Using cyber analytics to help you get on top of cybercrime

Third-generation Security Operations Centers
Contents

Introduction 1
Why have Security Operations Centers needed to change? 3
How can Active Defense be driven by threat intelligence? 7
Can data science be integrated into security operations? 11
Conclusion 15
Can using cyber analytics help you stay ahead of cybercrime?

In an increasingly online world, securing an organization’s digital assets is a key business concern. Cybersecurity is no longer regarded as a technical issue but is recognized as a fundamental business challenge for most organizations.

As the threatscape continues to evolve rapidly in both sophistication and scale, the need to protect organizations’ intellectual property, operations, brand and shareholder value, in addition to their customers’ data, is ever more critical. Advancements in the security industry have not kept pace with today’s diverse set of threat actors; organizations therefore find themselves in a position where off-the-shelf products and traditional services are not sufficient to address the risk.

Indeed, there is a need for bolder strategies and innovation in cybersecurity. Preparing for known attacks is challenging enough. But how do organizations build controls for the security risks they don’t even know about yet?

Leading organizations are doing more than improving on their current state. They are seeking to expand their efforts – to take bolder steps – to combat cyber threats and to keep pace with, or even get ahead of, the cyber attackers. Rather than waiting for the threats to come to them, these organizations are leveraging threat intelligence to prioritize efforts that enhance visibility and enable an Active Defense through tailored monitoring, analytics, hunting and prompt detection for their most critical proprietary data and business systems.

In recent years, organizations have recognized the benefits of having a well-functioning Security Operations Center (SOC). These include enabling cybersecurity functions to respond faster, work more collaboratively and share knowledge more effectively. First generation SOCs tended to focus upon signature-based controls, such as antivirus and intrusion detection systems, allowing organizations to detect “known bad” artifacts associated with an attack. The second generation of SOCs heralded the advent of 24x7 operations in recognition that attackers don’t close for the day, even if your business does.

EY is now seeing the emergence of the third generation of Security Operations Centers based around the development of professionally analyzed threat intelligence and cyber analytics to enable an Active Defense. Leading organizations seek to leverage cyber analytics platforms built on large-volume data-processing architecture, or so-called “lambda architecture”. This architecture combines batch and real-time processing and enables anomaly detection capabilities based on mathematics and statistical modelling that can handle terabytes worth of data daily. The third generation of security operations also facilitates proactive breach hunting, the integration of an enterprise cyber threat-management framework and the convergence of data science with security operations, enabling organizations to process large volumes of data for possible early indicators of compromise.

A key advantage to deploying a cyber analytics platform is its agility in using data science to speed up the ability to detect and respond to security incidents. This includes mechanisms to slow down the attackers through custom models that prevent them from replicating environments and learning to circumvent deployed controls.
Using cyber analytics to help you get on top of cybercrime — Third-generation Security Operations Centers
Why have Security Operations Centers needed to change?

What does a SOC do?

A well-functioning Security Operations Centre can form the heart of effective detection. It can enable information security functions to respond faster, work more collaboratively and share knowledge more effectively.

This document is intended to provide the reader with insights into the evolving state of SOCs in the context of emerging cyber threats. For a more introductory overview of fundamental SOC principles, we recommend reading Security Operations Centers – helping you get ahead of cybercrime.

www.ey.com/SOC

How SOCs keep up with the latest threats

In comparison with last year’s results, respondents to the 2015 survey recorded a marked increase in activity across all aspects of how their SOCs keep abreast of the latest threats. This indicates that organizations are making more concerted efforts to formalize and expand their SOC capabilities to better address emerging and increasingly sophisticated threats.

51%

Only 51% of organizations with a SOC initiate an investigation within one hour of a discovered incident.

23%

Only 23% consider their SOC to be tightly integrated with heads of business to regularly understand business concerns.
Third-generation SOC principles

While detecting signatures of known bad activities remains a relevant function of a SOC, third-generation SOCs have evolved to focus on identifying new threats for which no previous baseline has been observed. To achieve this capability, organizations need to integrate and align their various cybersecurity resources and investments, as outlined in the following guiding principles.

- **Integrated security operations**
  While organizations continue to significantly enhance their cybersecurity investments, threats continue to accelerate and outpace traditional security defenses and operational approaches. This causes many organizations to struggle to identify where to focus their investment and performance-improvement initiatives. Against this background, the need to establish richer context to aid operational and strategic cybersecurity decision-making is key. The third generation of security operations requires an enterprise-wide approach that integrates an organization’s various cybersecurity investments and activities.

- **Enterprise cyber threat management framework**
  A third-generation SOC requires an enterprise cyber threat-management framework to be designed and fully integrated around key business needs. Leveraging an appropriate cyber threat-management framework allows an organization to align its cybersecurity objectives with the rapidly accelerating threat landscape, its business priorities and its risk appetite. Such frameworks also enable organizations to maximize individual cybersecurity investments that may have already been made across the organization.

Enterprise cyber threat-management framework
The third-generation SOC principles empower an organization to implement an operating model for its SOC that supports the organization’s wider cyber threat-management framework and seamlessly integrates all cybersecurity disciplines, including threat management, threat intelligence, vulnerability management and cyber analytics.

Furthermore, these principles help an organization to define a set of clear improvement activities that are connected to achievable objectives. The team builds counter-measures, hunts hidden intruders and fortifies defenses based on real reporting about the behavior of real attackers.

This enables decision-makers to connect resource deployment directly to measures of cybersecurity program effectiveness. Instead of focusing on performance measures like “number of patches applied” and “number of tickets closed,” effectiveness is demonstrated via a decrease in successful targeted attacks and a decrease in the time required to discover and eradicate the attacks that were successful.

For further guidance on building an effective cybersecurity program, please refer to our Cyber Program Management – Identifying ways to get ahead of cybercrime report.

www.ey.com/CPM
How can Active Defense be driven by threat intelligence?

Active Defense is a deliberately planned and continuously executed campaign to identify and eradicate hidden attackers and defeat likely threat scenarios targeting an organization’s most critical assets.

It is an agile operational cycle designed to achieve rapid results and accelerate learning. Cyber Threat Intelligence (CTI) analysis can yield new insights about adversaries or the enterprise and generate actionable recommendations that allow the Active Defense team to execute missions focused on hunting or fortification. It is key to note that Active Defense enhances but does not replace security monitoring and incident response.

Keeping pace with determined attackers requires constant research and the ability to translate business strategy into actionable intelligence, understanding what it is that makes the business successful and then applying the cyber lenses to understand:

- **Who** would want to attack the organization (e.g., nation-state, activists or cyber criminals)?
- **What** would the adversaries be after? Organizations must understand what their most critical business assets are.
- **How** would the adversaries try to attack the organization? This includes understanding what types of techniques they would use (e.g., phishing campaigns, social engineering, etc.). Organizations must track their adversaries’ strategic goals, technical tactics and motives.

<table>
<thead>
<tr>
<th>Typical attack life-cycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intelligence gathering</td>
</tr>
<tr>
<td>Background research</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

- Highest-maturity SOCs have deeply embedded functional awareness of their organization’s high-value assets and external threat factors.
- They integrate threat intelligence, security monitoring, incident response and network and application vulnerability management to understand likely advanced attack paths and deploy counter-measures.
- By infusing the SOC with actionable threat intelligence, the organization maps the attackers’ likely paths and tactics, techniques and procedures (TTPs) to its most critical assets.
Step 1: Identify high-value assets and critical information
Step 2: Identify likely adversaries (intelligence/previous incidents)
Step 3: Identify likely courses of action for potential adversaries
Step 4: Leverage threat intelligence to identify tactics and preferred targets of the most dangerous/most likely adversary
Once organizations understand the business needs, risk appetite, industry-specific threat intelligence, threat-based security monitoring and vulnerability management, they need to map these to the kill chain. This provides the ability to see which types of attack techniques are used and the type of assets the attacker would target throughout the life cycle of the attack. With a well-mapped kill chain, organizations will be best placed to conduct counter-measure planning, hunting, anomaly analysis and more.

Active Defense does not replace traditional security operations capabilities. However, maximum effectiveness from an Active Defense program requires appropriate maturity levels in a range of competencies. These include security operations competencies, such as security monitoring and threat intelligence, in addition to activities such as asset identification and classification. By focusing on an Active Defense capability as a desired maturity level, decision-makers and security practitioners can engage in meaningful discussions about the steps for organizational improvement that will realize the benefits described herein. Activities include:

1. **Fortification**
   a. **Tailored counter-measures**: leverage insight from the intelligence process to design and implement counter-measures that defeat specific threat scenarios
   b. **Network reconnaissance**: manual identification and validation of complex vulnerabilities and threat scenarios and the development of network situational awareness for decision-makers

2. **Hunting**
   a. **Proactive forensics**: focused investigation for anomalous and malicious activity that cannot be detected by automated security-monitoring tools
   b. **Trapping and coercion**: alter network and endpoint conditions to provoke a hidden attacker into engaging in malicious activity liable to be detected by targeted intensive monitoring

Data and outputs from cyber analytics and threat intelligence enable Active Defense activities to take place – i.e., an effective Active Defense framework provides the “execution” element of cyber analytics and threat intelligence. It enables the definition of third-generation playbooks and use cases, to be leveraged by the data scientists for the creation of the models to identify and respond to cyber attacks.
Using cyber analytics to help you get on top of cybercrime — Third-generation Security Operations Centers
Can data science be integrated into security operations?

Data science, based on business-focused playbooks and identified use cases, can be leveraged to apply scoring to events, and combinations of events, in order to:

1. Produce continuous behavioral monitoring tools
2. Prioritize events for incident response and hunting
3. Provide agile response in the face of innovative attackers

Behavioral analytics for continuous monitoring

Leveraging analytics allows organizations to extract and present meaningful patterns from data. In the context of security, this has traditionally meant that rules and patterns can be extracted from past attacks and then matched against incoming data feeds.

With the evolution of the third generation of Security Operations Centers, behavioral analytics is extending previously accepted cyber analytics uses and capabilities by measuring the deviation from past behavior. Using statistical modeling, anomalies can be identified that indicate changes in behavior consistent with attackers. A major advantage of behavioral methods is that they do not require evidence of past malicious behavior and can be self-learning. Turn them on, expose them to data, and they will start learning what is “normal” versus what is “abnormal.”
The difficulty lies in identifying rare behavior that is consistent with attacks, not just rare but benign behavior. This is where data science needs to borrow from operational knowledge, in the form of incident response and penetration testers, to make sure that the statistical questions are being asked of the right data, in the right way, to trigger awareness when a rare event is consistent with attack behavior. It is rare to find data scientists with the combination of cybersecurity experience and data modeling skills, which is why acquiring this as a service is the primary delivery mechanism for many organizations.

By building statistical models to represent past behavior, organizations are beginning to score currently observed data and drive third-generation security-monitoring detection mechanisms. Sufficiently unusual events trigger alerts that are fed to dashboards or other reporting mechanisms to give to incident-response front-line detectors.

**Statistical hunting**

Leveraging analytics allows organizations to extract and present meaningful patterns from data. In the context of security, this has traditionally meant that rules and patterns can be extracted from past attacks and then matched against incoming data feeds.
Continuous innovation

The innovation speed of adversaries is far higher than that of the defense. Previously unknown, or so-called zero-day, vulnerabilities are commonplace. Even more challenging is the fact that attackers need only to identify one new method of attack behavior to avoid detection, whereas defenders need to cover all possible concepts of operations—an impossible task. Defensive tools suffer from the need to undergo product sales cycles that are in the order of years to bring new methods to market. Finally, the underlying network technology is constantly changing underneath the defenders, with the advent of “Bring Your Own Device” and the Internet of Things (IoT). There is a need to accelerate defensive operations, and data science can help.

Through interaction with hunting teams, incident responders and penetration testers, data scientists can rapidly deploy new methods for detection, acting directly on operational data to produce new continuous-monitoring tools and future indicators of attack. Organizations need to be able to ask thousands of questions of their data, determine which are effective and bring those rapidly into production.

Red teaming

The terms “red team” and “blue team” derive from traditional military war games: red teams are the attackers and blue teams are the defenders. In current cybersecurity usage, a red team is a group that actively challenges an organization to improve the effectiveness of its security via specific exercises that leverage techniques including penetration testing and social engineering, among others.

Such exercises should be undertaken regularly to monitor that both the organization as a whole and the platform architecture itself are secure from attack, using techniques similar to those exhibited by real attackers. Organizations need to ensure that any findings are fed back into the development life cycle for remediation.

Running red team versus blue team scenarios enables organizations to see how the cyber platform detects attacks and where opportunities exist to modify or build new detection models throughout the attack kill chain. Along with identifying potential blind spots within the network, this has the added benefit of training the new generation of hunters using controlled exercises. This is especially effective when a red team member is paired with the blue team, notifying the blue team of progress and validating detection.

Red team intelligence should be sourced from a variety of locations, including research papers, presentations and forums. By applying this information to the platform, an organization can determine how effective the cyber analytics are and whether there is a need for new models and anomaly-detection modules to be developed. Red team attack tools and methodologies are evolving faster than defensive tools and methodologies, so pairing red team researchers with data scientists and blue team hunters rapidly reduces the time to generate new models and modules. The red team can simulate the new attacks within the network to validate platform detection.
The ever-changing threatscape of an increasingly digital world challenges the defensive capabilities of even the most mature organizations.

A well-functioning SOC can form the heart of effective defense and provide a safe environment for the business to deliver on its core strategic objectives.

We are witnessing the convergence of specialist skill sets from disciplines related to cybersecurity, data science and analytics into advanced SOC ecosystems, where the whole is greater than the sum of its parts.

The driver behind third-generation security operations is an integrated cyber threat-management program. It integrates and enhances the enterprise’s existing security capabilities to achieve greater effectiveness against persistent attackers through an Active Defense. By implementing and executing an iterative cycle with built-in mechanisms for continuous learning and improvement, powered by cyber analytics and threat intelligence, organizations can realize gains in efficiency, accountability and governance capabilities. These gains translate directly into an improved return on investment for security programs by increasing the effectiveness of security operations and reducing the effectiveness of targeted attacks.

Questions for the board

How confident are you that your organization is not currently compromised? How do you know?

Do you have the right skills within your team to detect and respond to a targeted cyber attack?

Are you maximizing the return on your cybersecurity investments by integrating them under an aligned common framework?

Is your decision-making informed by accurate, intelligence-driven information?

Is your SOC aligned with your business strategy to ensure focus is retained on high-value assets?

How can EY help?

Whether you are designing a SOC from scratch or improving your existing capabilities, EY can help you through every step of the journey.

Our approach of integrating threat intelligence, security monitoring, incident response and security analytics reflects the reality of detecting APT-style behaviour on your network, including endpoint threat detection and data exfiltration.

Threats continue to evolve; your SOC must too. Our services are designed to wrap experienced people and efficient processes around leading technologies to provide a business-focused SOC that can evolve with your organization’s needs and the changing threat landscape.
Using cyber analytics to help you get on top of cybercrime — Third-generation Security Operations Centers

**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).

---

1. **Creating trust in the digital world:** EY’s Global Information Security Survey 2015
2. **Managed SOC:** EY’s Advanced Security Center: world-class cybersecurity working for you
   - [www.ey.com/managedSOC](http://www.ey.com/managedSOC)
3. **Achieving resilience in the cyber ecosystem**
   - [www.ey.com/cyberecosystem](http://www.ey.com/cyberecosystem)
4. **Reducing risk with Cyber Threat Intelligence**
   - [www.ey.com/CTI](http://www.ey.com/CTI)
5. **Cybersecurity and the Internet of Things**
   - [www.ey.com/IOT](http://www.ey.com/IOT)
6. **Cyber program management: identifying ways to get ahead of cybercrime**
   - [www.ey.com/CPM](http://www.ey.com/CPM)
7. **Get ahead of cybercrime:** EY’s Global Information Security Survey 2014
8. **There’s no reward without risk:** EY’s global governance, risk and compliance survey 2015
9. **Unlocking the value of your program investments:** How predictive analytics can help in achieving successful outcomes
   - [www.ey.com/PRM](http://www.ey.com/PRM)
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 find 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.
EYG no. AU3587
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 inspire 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>Scott Gelber</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>