

ninjaOne

Privacy and Compliance

We classify data based on sensitivity, exposure, and activity and enables data subject access requests.

privIQ

VARONIS

Security Assessment

Vulnerability assessments and penetration testing for cyber security.

intruder

Remote Management

Securely manage your devices and network infrastructure.

ninjaOne

Backup Management

Protect your data with multi-tenant cloud-first backup.

ninjaOne

Threat Detection

Analyze the right telemetry from data, directory services, and edge devices.

intruder

Patch Management

Fully automate your patching, improve software compliance.

ninjaOne

“IF YOU THINK THAT COMPLIANCE IS EXPENSIVE,
TRY NON-COMPLIANCE”

Former US Attorney General Paul McNulty

CONTACTS

29 DOMINICA VILLAGE, CARIBBEAN BEACH CLUB, KOSMOS, 0261
082 687 5647
info@3lmprojects.co.za
www.3lmprojects.co.za

THANK YOU