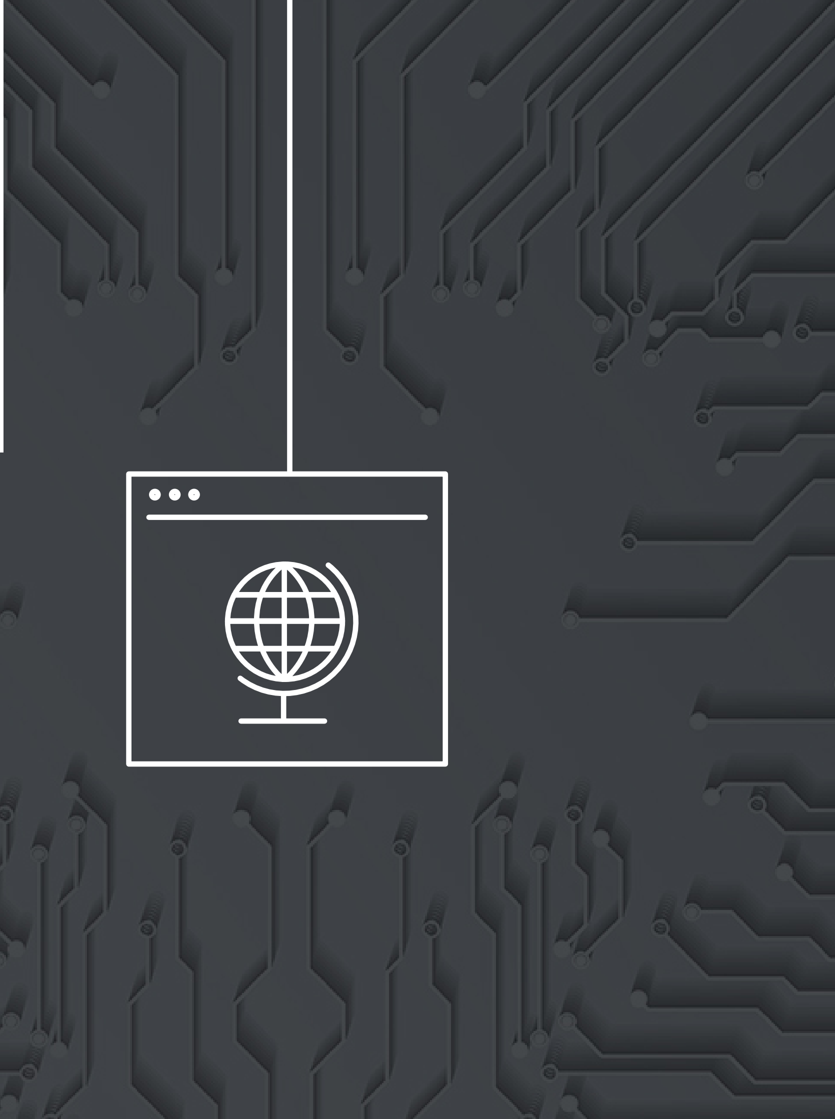
Deloitte.

Managed Security Services

Secure. Vigilant. Resilient.

CyberIntelligenceCentre



Cyber Fusion Framework

Cyber **Watch**

- Cyber Threat Intelligence
- Cyber Threat Course of Action
- Custom Cyber Surveillance, Darknet Analysis and Threat Reconnaissance
- Beacon and Disclosure Monitoring
- Brand Semantic and Natural Language Processing
- Intelligence and Threat Level Predictive Analytics

Cyber **Check**

- Cyber Threat Intelligence
- Cyber Threat Course of Action
- Custom Cyber Surveillance, Darknet Analysis and Threat Reconnaissance
- Beacon and Disclosure Monitoring
- Brand Semantic and Natural Language Processing
- Intelligence and Threat Level Predictive Analytics

Cyber **Monitor**

- Situational Threat and Security Monitoring
- Cyber Predictive Analytics
- Cyber Outlier, Anomaly and Temporal Analytics
- Brand Monitoring
- Malcode and Emerging Threat Monitoring and Surveillance
- Advanced (Persistent) and Targeted Monitoring
- Cyber Threat and Targeted User Threat Monitoring

Cyber **Govern**

- Cyber Governance, Policy and Continuity Planning
- Cyber Business Alignment and Executive Reporting
- Business Cyber Threat Landscape Assessment, Modelling and Risk Situational Awareness
- Cyber Readiness and Enterprise Resiliency
- Cyber Training, Awareness and Employee Planning

Cyber **Prepare**

- Cyber Threat and Risk Planning
- Cyber Threat Response Crisis Preparation
- Cyber Simulation and War Gaming
- Cyber Business Continuity and Services Recovery Planning
- Cyber Lifecycle Management

Cyber **Protect**

- Managed Network and Email Breach Detection and Containment
- Managed Endpoint Breach Protection
- Managed Advanced Threat, Malware and Malcode Threat Management Services
- Secure Software Development
- Identity and Access Management
- Information and Threat Resiliency
- Application Protection
- Data Loss Prevention

Cyber **Respond**

- Incident Support
- Cyber Take-Down and Recovery Assistance
- Crisis Management
- Forensics and Advanced Threat Analysis
- Breach Response and Recovery
- Litigation Support
- Response, Eradication, Hardening and Resiliency

Cyber **2020**

- Identity and Access Management
- Cyber Business Alignment and Executive Reporting
- Application and DLP Protection

Cyber Watch

Client and business centric intelligence, surveillance and brand monitoring capability. The value of this capability is the alignment of cyber threat intelligence, surveillance and other related services with the objective of reducing exposures and the threat profile of our clients.

Cyber Threat Intelligence	Services to analyse for emerging threats, vulnerabilities, industry exploits and related risks in cyber. Our Global Intelligence team is designed in a coordinated manner to utilise the strength and breadth of the Deloitte Global structure to collect and analyse threats based on regional language, sentiment and analytics, while aggregating and disseminating it centrally. Unlike typical MSS, our intelligence service does not rely solely on our own intelligence sources. We include a convergence of the best commercial intelligence providers, our own intelligence and Darkspace (Darknet) intelligence, Open Source Intelligence, HoneyNets, Vendor Advisories, Governmental Intelligence and other related input. Our Managed Services utilise sophisticated technology to aggregate, converge, triangulate and enrich intelligence that is then distributed to all our Cyber Intelligence Centres. Unlike typical Managed Security Services (MSS), our Automated Intelligence Fusion can analyse up to 45 languages.
Cyber Threat Course of Action	A key aspect to an effective intelligence program is the ability to convert advisories and flash notifications (Intelligence) to actionable content. This content can be used to secure and in some instances enhance other streams in the Cyber defence program. This service will provide the organisation with timely Course of Action for intel advisories.
Custom Cyber Surveillance, Darknet Analysis and Threat Reconnaissance	Focused services designed to assess threat to the organisation or potential compromise of the organisations sensitive data (customer information, credentials etc.). Our services include the analysis of the Darknet, common drop sites for data, cyber chatter, carding forums and other related services. Where required Deloitte can work with the organisation to define a protocol for interception and take down, which is covered in the Cyber Respond service offering.
Beacon and Disclosure Monitoring	Assessment of systems within the organisation that are "leaking" information about the organisation that may not be picked up by typical controls. This ranges from data leakage to privilege users that are disclosing information about the organisation on chat rooms, for example.
Brand Semantic and Natural Language Processing	Assessment of brand perception that could affect the organisation cyber profile and threat level. For this service our Managed Services Intelligence Centre monitors for cyber chatter against the organisation and assesses threat level. Unlike brand monitoring, our teams are assessing threat level for Tactics, Techniques, Procedures and Actors (TTPA).
Intelligence and Threat Level Predictive Analytics	Using advanced analytic methods to assess leading intelligence indicators that can impact threat level.

Cyber Check

Managed solutions to provide lifecycle based (ongoing) validation of security and threat posture, both from an enterprise and threat actor perspective. This includes focused posture assessment, targeted vulnerability management, application testing, Advanced Threat Resiliency Assessment and other related services.

Posture Assessment	Ongoing dynamic assessment of posture utilising a combination of real time threats, vulnerabilities, configuration, intelligence and threat level. Using advanced tools, our managed services can analyse and assess for weaknesses based on the triangulation of the factors indicated above. The result is a prioritised remediation and resiliency program for the organisation.
Application Security Validation	Assess ongoing threats to applications (web sites, applications, databases), based on emerging threats, intelligence, changes in configuration and other related application posture changes. The Managed Services will run control application validation procedures and feed this information into the Posture Assessment Analytic Tools as part of the active threat defences.
Active Vulnerability Management	Managed Active Vulnerability Management includes validation, assessment and discovery of vulnerability footprint by actively enumerating exposure on systems. This is a precise and focused method for assessing posture. The results of which are fed into our Cyber Monitor, Watch and other programs.
Passive Vulnerability Management	Most organisations are not able to scan their entire enterprise for multiple reasons including: a) Scale and time to execute on active vulnerability management b) dynamic nature of assets and c) Possible disruption. Our managed vulnerability management methods utilise network sensors to assess for the use of vulnerable applications, systems or even exploits in flight. This can be used to enumerate applications that at times cannot be discovered using active vulnerability management methods.
Threat Resiliency Readiness	Managed assessment, reporting and dashboard of threat resiliency dynamically based on posture, intelligence and real time threats.
User Awareness Analysis	Managed validation of the effectiveness of user awareness programs and institutionalisation of methods. Users being the last line of defence, this managed service validates the core targets of advanced threats.

Cyber Monitor

Advanced analytics monitoring, sensory and analysis solutions that consumes and monitors your logs for the presence of compliance and cyber security issues providing the threat analysis and business context to enable Respond.

Situational Threat and Security Monitoring	Real time threat monitoring, assessment of security context, changing risk profile and other related activities. The monitoring solution based on Deloitte's award winning DAT (Deloitte Advanced Threat) solution that is designed to detect conventional and advanced threats.
Cyber Predictive Analytics	Enhanced analytics to use leading indicators that affect the organisation, peers and/or other organisations in our advanced predictive model to derive early warning indicators that could target the organisation. The objective is to reduce the exposure window and increase response effectiveness of the monitoring capability.
Cyber Outlier, Anomaly and Temporal Analytics	Enhanced real time and analytics technology used by our hunt teams to analyse for outliers, slow and low attacks, anomalies and temporal threats. Output of this service is available through a mobile friendly portal.
Brand Monitoring	Monitoring of threat level to the organisation's brand. This includes chatter hostility/semantic analysis, brand sentiment and other methods to assess threat actors, methods and motive to target the organisation. Our Managed service in brand monitoring supports up to 40 languages and our engine supports Natural Language Processing.
Malcode and Emerging Threat Monitoring and Surveillance	Service to intercept, collect, analyse and monitor for threats against the organisation. Our Managed Services utilises a global network of Honeynets to collect Malcode, analyse the payload and assess the risk to the organisation. For example, is the organisation the intended target for the threat?
Advanced (Persistent) and Targeted Monitoring	Activities related to bespoke monitoring of Advanced Threats against the organisation environment using analytical, advanced tooling and focused hunt processes. Our managed services team is broken into a multi-tier hunt structure to break advanced threats into DAT (Deloitte Advanced Threat) capsules. Each capsule is designed to address specific actor motives and targets.
Cyber Threat and Targeted User Threat Monitoring	Monitoring of users and targets that are often the focus of attention by adversaries of the organisation. This includes advanced threat monitoring for indicators that depict a potential breach or compromise of the users system.

Cyber Govern

Cyber governance, risk, and compliance capability. Objective is to align, initialise, measure and evolve the Cyber Security program to align with business continuity, objectives and outcomes.

Cyber Governance, Policy and Continuity Planning	Ensuring there is appropriate governance, defined roles, responsibilities, established alignment with business continuity, champion, reporting structure and other related aspects of Cyber preparedness and planning.
Cyber Business Alignment and Executive Reporting	Ensuring there is appropriate communication and alignment of the Cyber (MSS) with the business. This includes Executive Committee presentation, board briefings (typically quarterly) and other related activities.
Business Cyber Threat Landscape Assessment, Modelling and (Risk) Situational Awareness	This answers the question of "Who is or could be targeting us? What do they want? How could this change? And how are the methods (TTP's) they may use. During this activity Deloitte would perform a Threat Landscape Assessment, align the Threat Landscape with the Business and ensure that measures and methods (use cases, content, and discoverability) are developed to align with risk to the organisation.
Cyber Readiness and Enterprise Readiness	Activities to ensure there is a multi-layered approach to ensure resiliency. This includes appropriate Cyber controls, methods, awareness, training and other related methods.
Cyber Training, Awareness and Employee Planning	Activities to ensure there is enough resiliency at the "Last line of defence", the user. This includes focused user training, awareness campaign, employee communications (e.g. change in threat landscape results in the organisation employees being targeted through an advanced malware) and other methods. This works in unison with Cyber Monitor in that the service (Cyber Monitor) will feed key risk Indicators into the Cyber Govern program.

Cyber Prepare

Methods, processes, capability and enablers to ensure cyber readiness and preparation at all levels of the organisation. This includes executive reporting, preparation, resiliency and other programs.

Cyber Threat and Risk Planning	Activities to ensure the appropriate mapping of business risk, threat landscape, use cases and measures. The objective of this activity is to align the MSS with the tangible business outcomes.
Cyber Threat Response Crisis Preparation	Measures and activities to ensure that the organisation is able to respond to a cyber-attack and the resulting crisis. This includes table-top scenario planning, definition of roles and responsibilities, call-out, prioritisation, threat containment strategy and other related activities.
Cyber Simulation and War Gaming	Activities to replicate top ten (10) threat scenarios to the organisation that can result in existential risk to the organisation. These are typically drills and simulated scenarios that involves monitoring, CERT, executive briefing and in some instances legal. The objective is to ensure there is awareness and an established plan for a major cyber crisis.
Cyber Business Continuity and Services Recovery Planning	Activities to assist with recovery of services that are the result of a cyber-attack. This includes planning, preparedness and activities should the organisation encounter a Cyber Attack. This includes technical play-books, established roles and responsibilities, call-outs, control measures and other related activities.
Cyber Lifecycle Management	Onsite support that interfaces with the MSS. This is a team of individuals that are assigned to the organisation to ensure appropriate handling of call-outs from the MSS, triage and institutionalisation of cases. The key benefit is that there is appropriate alignment in both directions (from the organisation to the MSS and from the MSS to the organisation).

Cyber Protect

Solutions that are designed to provide focused managed-threat-managed-solutions for our clients. This includes solutions around Breach Detection, Advanced Threat Protection, Secure Code Development and other related services.

Managed Network and Email Breach Detection and Containment	Managed network malware and advanced threat detection and prevention. This includes the use of sandboxing, advanced recognition, signature, heuristics and other methods for Malcode interception.
Managed Endpoint Breach Protection	Managed endpoint advanced threat detection and prevention. This provides a platform to detect Advanced Threats against the end user and protect against Malcode execution.
Managed Advanced Threat, Malware and Malcode Threat Management Services	Moving beyond automation, this service includes the analysis of Malcode and advanced threat in the wild or within the organisation environment, to focus on targeted attacks. This includes a combination of automation, analytics, advanced hunt (manual) analysis and other methods.
Secure Software Development	Managed service to ensure appropriate software and application resiliency using lifecycle based analysis. This includes application scanning, code review and other related services.
Identity and Access Management	Managed identity and access management, includes user provisioning, certification, de-commissioning, validation and other related services.
Information and Threat Resiliency	Managed services and consulting around the analysis, documentation and presentation of resiliency recommendations based on what our Cyber Monitor services detect or profile.
Application Protection	Managed services for a holistic programme to protect applications, databases and other critical functions within the organisation's enterprise. This includes managed process, resources and technologies (e.g. Web Application Firewall, Content Delivery, Database Activity/Firewalling and other related methods).
Data Loss Prevention	Managed Data Loss Prevention methods which includes process, resources and technologies to detect violations or risks in data disclosure.

Cyber Respond

An outsourced Services to address threat Respond, containment and eradication. This includes (but not limited to) cyber take-down, recovery, forensics, breach Respond and other related services.

Incident Support	Managed incident support and coordination. Typically this is supported through our onsite resource that is allocated to the organisation, based on ongoing workload (of that resource). Additional expertise from Deloitte’s Fraud, Forensics and Litigation support staff can be brought in on a Time and Material basis.
Cyber Take-Down and Recovery Assistance	Managed services that integrate with our Cyber Watch capability, whereby if our Intelligence service detects a disclosure or change in threat posture warrants a cyber take-down or recovery, our managed service team will assist the organisation on a Time and Material basis. Our team will work with the organisation to define and agree to the appropriate risk assessment, engagement and take down protocol.
Crisis Management	Managed services and support around coordination and management of major cyber crisis.
Forensic and Advanced Threat Analysis	Advanced forensic and advanced threat forensic and threat analysis. Our managed service will utilise Deloitte’s industry specialist in fraud, forensics and investigations for this service offering.
Breach Response and Recovery	Should a breach occur, our managed service can assist with response and recovery services, utilising deep expertise in recovery.
Litigation Support	Deloitte Managed Services can assist with litigation support including expert witness, access to our legal teams etc.
Response, Eradication, Hardening and Resiliency	Post breach or incident response, eradication, hardening and resiliency services. Including (but not limited) to system hardening, application security, re-configuration, root cause analysis, training and other related activities.

Cyber 2020

These include services that Deloitte CRS aims to deliver over the course of the next few years.

Managed SSL	A certificate management solution that will manage the entire lifecycle of SSL certificates in order to reduce the cost and time related to managing multiple certificates.
Secure coding services and Security-by-design Architecture	Using secure design and development practices to develop software to ensure that security is integrated into the design of software rather than applied later.

Contacts

Derek Schraader
Risk Advisory Africa Leader: Cyber Risk Services
Mobile: +27 79 499 9046
Email: dschraader@deloitte.co.za

Cathy Gibson
Director: Risk Advisory Africa
Mobile: +27 82 330 7711
Email: cgibson@deloitte.co.za

Henry Peens
Associate Director: Risk Advisory Africa
Mobile: +27 82 496 8694
Email: hpeens@deloitte.co.za

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (DTTL), its network of member firms and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This communication is for internal distribution and use only among personnel of Deloitte Touche Tohmatsu Limited, its member firms, and their related entities (collectively, the “Deloitte network”). None of the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

Designed and produced by Creative Services at Deloitte, Johannesburg. (RA CIC/vee)