EY Ireland's Managed Security Operations Centre

NextGen - SOC
Dublin - Cork - Belfast

Building a better
working world

Contents

NextGen Security Operation Centre Services

1. Threat Detection and Response

- 24/7 Real Time Monitoring
- L1, L2, L3 Triaging
- Mean Time to Detect (MTTD)
- Mean Time to Respond (MTTR)
- Rapid response and remediation

2. Threat and Vulnerability Management

- Asset discovery
- Rogue device detection
- Secure configuration scanning
- Cyber exposure assessment
- Vulnerability life cycle management

3. Advanced Incident Response

- Readiness Assessment
- IR Plan, Design and Implementation
- Playbooks Design
- Playbooks Automation

4. Threat Intelligence

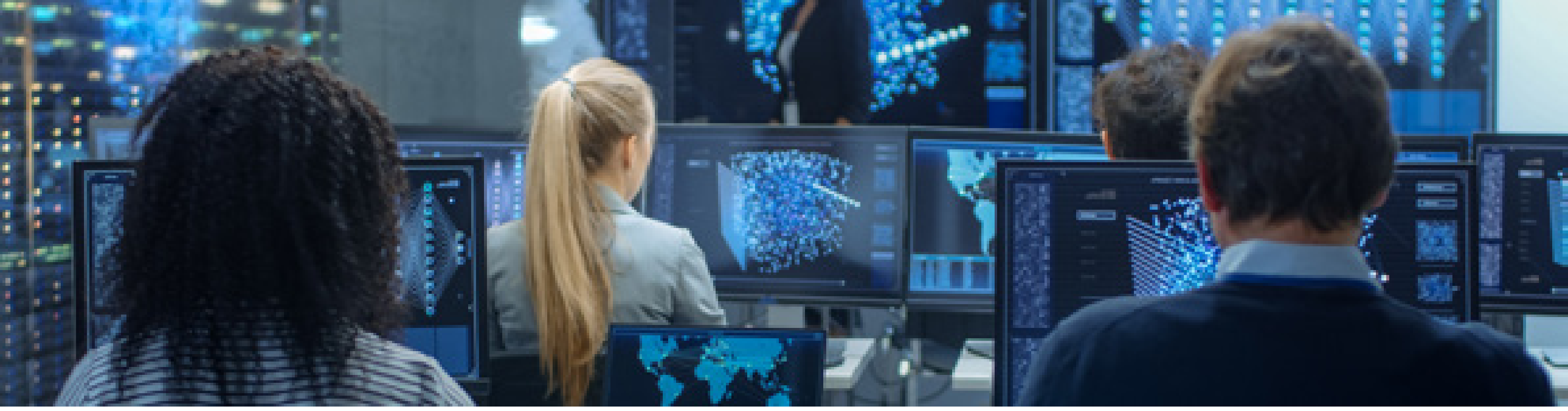
- Cyber Threat Intelligence
- Threat Hunting
- Sector specific threat actors
- Tactics, Techniques, and Procedures

5. Dark Web Monitoring

- 24/7 Data Breach Monitoring
- 24/7 Breach Alert Notifications
- Corporate Brand Protection
- C-level User Identity Protection

6. SOC Advisory and Maturity Assessment

- SOC Advisory Services
- SOC Capability Assessment
- SOC Implementation Services
- SOC Transformation



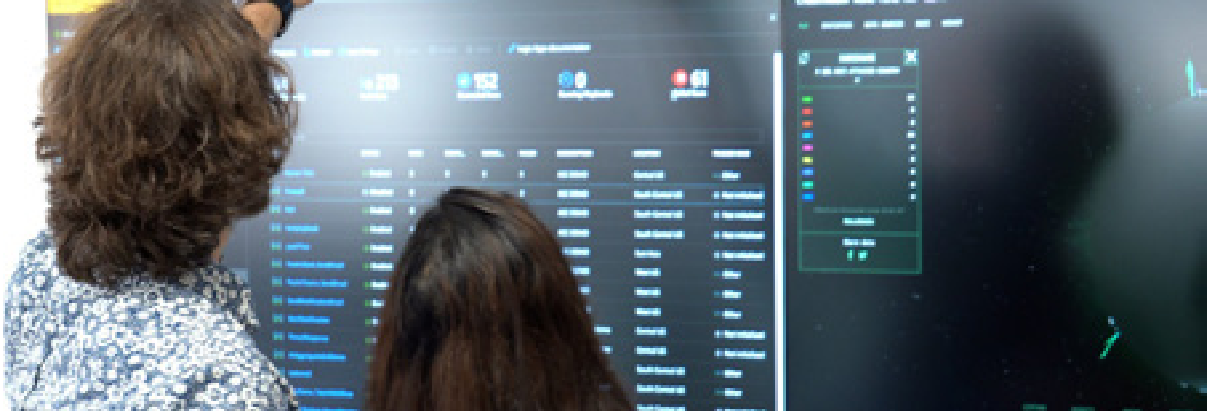
Threat Detection and Response

EY's Threat Detection and Response (TDR) solution consists of people, process and technology operating to detect, respond and contain a cyber attack before business assets are impacted. Our TDR solution enables clients to improve and accelerate deployment and maturation of their threat detection, threat response, and threat hunting services, and provide an integrated interface with incident response capabilities. It helps client's detect and contain attacks from the time hackers successfully penetrate an enterprise.

Built on end-to-end visibility of the attack lifecycle, and a strong foundation of advanced security operations which is powered by automation, analytics and a tierless operating model, clients can more efficiently disrupt and detect attacks.

Service Offerings:

- **First level monitoring and triaging of Alerts:**
  Utilizing our SIEM and SOAR technologies provides our analysts with first level monitoring and assistance in triaging alerts
- **Ransomware Readiness:**
  We offer intelligence-based attack simulation reports with tactical action items for improvement, enhanced endpoint detection and response signals for ransomware detection and alerting, and standard operating procedures and playbooks focused on ransomware threats
- **24/7 Real time monitoring**
  EY's Managed SOC has the capabilities to monitor, detect, and automate responses to incidents in real time harnessing our SIEM and SOAR solution
- **Rapid Response and Remediation:**
  Utilizing our technologies as well as our partnerships with the leaders in TDR solutions, EY has the capability to offer high detection accuracy by reducing false positive alerts, incorporate the MITRE ATT&CK framework so our security specialists can leverage the mitigation recommendations provided, and enabling automated playbooks to provide quick and coordinated responses



Threat and Vulnerability Management

EY's Threat and Vulnerability Management service is a continuous and proactive process that assists organisations in safeguarding their computer systems, networks, and enterprise applications against cyberattacks and data breaches.

Our experts can assist you in developing or improving your current vulnerability management programme, as well as reducing your overall risk exposure by mitigating as many vulnerabilities as possible.

We will design a continuous process that is in line with your organization's strategic goals and ensure it is kept up with new and emerging threats and dynamic environments.

Service Offerings:

- **Asset discovery and rogue device profiling:** Continuous asset discovery on premises and cloud (Amazon AWS, Microsoft Azure, Google Cloud Platform), including both hardware and software installed on it
- **Rogue device detection & prevention:** Automatically track all devices in your network through scheduled scanning, create a baseline of known assets, and get alerted when a rogue or unauthorized device connects to your network. Control who or what is allowed to connect to your network with switch port, IP address, MAC address management capabilities
- **Vulnerability and secure configuration scanning:** Scheduled risk-based assessment of your entire organization's cyber exposure, including vulnerabilities of all your assets, misconfigurations, risky software, and other potential security threats that put your organization at cyber risk. Prioritize remediations according to vulnerability criticality and demonstrate compliance with company and industry regulations and standards
- **Cyber Exposure Assessment:** Which combines risk-based vulnerability management, web application security, cloud security and identity security. EY can help organizations gain visibility across the modern attack surface and understand their cyber exposure areas, risk of such exposures, including any potential losses. This information is vital in prioritizing efforts based on what will prevent the most likely attacks, as well as creating an action plan to reduce cyber risk exposure over time
- **EY Managed Vulnerability Lifecycle:** Let EY create a Vulnerability Management strategy as per best practices, tailored to your business requirements, and manage all steps of the lifecycle

Advanced Incident Response

EY's Advanced Incident Response service offers the ability to rapidly identify an attack, minimize the damage, contain the incident, remediate the cause, and finally reduce the risk of similar incidents.

We have specialists that can design and implement an Incident Response programme, and a dedicated team of analysts that will provide support for all incident handling measures.

Service Offerings:

- **Incident Response Assessment:** Provides an assessment review of your organisation's abilities to protect against and respond to security related incidents. Identify any deficiencies in response measures and remediate them accordingly
- **Incident Response Plan, Design, and Implementation:** We can help your organization handle a data breach rapidly and efficiently while at the same time minimizing any damage caused. This will involve identifying and prioritizing assets, identifying potential risks, establishing procedures, setting up a response team, and determining what tools would work best for you
- **Incident Response Delivery 24/7:** Because the digital world never sleeps it makes sense to have our experts ready to respond 24/7 should an incident occur. The EY incident response team operates around the clock to detect and analyse anomalies within your organization as soon as possible. Our team of experienced analysts have access to cutting edge technology that offers highly accurate detections which reduces the mean time to detect (MTD) and respond to many different types of threats. We have partnerships with some of the biggest and most respected cyber security vendors in the business
- **Incident Response Playbook Design:** Playbooks are a critical component of cyber security as they help bridge the gap between an organization's policies and procedures and a security automation solution. We have the experts at hand to design a playbook to suit the needs of your organization in order to eliminate unnecessary steps from the incident response process

Cyber Threat Intelligence

In order to prevent or limit the impact of a threat, you must be able to fully understand it. To make this possible, organisations need threat intelligence, data about your advisories, their capabilities, motives, tools, and methodologies. EY leverages the most up to date and relevant threat intelligence sources on the market today.

Service Offerings:

- **Cyber threat intelligence:**
  EY's incident response team utilizes the most sophisticated threat intelligence solutions to help organizations easily consume intelligence, take action, and minimize manual tasks. The tools used at EY help to automate the threat investigation process and produce intelligence reporting and IOC's specifically tailored for any threats encountered by your organisation. This enables teams to better understand, respond quicker, and proactively stay ahead of the attackers
- **Daily IOC hunt:**
  We will scan and alert for multiple IOCs in your network, some of which are: unusual activity of privileged user accounts, higher than normal volume of traffic, multiple requests for the same file, traffic to open or unused ports, known vulnerabilities that have been exploited in the wild
- **Threat hunting:**
  EY's cyber security threat hunters add the human element to enterprise security which complements the automated systems they use. Our skilled security specialists can nullify threats before they are able to cause serious damage. This is done by utilizing some of the most popular threat hunting frameworks available today, two of which are, the MITRE PRE-ATT&CK and ATT&CK frameworks. This enables our analysts to investigate IOCs and TTPs used by threat actors across the globe and create use cases based on this information which enables us to stay ahead of the most sophisticated of threat actors
- **Target malware alerting:**
  Integrating threat intelligence with our SIEM and SOAR solutions enables us to monitor our clients' networks in real-time which facilitates rapid alerting and response times. This is vital to preventing and containing attacks as soon as possible
- **Continuous alerting of advisories Tactics, Techniques, and Procedures:**
  Threat intelligence enables us to be proactive when is comes to cyber attacks. Continuously updating the TTP's and IOC's used by threat actors, and integrating them with our security tools, enables our clients to continuously stay one step ahead of them

Dark Web Monitoring

With more data breaches happening every day, it is likely your organization's information might be available on the Dark Web.

Your employee's information can be traded by hackers on the Dark Web either through sale on marketplaces or by openly appearing on free lists.

Having compromised information available on the Dark Web can increase your risk of becoming a target of cyber-attacks.

In addition to other defence strategies to protect yourself from malicious actors, the ability to find out what hackers have on you is a distinct advantage and can be used as a warning to take corrective measures and tighten up your technical security controls around sensitive data.

Service Offerings:

- **Dark Web Scan:**
  The identities that you register with the service can include the names, addresses, and email addresses of your employees, key personnel, and administrators. EY will scan the Dark Web for signs of compromised information associated with your business, employees, and your data. If a data leak is detected, we will immediately notify you and work with you to take evasive action - in example, you will need to force all users to change their passwords if a credentials leak is detected

- **Corporate brand protection service:**
  EY will continuously monitor your brand identity on the Dark Web by perform data searches using web bots, with a goal of protecting your brand and your organization's reputation. We will constantly monitor Dark Web for your domain name(s), personal information about employees, intellectual property, insider information, payment card numbers, bank accounts, and immediately notify you on any mentions of your company and employees in the context of threats

SOC Advisory and Maturity Assessment Services

SOC advisory and maturity assessment services are professional consulting services that help organizations enhance their security posture by providing guidance and recommendations on establishing, operating, and managing a SOC

Service Offerings:

- **SOC design and architecture:** Consulting on SOC design and architecture, including the selection of technology, tools, processes and data requirements
- **SOC implementation:** Assistance with the implementation of the SOC, including project planning, deployment, and testing
- **SOC operations:** Ongoing support and guidance for SOC operations, including incident response, monitoring, and reporting
- **SOC maturity assessments:** Evaluating the effectiveness of the SOC and providing recommendations for improvement
- **SOC training and awareness:** Developing training programs for SOC personnel and raising awareness of security risks across the organization

Contact Us

Securing your organization gives you the confidence to lead transformational change, innovate with speed and build a better working world for your stakeholders.

EY has created these services specifically to help our clients address the challenge of accessing specialist cyber skills at the right cost necessary to enable businesses to thrive against a backdrop of increasingly sophisticated and aggressive cyber threat actors.

Service Offerings:

- We have a team of over 100 specialist cyber professionals on the Island of Ireland delivering for clients across all industries and capability domains, from strategic consulting and architectural design through to engineering and operations
- We have strategic alliances with many of the leading cyber industry vendors
- We have 63 cybersecurity centres globally, supporting 150 countries
- We develop trust with the client, in order to co-innovate and co-create new solutions
- We provide sector-specific knowledge and multidisciplinary experience, as well as access to the latest innovations

Puneet Kukreja
Partner, Head of Cyber
puneet.kukreja@ie.ey.com

Carol Murphy
Partner, Head of Markets Cyber
carol.murphy@ie.ey.com

Hugh Callaghan
Partner, Cyber Chief Strategy Officer
hugh.callaghan@ie.ey.com

Angelika Nowicka Venkata
Director, Cyber Operate Leader
angelika.nowicka.venkata@ie.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organisation, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organisation, please visit ey.com.

P023866.indd 04/23. Produced by Creative (Ireland)
ED none

The Irish firm Ernst & Young is a member practice of Ernst & Young Global Limited. It is authorised by the Institute of Chartered Accountants in Ireland to carry on investment business in the Republic of Ireland.
Ernst & Young, Harcourt Centre, Harcourt Street, Dublin 2, Ireland.

Information in this publication is intended to provide only a general outline of the subjects covered. It should neither be regarded as comprehensive nor sufficient for making decisions, nor should it be used in place of professional advice. Ernst & Young accepts no responsibility for any loss arising from any action taken or not taken by anyone using this material.

ey.com