Managed SOC

EY’s Advanced Security Center: world-class cybersecurity working for you
Ice-climbing requires trusted teamwork and agility to continually detect and respond to hidden dangers in a challenging and ever-changing landscape — so does your SOC.

Contents

Introduction ............... 1
How EY can help you ....... 4
EY differentiators ........... 7
Introduction

Challenges organizations face

We have entered the era of targeted cyber attacks. The question is not “if” your company has been breached, or even “when”. It has already happened. The real questions are: is your organization aware of it, and are you capable of detecting and responding to future threats?

An effective Security Operations Center (SOC) can form the heart of an organization’s operational defense against advanced cyber attacks. However, many organizations struggle to implement their SOC ambitions. When developed in-house, SOC challenges include identifying suitably skilled resources to provide 24x7 coverage and leveraging the most effective technologies for advanced threat detection and reporting metrics.

While outsourced Managed Security Service Providers (MSSPs) implementations can help with the resourcing challenges, they often focus on log aggregation and perimeter monitoring and can lack sufficient business context to allow an organization to effectively assess the practical impact of a threat on its business. EY’s Managed SOC service has been designed to overcome these, and other, limitations currently present in the SOC marketplace.

EY’s Managed SOC provides a hybrid resourcing model of on-site and off-site professionals, combining 24x7 coverage with a SOC model that is customized around your core business needs. Through the use of advanced monitoring technologies, EY’s Managed SOC provides your business with greater threat detection capabilities than is possible via traditional log aggregation and perimeter monitoring provided by MSSP approaches. We have integrated threat intelligence, security monitoring, incident response and security analytics competencies to reflect the reality of detecting Advanced Persistent Threat (APT) style behavior on your network, including endpoint threat detection and data exfiltration.

Threats continue to evolve; your SOC must too. EY’s Managed SOC is designed to wrap experienced people and efficient processes around leading technologies to provide a business-focused SOC that will evolve with your organization’s needs and the changing threat landscape.

It is important that organizations not only maintain traditional security controls but continue to evolve their ability to rapidly detect and respond to threats.

56% of respondents say that it is “unlikely or highly unlikely” that their organization would be able to detect a sophisticated attack.*

---

Above we have highlighted the most common cyber threats and their perpetrators. Against this background, it is important that organizations not only maintain traditional security controls but continue to evolve their ability to rapidly detect and respond to threats. Tightly coupling leading-edge detection and response capabilities with cyber threat intelligence (CTI) not only equips an organization with the ability to address present threats but helps to ensures that their defensive capabilities will continually evolve to address new and emerging future threats.

However, building a security operations center (SOC) environment with the correct balance between preventive, detective and reactive controls, along with threat intelligence abilities, can prove challenging.

<table>
<thead>
<tr>
<th>Who</th>
<th>Why</th>
<th>What</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lone casual opportunistic attackers</td>
<td>Curiosity, mischief, malice</td>
<td>Website defacement or opportunistic hacking</td>
</tr>
<tr>
<td>Anonymous, ideological “hacktivism”</td>
<td>Disruption, humiliation, political aims</td>
<td>Denial of service, social media, data breaches</td>
</tr>
<tr>
<td>Organized criminals, malware</td>
<td>Financial gain via online fraud and extortion</td>
<td>Mainstream malware: Trojans and ransomware</td>
</tr>
<tr>
<td>Advanced persistent threat</td>
<td>IP theft, financial gain via espionage</td>
<td>Targeted malware, corporate espionage</td>
</tr>
<tr>
<td>Nation-state-sponsored cyberattack</td>
<td>Large-scale IP theft, critical infrastructure disruption</td>
<td>Diplomatic espionage, cyber sabotage</td>
</tr>
</tbody>
</table>

**Indicative threat sophistication**

**Threats that most organizations recognize the need to mitigate**

**Emphasis on detect and response**
When building an SOC, typical difficulty factors include:

<table>
<thead>
<tr>
<th>SecurityMonitoring</th>
<th>IncidentResponse</th>
<th>ThreatIntelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>No aggregated source of log data to enable efficient security monitoring, including event correlation</td>
<td>Lack of threat-focused, proactive monitoring</td>
<td>Companies have so much data to manage that it becomes hard to find the “needle in the haystack” of an attack</td>
</tr>
<tr>
<td>Lack of threat-focused, proactive monitoring</td>
<td>Monitoring rules and/or procedures are not aligned with attacker techniques, tactics and procedures and are not aligned to threat intelligence</td>
<td>External feeds of data are rarely tuned to the business</td>
</tr>
<tr>
<td>Monitoring rules and/or procedures are not aligned with attacker techniques, tactics and procedures and are not aligned to threat intelligence</td>
<td>Monitoring rules inadequately tuned, with too many false positives</td>
<td>Alerts for threat conditions consider external trends and not the existing capabilities to deter</td>
</tr>
<tr>
<td>Monitoring rules inadequately tuned, with too many false positives</td>
<td>Lack of team focused on detection analysis</td>
<td>Attacker techniques change, which will outdate the intelligence you have on them</td>
</tr>
<tr>
<td>Lack of team focused on detection analysis</td>
<td>Monitoring teams overwhelmed with events</td>
<td>Information ages and may quickly become irrelevant</td>
</tr>
<tr>
<td>Monitoring teams overwhelmed with events</td>
<td>Monitored threat vectors too narrowly focused (e.g., network monitoring only, no host-based IDS)</td>
<td></td>
</tr>
</tbody>
</table>
EY’s Managed SOC service has redefined security operations to meet the next generation of emerging cyber threats. Our service mission is to provide your organization with a highly mature detection and response capability designed to mitigate against threats that put your most critical business assets at risk. We will accomplish this by providing a high-performing team, executing process discipline and optimizing the use of technologies. In addition, by integrating these domains with our CTI capabilities, our Managed SOC also advances your ability to predict future threats.

For over 15 years, EY’s global Advanced Security Center (ASC) team has been delivering a range of cybersecurity services to many of our largest clients. This has included providing SOC design and build, along with strategic advisory services that are aligned to individual business requirements.

Our Managed SOC service combines our ASC advisory assessment, design and build experience, with information security professionals that possess a strong track record of operating SOCs on behalf of our clients. We differentiate our Managed SOC by offering you a high-end and customized service that is developed in a bespoke nature to match your specific business security needs.

For new SOC builds, our Triple Stack technology provides a unique integration of industry-leading commercial off-the-shelf (COTS) tools to monitor advanced threats on your endpoints and network, in addition to offering log aggregation and data analytics. We recognize that many organizations already possess a degree of security monitoring. Our team is also deeply experienced with a range of associated security-monitoring products and holds various related certifications. Accordingly, not only can we operate your existing monitoring capability, but we can complement your current capabilities with appropriate technologies from our Triple Stack solution to provide you with an enriched and forward-looking suite of services that will help you deal with new and emerging threats as they arise.

Our operation model

Our Managed SOC operates via a co-sourced or outsourced delivery model, with our professionals working closely with your team. In addition to establishing (or augmenting) your SOC, EY will provide security monitoring and incident response services to you via a managed service 24x7, anywhere in the world. The SOC will also be tightly linked with our threat intelligence team to facilitate the sharing of new and emerging indicators of compromise. To ensure that our Managed SOC provides maximum value to your business, we complement the technical components with scalable and managed “people” and “process” functions.

How EY can help you

EY’s Managed SOC service has redefined security operations to meet the next generation of emerging cyber threats. Our service mission is to provide your organization with a highly mature detection and response capability designed to mitigate against threats that put your most critical business assets at risk. We will accomplish this by providing a high-performing team, executing process discipline and optimizing the use of technologies. In addition, by integrating these domains with our CTI capabilities, our Managed SOC also advances your ability to predict future threats.

For over 15 years, EY’s global Advanced Security Center (ASC) team has been delivering a range of cybersecurity services to many of our largest clients. This has included providing SOC design and build, along with strategic advisory services that are aligned to individual business requirements.

Our Managed SOC service combines our ASC advisory assessment, design and build experience, with information security professionals that possess a strong track record of operating SOCs on behalf of our clients. We differentiate our Managed SOC by offering you a high-end and customized service that is developed in a bespoke nature to match your specific business security needs.

For new SOC builds, our Triple Stack technology provides a unique integration of industry-leading commercial off-the-shelf (COTS) tools to monitor advanced threats on your endpoints and network, in addition to offering log aggregation and data analytics. We recognize that many organizations already possess a degree of security monitoring. Our team is also deeply experienced with a range of associated security-monitoring products and holds various related certifications. Accordingly, not only can we operate your existing monitoring capability, but we can complement your current capabilities with appropriate technologies from our Triple Stack solution to provide you with an enriched and forward-looking suite of services that will help you deal with new and emerging threats as they arise.

Our operation model

Our Managed SOC operates via a co-sourced or outsourced delivery model, with our professionals working closely with your team. In addition to establishing (or augmenting) your SOC, EY will provide security monitoring and incident response services to you via a managed service 24x7, anywhere in the world. The SOC will also be tightly linked with our threat intelligence team to facilitate the sharing of new and emerging indicators of compromise. To ensure that our Managed SOC provides maximum value to your business, we complement the technical components with scalable and managed “people” and “process” functions.
## Enabling functions

<table>
<thead>
<tr>
<th>Program management</th>
<th>Services</th>
<th>Service activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology management</td>
<td>Security monitoring</td>
<td>Real-time monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pro-active hunting</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Alert analysis and triage</td>
</tr>
<tr>
<td></td>
<td>Incident response</td>
<td>Incident investigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Active guidance on containment, eradication and remediation</td>
</tr>
<tr>
<td></td>
<td>Threat intelligence</td>
<td>Malware analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tactical intelligence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Strategic intelligence</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### In scope

- [ ] Available if needed

---

### People

Our team will work closely with your in-house information security function to provide skilled on-site resources throughout the design and build phases of the project. Once normal operations commence, our remote 24x7 security monitoring team will be complemented by an on-site resource for 8x5 normal business hours operation to assist with advanced monitoring and response services.

1 Team responsible for deploying and maintaining all programmatic aspects of the MSOC service, including communications, metrics, documentation and training.

2 Team responsible for deploying and maintaining all technical components of the MSOC service.
Process
Managing a SOC in a clear and well-defined manner is crucial for its success. We will work closely with you to bring our proven SOC management processes to your environment and tailor them to your organization’s needs, where necessary.

Together, we will agree your managed SOC philosophy to drive a consistent approach. This will include:
- Mission statement
- Services
- Team structure
- Integration model
- Roles and responsibilities
- Metrics/KPIs
- Alert prioritization matrix
- Incident categorization
- Incident severity process
- Alert triage process
- IR processes
- Playbooks

Enabling technology

EY’s Cyber Threat Management (CTM) Services

Research and development

EY’s ASC

ASC private cloud

MSOC integration & service management layer

EY Managed SOC manual

Design/build
- Log aggregation
- Network monitor
- Endpoint monitor

Client 1
Client 2
Client 3
Client n

Operate
- Log aggregation
- Network monitor
- Endpoint monitor

Mission statement
Services
Team structure
Integration model
Roles and responsibilities
Metrics/KPIs
Alert prioritization matrix
Incident categorization
Incident severity process
Alert triage process
IR processes
Playbooks

L&D
Collaboration
Sandbox

Threat intelligence
Security monitoring
Incident response
Vulnerability identification
Remediation
Countermeasure planning
## EY differentiators

<table>
<thead>
<tr>
<th>EY differentiators</th>
<th>How we accomplish this</th>
<th>Value</th>
</tr>
</thead>
</table>
| "High touch" on-site resources to supplement 24x7x365 off-site resources | ▶ Heavy on-site presence during service initiation  
▶ Regular on-site rotation during standard business hours | ▶ More efficient validation of incident and greater assistance with response recommendations and/or execution assistance  
▶ Easier to identify and assist with capability improvements  
▶ Enriched service offering, customized to your specific monitoring priorities |
| Can be delivered as a co-source service, allowing your resources to be on the team and have access to EY’s monitoring solutions | ▶ Your team will have the access to our monitoring infrastructure to participate in monitoring and response  
▶ Regular on-site rotation during standard operations | ▶ Ability to manage cost by supplementing our analysts with yours  
▶ You retain direct access to your data (as needed)  
▶ Efficiency gained on incident containment and recovery |
| Industry-leading commercial off-the-shelf (COTS) solutions offered as part of EY’s services | ▶ Advanced monitoring and response solutions that provide visibility to endpoint and network activity, enabled by multiple, industry-leading commercial threat feeds  
▶ Deep analysis into session data, including content analysis and in-motion DLP  
▶ Aggregated logs, search, alerting, correlation and workflow | ▶ Increased ability to understand scope and extent of incidents  
▶ Rich data aggregation and search allows for “incident discovery” or “proactive hunting” when not alerted through predefined alert rules  
▶ Increased ability to detect interactive attackers |
| Breadth and depth of EY’s information security services available to assist with incident remediation advice | ▶ Access to a professional team with experience in major breach response  
▶ Access to EY’s subject matter resources to advise on a wide range of tactical and strategic information security improvements to help remediate incident root causes | ▶ Resources with deep knowledge of your environment to assist with improvement projects  
▶ Accelerated identification and prioritization of security improvements |
| Expertise in process design and operating effectiveness | ▶ Tried-and-tested, documented processes, procedures and playbooks  
▶ Process effectiveness monitoring and tuning | ▶ Manage impact to IT and security for incident containment and attacker eradication activities |
| Customized, robust metrics that provide insights to identify security program improvements | ▶ Metrics informed by business value or outcomes relevant to the business  
▶ Analytics used to inform countermeasure recommendations and identify areas to focus on improving defense posture effectiveness | ▶ Ability to describe security invasions in a manner that is meaningful to the business  
▶ Assists with prioritizing and funding improvement efforts  
▶ Generate information that drives good decision making |
| Ability to manage general, commodity malware and detect advanced threats/interactive attackers moving laterally, escalating privileges and targeting your high value assets | ▶ EY customized rules based on our extensive knowledge via our attack and penetration (A&P) services of how attackers compromise environments  
▶ Proactive hunting through rich data set and analytics engine  
▶ Focus beyond malware infections  
▶ Indicators from industry-leading commercial threat feeds | ▶ Increased ability to detect attackers with ability and intent to make material impact on your business |
Want to learn more?

**Insights on governance, risk and compliance** is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective. Please visit our Insights on governance, risk and compliance series at [www.ey.com/GRCinsights](http://www.ey.com/GRCinsights).

**Security Operations Centers — helping you get ahead of cybercrime**
[www.ey.com/SOC](http://www.ey.com/SOC)

**Get ahead of cybercrime: EY’s Global Information Security Survey 2014**
[www.ey.com/GISS](http://www.ey.com/GISS)

**Achieving resilience in the cyber ecosystem**
[www.ey.com/cyberecosystem](http://www.ey.com/cyberecosystem)

**Cyber threat intelligence — how to get ahead of cybercrime**
[www.ey.com/CTI](http://www.ey.com/CTI)

**Cyber Program Management: identifying ways to get ahead of cybercrime**
[www.ey.com/CPM](http://www.ey.com/CPM)

**Cybersecurity and the Internet of Things**
[www.ey.com/IOT](http://www.ey.com/IOT)

If you would like assistance or further information in relation to our Managed SOC services, please feel free to contact one of the following ASC team members:

**Global CTM Leader**

James Phillippe  
Email: james.phillippe@ey.com  
Phone: +1 713 750 8610

**Americas**

Chris Crevits  
Email: chris.crevits@ey.com  
Phone: +1 314 290 1786

**EMEIA**

Aidan Lynch  
Email: aidan.lynch@ie.ey.com  
Phone: +353 1 221 2994

**Asia-Pac**

Steve Lam  
Email: steve-yk.lam@sg.ey.com  
Phone: +65 6309 8062
If you were under cyber attack, would you ever know?

As many organizations have learned, sometimes the hard way, cyber attacks are no longer a matter of if, but when. Hackers are increasingly relentless. When one tactic fails, they will try another until they breach an organization's defenses. At the same time, technology is increasing an organization's vulnerability to attack through increased online presence, broader use of social media, mass adoption of mobile devices, increased usage of cloud services, and the collection and analysis of big data. Our ecosystems of digitally connected entities, people and data increase the likelihood of exposure to cybercrime in both the work and home environment. Even traditionally closed operational technology systems are now being given IP addresses, enabling cyber threats to make their way out of back-office systems and into critical infrastructures such as power generation and transportation systems.

For EY Advisory, a better working world means solving big, complex industry issues and capitalizing on opportunities to deliver outcomes that grow, optimize and protect our clients’ businesses. We’ve shaped a global ecosystem of consultants, industry professionals and alliance partners with one focus in mind – you.

Anticipating cyber attacks is the only way to be ahead of cyber criminals. With our focus on you, we ask better questions about your operations, priorities and vulnerabilities. We then work with you to co-create more innovative answers that help you activate, adapt and anticipate cyber crime. Together, we help you deliver better outcomes and long-lasting results, from strategy to execution.

We believe that when organizations manage cybersecurity better, the world works better.

So, if you were under cyber attack, would you ever know? Ask EY.

The better the question. The better the answer. The better the world works.
About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, 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. For more information about our organization, please visit ey.com.

© 2015 EYGM Limited. All Rights Reserved.
EY no. AU3201
ED None

In line with EY’s commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com/GRCinsights

About EY’s Advisory Services

In a world of unprecedented change, EY Advisory believes a better working world means solving big, complex industry issues and capitalizing on opportunities to help deliver outcomes that grow, optimize and protect clients’ businesses.

Through a collaborative, industry-focused approach, EY Advisory combines a wealth of consulting capabilities — strategy, customer, finance, IT, supply chain, people and organizational change, program management and risk — with a complete understanding of a client’s most complex issues and opportunities, such as digital disruption, innovation, analytics, cybersecurity, risk and transformation. EY Advisory’s high-performance teams also draw on the breadth of EY’s Assurance, Tax and Transaction Advisory service professionals, as well as the organization’s industry centers of excellence, to help clients deliver sustainable results.

True to EY’s 150-year heritage in finance and risk, EY Advisory thinks about risk management when working on performance improvement, and performance improvement is top of mind when providing risk management services. EY Advisory also infuses analytics, cybersecurity and digital into every service offering.

EY Advisory’s global connectivity, diversity and collaborative culture inspires its consultants to ask better questions. EY consultants develop trusted relationships with clients across the C-suite, functions and business unit leadership levels, from Fortune 100 multinationals to leading disruptive innovators. Together, EY works with clients to co-create more innovative answers that help their businesses work better.

The better the question. The better the answer. The better the world works.

With 40,000 consultants and industry professionals across more than 150 countries, we work with you to help address your most complex industry issues, from strategy to execution. To find out more about how our Risk Advisory services could help your organization, speak to your local EY professional or a member of our global team, or view ey.com/advisory

Our Risk Advisory Leaders are:

<table>
<thead>
<tr>
<th>Global Risk Leader</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paul van Kessel</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Area Risk Leaders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Americas</td>
</tr>
<tr>
<td>Amy Brachio</td>
</tr>
<tr>
<td>EMEIA</td>
</tr>
<tr>
<td>Jonathan Blackmore</td>
</tr>
<tr>
<td>Asia-Pacific</td>
</tr>
<tr>
<td>Iain Burnet</td>
</tr>
<tr>
<td>Japan</td>
</tr>
<tr>
<td>Yoshihiro Azuma</td>
</tr>
</tbody>
</table>

Our Cybersecurity Leaders are:

<table>
<thead>
<tr>
<th>Global Cybersecurity Leader</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ken Allan</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Area Cybersecurity Leaders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Americas</td>
</tr>
<tr>
<td>Bob Sydow</td>
</tr>
<tr>
<td>EMEIA</td>
</tr>
<tr>
<td>Ken Allan</td>
</tr>
<tr>
<td>Asia-Pacific</td>
</tr>
<tr>
<td>Paul O’Rourke</td>
</tr>
<tr>
<td>Japan</td>
</tr>
<tr>
<td>Shinichiro Nagao</td>
</tr>
</tbody>
</table>