



SIDR Solutions & Technologies Pvt. Ltd

## Managed Security Services Portfolio



# The next level of **Managed Security Services** – now available for **your business**

Determined, capable cyber criminals don't concentrate their efforts on those organisations best-equipped to defend against their attacks. It's difficult, expensive and time consuming to get the right mixture of people, process, technology and training in place, and maintaining these defences while adapting to constantly-changing threats is a huge task. Traditional defences are reaching traditional limits,

SIDR has been trusted to protect the networks, data and devices of organizations – and we can bring that scale, cutting edge knowledge and security operations capability to your defense.

Managed security services may be the answer but, instead of reaching for an “off the shelf” solution, try a service that focuses on what matters to you which can scale and adapt to your specific business requirements in an ever changing world. It is time to choose a managed security service which goes beyond traditional limits, SIDR managed security portfolio delivers a customisable service to:

- Profile, understand the threat, risk, vulnerabilities and your security response
- Manage your security infrastructure to be always efficient and optimised
- Monitor your complete infrastructure, correlate and visualise information

- Detect anomalies, investigate and eliminate the false
- Respond quickly and completely to campaigns of attack SIDR Managed Security Services help our customers to enhance and develop their security operations in line with their unique business challenges and security objectives. A security partnership with SIDR allows:
- Intelligence led and threat focused detection and response
- Proactive threat hunting for insider and external threats
- Accuracy and speed of response through machine accelerated human decisions
- Complete infrastructure coverage from endpoint to cloud
- Access to The latest technology techniques and processes, all supported by our experienced staff





Available with regional data residency, all services are delivered by dedicated 24x7 Security Operations Centers. Staffed by skilled, experienced, qualified and security cleared personnel SIDR deliver the unique service mix you require to allow you to focus on your business challenges whilst relieving your security operation pressures.

## Prepare

The Prepare solution area focuses on increasing organisational understanding. Services deliver understanding

- Cyber Threat Intelligence (threat signature feeds, research, and reports)

Cyber Threat Intelligence helps clients be aware of potential

	Know the enemy and know yourself	Make security operations more efficient and cost effective	Ensure compliance and improve detection capabilities	Proactive searching, investigation and forensic analysis of anomalies
Desired outcome	<ul style="list-style-type: none"> <li>• Know what is attacking and where, when and how</li> <li>• Discover your weaknesses</li> <li>• Visualize your infrastructure</li> </ul>	<ul style="list-style-type: none"> <li>• Increase operational efficiency</li> <li>• Increase threat resistance</li> </ul>	<ul style="list-style-type: none"> <li>• Regulatory / policy compliance</li> <li>• Increase effectiveness of detection</li> <li>• Identify known threats and vulnerabilities</li> </ul>	<ul style="list-style-type: none"> <li>• Hunt and detect the most sophisticated threats</li> <li>• Decrease time to complete remediation</li> </ul>
Solution area	Prepare 	Manage 	Monitor 	Detect & respond 
MSS portfolio	<ul style="list-style-type: none"> <li>• Threat Intelligence services <ul style="list-style-type: none"> <li>• Threat feeds</li> <li>• Threat research</li> <li>• Target Intelligence</li> </ul> </li> <li>• Vulnerability scanning</li> <li>• Network visualization</li> </ul>	<ul style="list-style-type: none"> <li>• Security device management</li> <li>• Log retention and management</li> <li>• Vulnerability management</li> </ul>	<ul style="list-style-type: none"> <li>• Security event monitoring</li> <li>• Complete security monitoring <ul style="list-style-type: none"> <li>• Network</li> <li>• Endpoint</li> <li>• Cloud</li> </ul> </li> <li>• Compliance monitoring</li> </ul>	<ul style="list-style-type: none"> <li>• Managed detection and response – threat hunting across: <ul style="list-style-type: none"> <li>• Network</li> <li>• Endpoint</li> <li>• Cloud</li> </ul> </li> </ul>
Supporting services	<ul style="list-style-type: none"> <li>• Penetration testing</li> <li>• Strategy consulting</li> <li>• Cyber risk consult</li> </ul>	<ul style="list-style-type: none"> <li>• Technical and operational support</li> </ul>	<ul style="list-style-type: none"> <li>• Incident response</li> <li>• Malware analysis</li> </ul>	

of the actual, probable and possible attack and the potential risk, impact and ability to defend against and respond to a range of threats. Discovery of an organisations online footprint also allows a valuable window into available material for attackers to use, and helps manage and control organisational and employee behaviour in relation to making information public. [Threat Intelligence services](#)

attacks before they even happen. Our Cyber Threat Intelligence team investigates and tracks cyber attacks against organisations around the world. From this, SIDR builds rich profiles of high-priority threat actor campaigns. SIDR continually updates these profiles with new observations, and the insights feed our cyber security services. Our high quality signatures are updated on a daily basis from investigations and through relationships with third parties. The threat signature feed can be automatically deployed into a SIEM or other network defences. This in turn enables our clients to keep ahead of the attackers, improving

situational awareness of attacks in the client's business sector or location, and enabling prioritised incident investigation. Delivering rich context around tactics, techniques and procedures (TTPs) allows for more accurate detection but also the prediction of even the most insidious of potential sophisticated threats.

If sensitive client data is accidentally released online, it may be a potential weapon for attackers. Our next service deals with this increasingly complex data detection.

- Target Intelligence

Target Intelligence, sometimes referred to as open source or OSINT, enables customers to understand what an attacker can learn about their organisation from open Internet sources that may be damaging. The service maps out organisation's online footprint and discovers potentially sensitive data, such as network diagrams, user details, data leaks, and so on.

This data could be used by an attacker against the organisation either directly to target their attack or through techniques like social engineering to create new weaknesses. This service provides the specialist skills and tools required to discover this data.

#### Vulnerability Scanning and Assessment

SIDR provides both internal and external scanning to locate weak points into or inside a client's infrastructure before they can be exploited by an attacker. The service generates a report that highlights the vulnerabilities found, how they can be fixed, and how exploitable they are.

## Supported at every step, **modular and tailored** to your requirements

This report provides increased visibility and specific actions to resolve these vulnerabilities more efficiently.

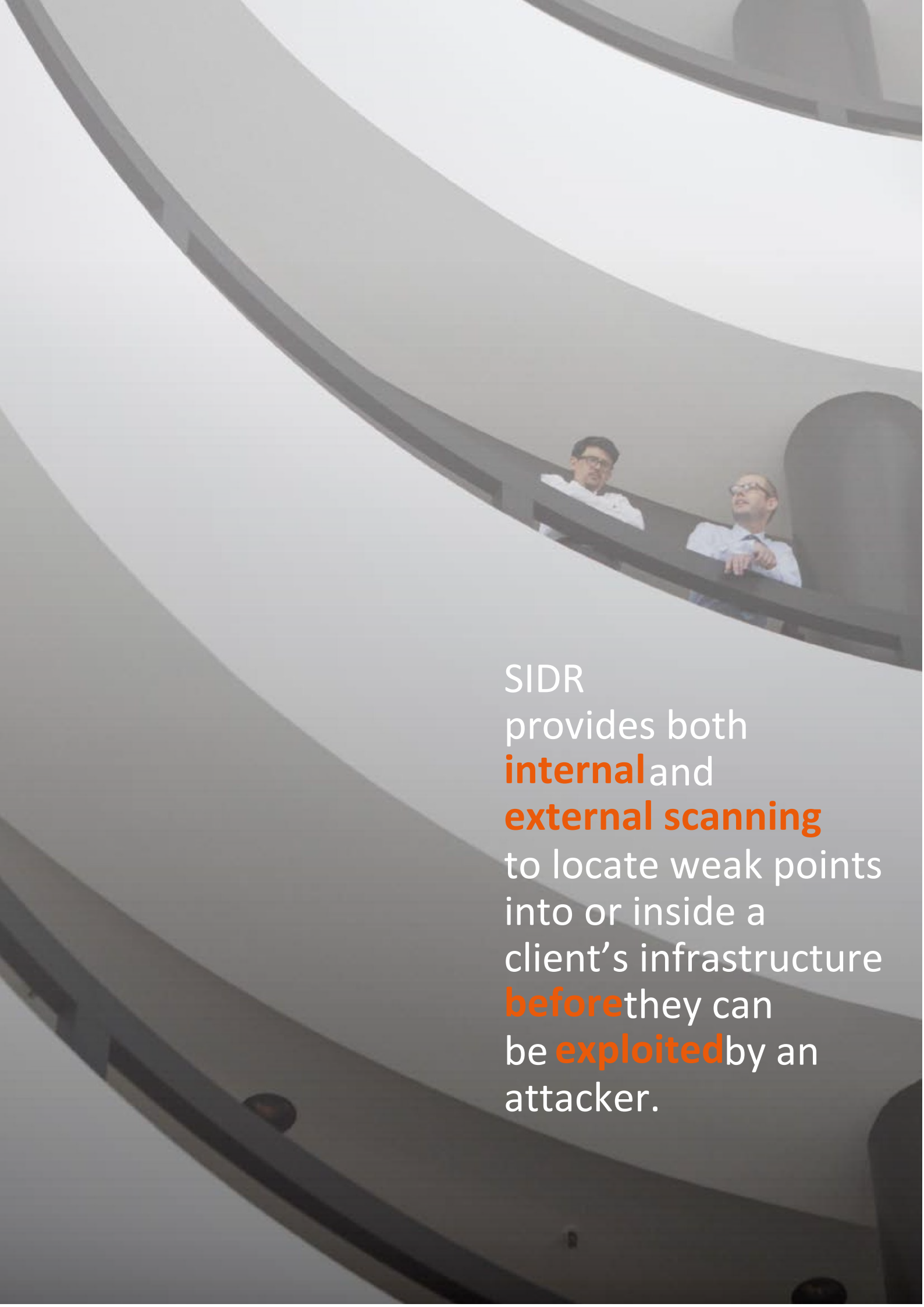
As networks become more complex, it is vital to keep track of existing network infrastructure to ensure potential vulnerabilities are easy to locate.

#### Network Visualisation

Our Network Visualisation service provides a greater understanding of a client's network infrastructure and allows it to be visualised through a network map. This enables the client to understand the full scale and topology of their network, which helps minimize the risk of any potential changes to their existing infrastructure. The network map improves incident diagnosis and response, helps to traverse complex networks and locate assets quickly, and helps to identify potential weaknesses and issues.

The service tracks changes to the network infrastructure which is critical to testing of the network infrastructure. Having a retrospective view of the network improves the ability to test the resilience of the current security operations, by exploring potential weakness in current infrastructure resulting in a plan for improvement and closing of the gaps.



A photograph of two men standing on a curved, modern architectural structure, possibly a balcony or walkway. The structure is made of light-colored concrete or stone with dark metal railings. The man on the left is wearing a white shirt and glasses, looking towards the camera. The man on the right is wearing a light blue shirt and glasses, looking away from the camera. The background is a bright, overcast sky.

SIDR  
provides both  
**internal** and  
**external scanning**  
to locate weak points  
into or inside a  
client's infrastructure  
**before** they can  
be **exploited** by an  
attacker.

## Prepare supporting services

### Penetration Testing

The Intelligence-Led Penetration Testing services that SIDR provides combines two market leading services:

- Our renowned threat intelligence service provides current, up to date, detailed insight and awareness of threat actors, their attack vectors and their motivations, through some of the most sophisticated and advanced threat intelligence available
- Our highly respected and accredited penetration testing technical assessments of network security and business risk

When combined, the result is a powerful service that differentiates itself from standard penetration testing services, providing customers with an end-to-end, informed and focussed technical assessment of their network security, detection and response capability.

### Cyber Risk Consulting

Consulting engagements are available to support all of our managed services. Expert help is at hand to meet any security challenge. Whether the client is looking to overhaul or update their security strategy, mature their security programme, or assess their risk, quality of controls or architecture, SIDR delivers a range of cyber security strategy and improvement services to help boards and their businesses understand and tackle cyber risks and opportunities cost-effectively and with minimum disruption.

### Strategy Consulting

Our advisory services help clients understand and manage cyber risk. They deliver a clear understanding of an organisation's exposure to cyber attack, and the impact such an attack would have on their business. This enables them to make informed investment decisions and to put pragmatic, cost effective cyber defences in place.

With over years of experience working with organisations that take security very seriously, we understand what works and what doesn't.

## Manage

The Manage solution area improves operational efficiency, reduces the redundant security technology investment, and provides better protection coverage. It consists of three parts: Log Management, Security Device Management, and Vulnerability Management in addition to the Technical and Operational Support service.

### Log Management

Log Management is a cost effective and scalable method of retaining, searching and retrieving security logs from servers, routers, security devices and other infrastructure of interest such as Point of Sale, or POS devices, cloud services, web servers and databases to improve security. In addition to the incident forensics benefits of Log Management, it is often mandatory for compliance purposes, especially in financial services where data from transactions must be archived for future investigations. Customers have access to stored logs, which can be searched and extracted to support customer investigations and forensics outside of contracted managed security services

In order to provide fundamental network security, all devices on the network must be secure and maintained. If a client is looking to reduce cost, overhead or add support to new devices the SIDR' Security Device Management service can take on that management responsibility.

### Security Device Management

Security Device Management ensures that a client's network infrastructure functions as designed, and is continuously and efficiently updated and always optimally configured. Our service manages the security devices and technology on the client's network, and guarantees that devices are configuration controlled, and monitored to ensure they are functioning correctly, and are always available. It also ensures that vulnerabilities are identified and patched, and keeps the devices and technologies up to date with relevant software upgrades. The incorporation of our comprehensive threat intelligence, which tracks the activities of the most advanced cyber attacks, allows the service to block sophisticated attacks at the perimeter of a client's network.



### Vulnerability Management

Vulnerability Management provides a scanning platform and an on-going vulnerability management programme to discover, manage and correct vulnerabilities in a prioritised way aligned to organisational risk. SIDR support the client through set up, implementation, scanning, reporting and help with remediation activities. This service helps the client establish and run a vulnerability management programme that is necessary for continual improvement in security posture and regulatory compliance.

## Manage supporting services

### Technical and operational support

Technical and Operational Support service and a consulting service to improve management within the customer security operations are available. These services are designed to improve the capabilities of our clients' employees by providing assistance on how to maintain a robust security practice, upgrade technology and direct staff to their maximum potential.



## Endpoint Security

**Monitoring** service attaches software to all hosts or endpoints within a client's network, such as laptops, desktops and servers. This **software** is known as an agent, and it captures data from each endpoint and passes it back to the Security Monitoring service. This data provides visibility into endpoint activity such as what processes are running, memory usage and network activity. These insights enable us to **discover malicious activity** or behaviour of both malware and the user of that endpoint, thus allowing an **improved response action** to the threat.

Complete Security monitoring

## Monitor

The Monitor solution provides storage, correlation and interrogation of relevant data aligned to client directed threat models, to build a clearer picture of the possible threat faced.

Security Monitoring delivers 24x7 real time monitoring of activity across clients infrastructure. Scalable, modular and aligned to the customer requirement, the service collects and analyses data from any directed source including logs, events, network traffic and feeds from security and network equipment, endpoints, servers and cloud.

Security Monitoring is delivered from a dedicated SOC, staffed by an expert team of analysts. Alerts are triaged, investigated and integrated into the client workflow with full and comprehensive remediation advice given to the client. Data is collated and stored and customer portals give access to the customer to perform ad hoc investigations with reports generated on compliance.

Services are modular and can align to the customer need and can be used in conjunction with each other to increase effectiveness of the overall monitoring and detection capability. It consists of three parts, Security Event Monitoring, Complete Security Monitoring, and Compliance Monitoring.

### Security Event Monitoring

This service is based around the monitoring and correlation of logs and events from various security and network devices. Analysts process and analyse these on behalf of the client and alerts triaged are entered into the client's workflow or blocked through automation according to client requirements. Devices and technologies monitored include Firewalls, IPS/IDS (Intrusion prevention or detections systems), VPN (virtual private network), gateway web, email, Antivirus AV, content and UTM (Unified Threat Management) devices.



the loop investigation delivers a threat focused monitoring service, delivering answers, not alerts.

SIDR processes and correlates vast amounts of log, event and network data as well as data from endpoints and cloud infrastructure as directed by the client. This data is correlated using our expansive and constantly updated threat recognition rules to look for threats. In the event of an alert, the attack source is automatically blocked on devices managed by SIDR. For customer-managed devices, a notification is sent with advice on how to combat the threat. Our complete security monitoring service also provides initial triage and investigation of these security incidents, with all security incidents investigated by human analysts before being reported to deliver a near zero false positive rate. This Service is based around an advanced security operations methodology and delivered 24x7x365 from a single SOC, and supported by a team, which enables better understanding and decision making based around the unique behaviour and risk profile of each client.

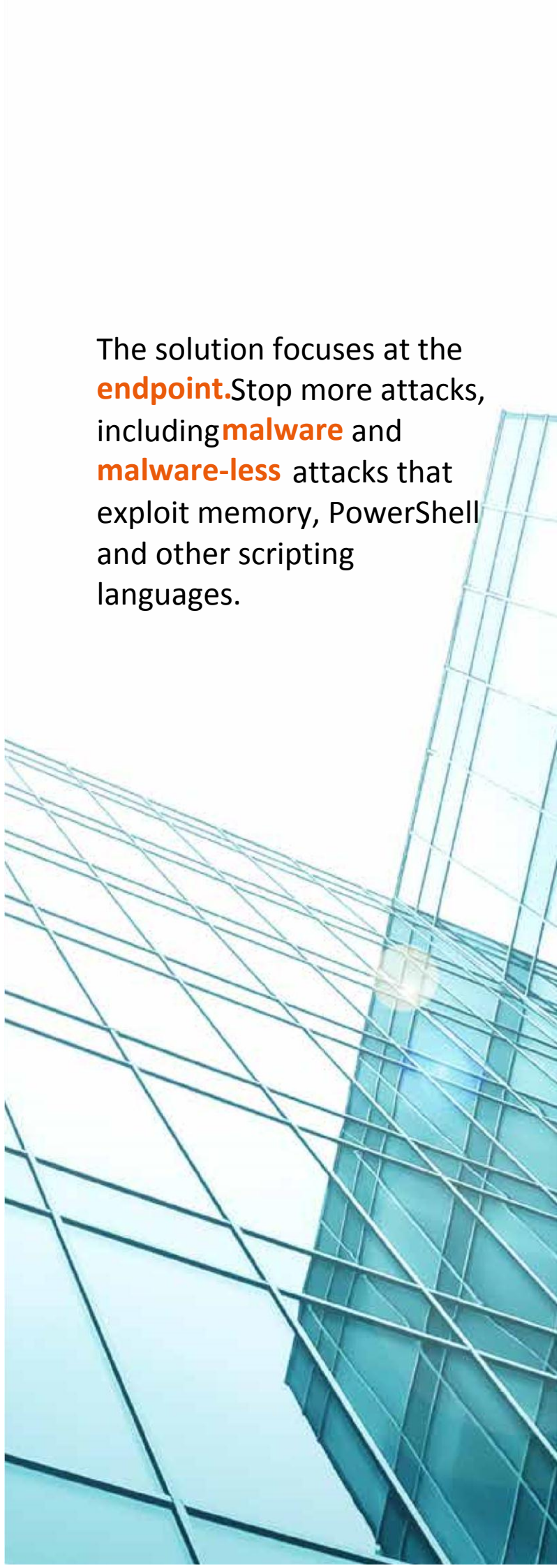
#### Endpoint Focus

As a component of the Complete Security Monitoring service, Endpoint Security Monitoring attaches agent software to all hosts or endpoints within a client's network, such as laptops, desktops and servers. The agent software captures data from each endpoint and sends it to the Security Monitoring service. This data provides visibility into endpoint activity such as what processes are running, memory usage and network activity. These statistics enable discovery of malicious activity or behaviour of both malware and the user of that endpoint, thus allowing an improved response action to the threat.

#### Compliance Monitoring

Many industry regulations, including ISO, RBI, PCI, IRDA, and HIPAA, require monitoring of security devices and logs to ensure the integrity of these systems and regular reporting. The Compliance Monitoring service simplifies security and compliance and is a turn-key solution to streamline audits. A combination of log management, security event monitoring and vulnerability scanning are employed to generate output reports to support compliance various needs.

The solution focuses at the **endpoint**. Stop more attacks, including **malware** and **malware-less** attacks that exploit memory, PowerShell and other scripting languages.



## Detect and Respond

The Detection and Response Solution area provides the ability to detect unknown threats, internal and external threats and non-malware enabled activity.

Often deployed in conjunction with the monitoring service, giving additional layers of protection not just against known or predictable, the Detection and Response solution consists of two parts: Managed Detection and Response and Threat Hunting service.

### Managed Detection and Response

This service takes away the necessity to make a snap or real-time decision for security operations. Able to process, store, fuse, correlate and visualize a vast variety and volume of data, it is designed to address more sophisticated attacks that masquerade as legitimate activity in order to breach security. In addition to the advanced methods of detection from monitoring, the SIDR threat analytics platform is utilized to apply behavioural-based detection analytics to the data, highlighting deviations and anomalies, which prompt deep investigation by SOC analysts. The behavioural-based detection isolates activity on the network that may appear normal but, in fact, is an indication of compromise which may have never been seen before. This allows the service to provide early warnings in the kill chain, thus providing an opportunity to reduce the impact of the attack. The end game is the comprehensive remediation and complete response to campaigns of activity, not just single threats. The service is fully supported by subject matter experts, feeding analyst-driven investigations, delivering answers not alerts. [Endpoint Focus](#)

This solution focuses, as many attackers do, at the endpoint. An additional component of the Managed Detection and Response Service, this gives a client organisation managed access to the next generation of Endpoint protection solutions. This service allows SIDR to stop more attacks, including both malware and increasingly common malware-less attack that exploit memory, PowerShell, and other scripting languages.

Endpoint detection and response service allows SIDR' SOC personnel to deliver full visibility into attack patterns and behaviour, and enables either SIDR or client administrators the ability to deliver complete response and remediation.

### Threat Hunting

A formal, proactive and continual threat hunting service enabled by the unique insight into threat actor behaviour and tactics, techniques, and procedures (TTPs) from SIDR intelligence service. This insight is gathered from SIDR' intelligence teams and incident response activity befitting from government and industry intelligence sharing and collective intelligence from our client base. A team of highly trained subject matter experts search for and investigate behavioural anomalies and deviations from an organisation's standard digital behaviour which could be indicators or attack or potential incidents.

Analysts start by formulating a hypothesis about specific activity types. Then, this behavioural activity is investigated using the SIDR threat analytics platform and a powerful combination of raw data search, machine learning and visualisation to fuse disparate data sets, uncover new malicious patterns of behaviour and adversary TTPs. When successful, the service informs and enriches automated analytics, correlation rules and signatures which improve existing detection mechanisms and create new, shareable threat intelligence.

## Detect and respond supporting services

### Incident Response and Malware Analysis

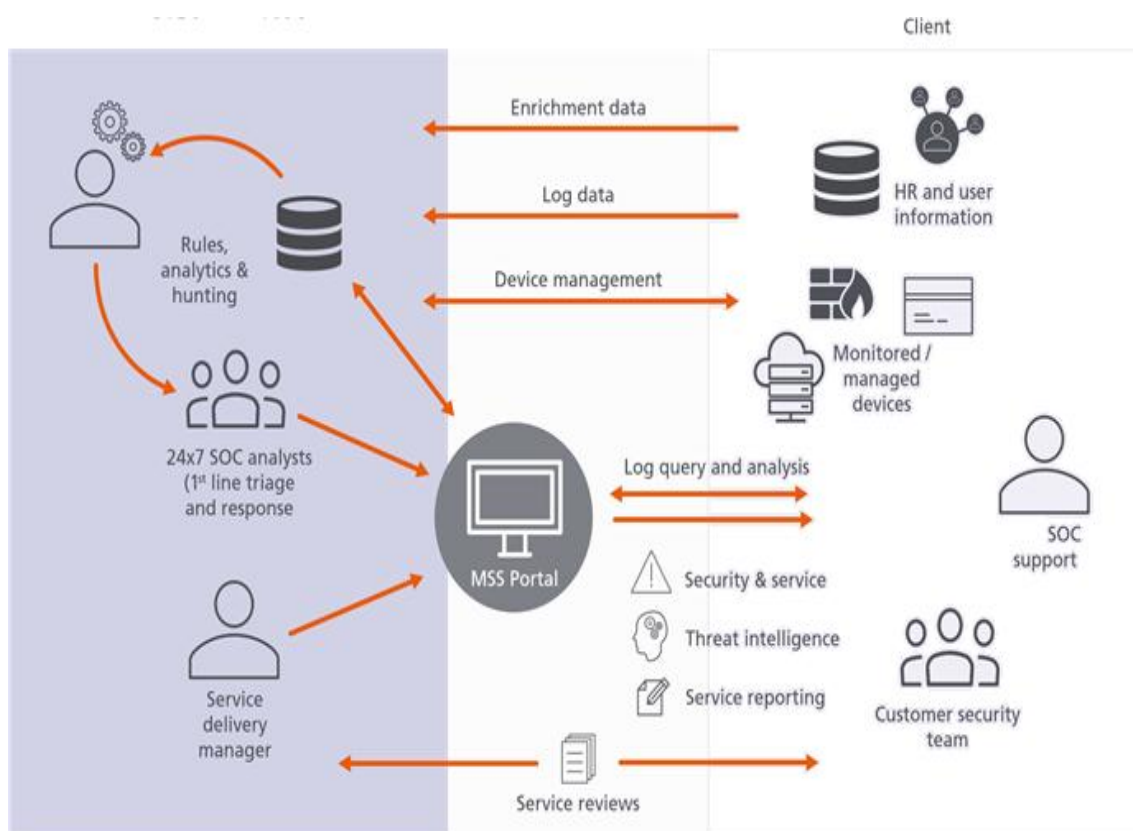
SIDR also offers Incident Response and Malware Analysis which provides clients' employees with the additional support required when dealing with unknown threats. Wider capabilities of incident management, forensic investigation and reverse engineering of malware are often delivered to support clients when needed.

Different interaction models are offered, depending on whether an IT provider or in-house security team is involved. Security device improvements can also be implemented, as can updates to incident readiness and assessment.

## Service tailored and delivered via Advanced Security Operations Centres

Supporting flexibility is important to SIDR. It enables our customers to consume a unique mix of services which support both their current security needs and their need to flexibly change over time. The service mix may be unique but the service delivery management and SOC operation is not.

All customers benefit from advanced (ASOC) operations, backed by a dedicated service delivery manager. This ensures that whatever security questions customers need answering or whatever challenges they may face in the future, SIDR can deliver flexibility, experience and expertise and a partnership customers can trust.





# CONTACT

## SIDR Solutions & Technologies Pvt. Ltd.

### Our Address

B 705, Venus Tower, Veera Desai  
Road, Andheri(W), Mumbai -  
400053

### Call Us

+91 9167994589  
+91 9821624926  
+91 8767766325