Symantec

Cyber Security Services

Symantec

The Cyber Guide

Questions Every CISO Must Answer

How secure is my organization?

One of the most difficult questions CISOs must answer

A cyber attack puts everything at risk — an organization's brand, reputation, and intellectual property. CISOs know they must make fast and informed decisions during a crisis and also quickly assess the scope and impact of the attack, identify who is attacking, and understand the motivations and goals of the attacker. Assessing the security of an organization is no small task.

With this in mind, CISOs around the globe shared four questions they use to gauge their security postures and the state of their security programs across every stage of the attack lifecycle—before, during, and after an attack. How confident are you in your answers to these questions and the additional questions they generate?

Does our threat intelligence program enable us to make faster, more definitive decisions?

- How do we know if we are being targeted, and can we identify emerging threats in our industry or geography with enough time and context to implement proactive controls?
- Who is responsible for implementing a threat intelligence program that integrates across our security technologies, teams, and executive cyber-risk decisions?
- How quickly can we understand who is attacking us—and the scope, impact, and severity level of an attack—to determine the best response to each incident?

Do our security operations allow us to diagnose critical threats in real time?

- How do we use real-time data analytics 24x7 to identify and categorize truly critical attack activity—from low-and-slow persistent events to more overt attacks?
- Do we correlate internal activity with relevant threat intelligence beyond our perimeter to more quickly identify advanced attacks?
- How do we balance proactive hunting with reactive identification of emerging threats, and do we continuously monitor for persistence mechanisms to hold off repeat or attack variants?

How quickly and effectively do our teams respond when faced with an incident?

- Does our cross-functional team know what process to follow in the first minutes, hours, and days following incident detection?
- When did we last test our incident response plan and assess for readiness? Did we improve?
- Do we continuously refine our processes based on lessons learned from past attacks?

How do we focus on our people to develop organizational preparedness for an attack?

- How do we train and test our security and IT teams on the latest attacker techniques?
- How prepared is our nontechnical employee base to recognize and avoid social engineering and other targeted attacks?
- How do we reduce turnover of our highly skilled security and IT professionals and maintain an engaging and innovative culture?

Symantec Cyber Security Services offers what no other organization can provide – an integrated and purpose-built portfolio of human expertise, advanced machine learning capabilities and technologies, and actionable global threat intelligence.

Each offering in the Cyber Security Services portfolio is designed to integrate with one another and fuel an organization's cybersecurity program with better insight and faster detection and response capabilities across the entire attack lifecycle.

BEFORE AN ATTACK:
Track and analyze adversary groups and key trends and events around the globe for actionable intelligence.

Symantec DeepSight™ Intelligence provides a deeper understanding of the threat landscape so organizations can make more informed decisions to proactively mitigate cybersecurity risk. Technical and strategic intelligence keeps security and intelligence teams informed of industry-specific vulnerabilities, providing advanced analysis of attacks, and sharing the motivations and techniques of threat actors.

DURING AN ATTACK:
Detect targeted and advanced persistent threats and campaigns.

Symantec Managed Security Services enables organizations to focus on critical alerts by utilizing advanced analytics, actionable threat intelligence, and a seasoned team of global security professionals who provide 24x7 threat monitoring and proactive threat hunting. Each customer is assigned a designated service manager and analyst team who are experts in the customer's industry, providing continual collaboration and partnership.

AFTER AN ATTACK: Respond quickly and effectively to credible security threats and incidents.

Symantec Incident Response Services work with organizations around the globe to validate and respond to incidents with speed and precision. Drawing from years of experience and leveraging powerful threat intelligence and industry-accepted forensics tools and procedures, Symantec helps organizations return to business as quickly as possible and strengthening an organization's overall ability to detect and eradicate future threats.

PREPARATION FOR AN ATTACK:
Strengthen cyber readiness across the entire organization to recognize and prevent advanced attacks.

Symantec Cyber Skills Development Services increase organizational resiliency to cyber attacks and develop security literacy of both technical and non-technical employees. This portfolio trains and assesses end-user susceptibility to attacks including those that leverage social engineering tactics such as spear phishing. Additionally, scenario-based, live-fire training provides a safe environment for technical users to understand the current threat landscape, motives, and methodologies of the adversary.

Confidence

Key Security Questions

With Symantec Cyber Security Services, organizations can confidently answer the four key questions, and many others, to gauge and improve their security posture and the state of their security programs across every stage of the attack lifecycle.

Does our threat intelligence program enable us to make faster, more definitive decisions?

- The ideal situation is to know about a threat **before it strikes** with enough time and detail to deflect and disrupt the attacker. Symantec delivers a form of advanced **cyber radar**, providing early warning of emerging attacks before they strike.
- Know the who, what, when, where, and how of global threats, including **cyber espionage**, **cyber crime**, and **hacktivist** threats to quickly assess cyber risk and implement necessary countermeasures.
- DeepSight Intelligence helps organizations understand the **scope**, **impact**, and **severity level** of an attack by using both technical and strategic adversary threat intelligence. Both types of intelligence are necessary to understand the actors and groups behind an attack, their motivations, exploited vulnerabilities, and malware utilized.
- Symantec experts follow more than 700,000 adversaries around the world and apply **intelligence tradecraft** to both Symantec intelligence and open-source collections. DeepSight teams understand who is **behind a threat**, the organization(s) being targeted, and methods and motivations of the attacker. They have access to the malicious code, the systems being hit, the emails that were sent, adversary insights, and a rich dataset to see the full scope of a threat. This fuels the creation of useable intelligence and **empowers fast action**.

Do our security operations allow us to diagnose critical threats in real time?

- Symantec has one of the **largest human networks of cyber experts armed with advanced analytics** to extend an organization's cybersecurity program across the entire attack chain.
- With an average of only four percent of alerts getting investigated[1], organizations often miss critical indicators of an attack due to a lack of skilled staff, experience, and the general inability to analyze most of their alerts.
- Every customer has a designated Symantec Managed Security Services **service manager** and analyst team monitoring their organization 24x7, applying relevant global threat intelligence and proactively hunting for advanced attacks that traditional security technology may have missed.
- When we find a new indicator of compromise across our **neural network** and threat-intelligence services, that knowledge is applied across the entire customer base to hunt and detect the threat before it potentially damages multiple organizations.
- When an attack occurs, our teams continuously monitor customer environments identified indicators and leverage global threat intelligence to ensure the threat is eradicated and there is no **advanced persistent threat activity**.

[1]2015 Ponemon Research

1,000+
certified cybersecurity professionals

15+ years
delivering advanced threat monitoring and log management

12+ average years
of active in-field investigation

700,000+
threat actors and groups tracked globally

One of the world's largest cyber war games programs

How quickly and effectively do our teams respond when faced with an incident?

- Symantec **helps to keep an incident from becoming a breach**. Once an incident occurs, it should be triaged as quickly as possible to stop attack activity and keep the attacker from exfiltrating information. Fast eradication of a threat is desired, yes, but steps are needed to isolate and remove the threat without impacting the ability to **preserve and safeguard evidence.**

- Our seasoned **incident response experts** work with organizations around the globe to quickly collect, preserve, and analyze evidence to **mitigate the business impact** of an incident. Investigators provide management support and communications, empowering security leaders to make the necessary business decisions return to normal operations.

- For organizations who also partner with Symantec Managed Security Services for threat monitoring, Incident Response investigators can engage and work with their Managed Security Services team to **more quickly assess and resolve the situation.** Incident Response teams also engage Symantec DeepSight experts to **identify relevant threat intelligence** that may aid in a faster understanding of the threat situation and resolution.

- Preparation is key. Symantec experts can assess and provide **readiness workshops** and **tabletop exercises** to build and test an organization's incident response program to more quickly and effectively respond in the minutes, days, and weeks after an incident occurs. **Cyber insurers** often consider incident response preparedness in their cyber risk assessments and policies.

- Reduce the probability and severity of future incidents by applying lessons learned from an incident to security-device management rules and policies. Symantec provides recommendations in post-incident comprehensive investigative reports.

In what ways are we focused on our people to develop organizational prepareness for an attack?

- The breadth of the **Symantec Cyber Skills Development** portfolio prepares the human element of cyber defense—both technical and non-technical employees. Employee action or non-action may aid an attacker to infiltrate the network.
- Spear-phishing campaigns increased by 55 percent in 2015[2]; attackers are getting more targeted and sophisticated in their delivery. Reduce the end-user exposure point and condition employees to recognize attacks and vulnerable situations with relevant, engaging security training and assessment programs.
- **Hiring, training, and retaining** key security professionals is challenging for organizations. Continuously challenge and keep security teams engaged and up-to-date on the latest attacker tools and tactics leveraging live-fire, virtual training scenarios.

[2]Symantec ISTR 2016

Symantec Cyber Security Services extend an organization's capabilities to assess and reduce cyber risk by providing what no other vendor can offer: **a portfolio powered by global threat intelligence, advanced analytics, and a global human warrior network**. Individual operations capabilities across security monitoring, threat intelligence, incident response, and cyber skills development are integrated to limit gaps between systems and operations and empower organizations to take faster, more decisive action against threats.

With Symantec, you can rely on one comprehensive and integrated portfolio, one designated team assigned to each customer, one interdisciplinary operation to provide better insight and faster detection and response to advanced threats before, during, and after an attack.

Get more information

Cyber Security Services:
symantec.com/cyber-security-services

Partnering with a World-Class Security Team

Extending security organizations globally with an integrated portfolio of human expertise, advanced analytics, and applied global threat intelligence.

Imagine what organizations could do if they had a fully staffed team of security experts — with years of experience in a Security Operations Center (SOC) or government agency — tracking activities of cybercriminals and combatting threat activity around the world. This dream team would include all the key skills required to run a state of the art security program; intelligence and real-time threat analysts to quickly and effectively identify incoming and active threats combined with forensics and response experts who have experience investigating a full array of incidents and know how to execute and drive a comprehensive incident response program.

More than 80% of organizations1 believe there's a shortage of security staff necessary to address today's advanced threats. Many security leaders need help building up their existing teams and often choose to extend their internal teams with external expertise.

Symantec™ Cyber Security Services provides around-the-clock access to the necessary skills and threat insights for a best-in-class organization, powered by world-class security professionals located around the globe who are dedicated to every stage of the attack chain—before, during, and after an attack. Our services are uniquely poised to bring the combined power of global insight into advanced security threats and incidents, while also providing local in-region security expertise.

Comprehensive expertise

Cyber Security Services teams are integrated, sharing insights and expertise of the global threat landscape across advanced monitoring services, security technology and response, and adversary and threat Intelligence. Areas of expertise include: human and technical intelligence
collection, intelligence analysis, cyber espionage and nation-state cyber threats, cybercrime threats (including point-of-sale malware), hacktivism, critical infrastructure security, computer forensics, cryptography, incident response, malware reverse engineering, botnet emulation and tracking, and vulnerability research and discovery.

Symantec security professionals are handpicked from organizations and government agencies around the world. Industry-tested professionals have earned a wide range of degrees and certifications with 100% SANS certified security intrusion analysts (GCIA) as well as certified incident handlers (GCIH), CISSP, GPEN, CSSLP, CE|H, STS, GCFA, OSCP, VTSP5, CCNA, CCNP, CCIE, FCNSA, Security+, CCNA Sec, SFCP,CCAI, CCNP Sec, JNCIS Sec, F5-CA, RHCSA, ITIL v3, SA1, SFCP, J.D., and M.S. in forensics.

Symantec security experts are members of HTCIA, HTCC, CTIN, CERT, ISC(2), and many other professional security forums.

[1] Michael Suby and Frank Dickson, The (ISC)2 Global Information Security Workforce Study, Frost & Sullivan, April 16, 2015.

Combined expertise

10

years
average
experience

in cybersecurity and intelligence

Best-in-class threat intelligence

Symantec threat intelligence analysts and researchers track over 700,000 cybercriminals around the globe. They apply intelligence tradecraft to transform raw threat data, adversary activities, and analyze data from one of the world's largest civilian network of threat intelligence, Symantec's Global Intelligence Network, to create in-depth research reports and actionable defense measures. They are equipped with an arsenal of industry and government experience, averaging 10 years in the industry, from agencies including: National CERTs, National Cyber-Forensics and Training Alliance, FBI National Defense Agencies, Air Force Cyber Command, and Computer Security Incident Response Capability.

Global visibility, local relationships

Cyber Security Services teams become an extension of an organization's security teams. Organizations partner with a designated team of experts who work closely with the customer's strategic and operational teams to tailor and align services to support their unique business models and goals.

When an incident occurs, organizations work with the same lead investigator throughout the engagement, ensuring consistency, expertise, and end-to-end knowledge of the incident. This global presence and close partnership with all customers allows Symantec to reduce security risks and respond more quickly to critical incidents.

Private-sector prowess

Symantec security experts have extensive experience in the private sector. They have founded startups and worked internationally with the Big Four consulting firms. They have served as security consultants and analysts in the world's leading fields of business, including: information security, finance, retail, telecommunications, manufacturing, entertainment and gaming, national infrastructure, and health care.

Public-sector excellence

Symantec security team members have spent years working at top levels in the United States, United Kingdom, and Australian governments in agencies including: Federal Bureau of Investigation, Central Intelligence Agency, U.S. Special Operations Command, National Security Agency, U.S. Department of theTreasury, U.S. Department of Defense, U.S. Department of Homeland Security, Joint Chiefs of Staff, European Commission Incident Response Team, European Commission Cyberattack Response Team, Government of Luxembourg Computer Emergency Response Team, and Australian Department of Defence.

The DeepSight Intelligence Managed Adversary and Threat Intelligence (MATI) team members have an average of 10 years of experience.

Areas of expertise include:

- Human and technical intelligence collection
- Intelligence analysis
- Cyber espionage and nation-state cyber threats
- Cybercrime threats including point-of-sale malware
- Hacktivism
- Industrial controls systems (ICS) security
- Advanced penetration testing
- Computer forensics
- Cryptography
- Incident response
- Malware reverse engineering and fuzzing
- Botnet emulation and tracking
- Vulnerability research and discovery

Public sector

- Federal Bureau of Investigation
- Central Intelligence Agency
- US Special Operations Command
- National Security Agency
- US Department of the Treasury
- US Department of Defense
- US Department of Homeland Security
- Joint Chiefs of Staff
- European Commission incident response team
- European Commission cyber-attack response team
- Luxembourgish National GovCERT
- Australian Department of Defense

Private sector

- Information security
- Telecommunications
- Finance
- Manufacturing
- Systems engineering

Patents and process know-how

Symantec experts possess skill and experience in all areas of patents and process security, including: automated threat intelligence across enterprise devices, machine-learning threat-intelligence feedback, dynamic malware analysis, and covert and counterintelligence methods.

Industrywide capability with all threat types

Understanding how threat actors work and the characteristics of their evolving attack technologies and methodologies is critical to anticipating future incidents. Symantec security experts have that understanding and experience with access to powerful threat intelligence and tools.

The following figures summarize the incidents Symantec has triaged, investigated, and contained since January 2013 by vertical, incident type, and membership in the Fortune 500.

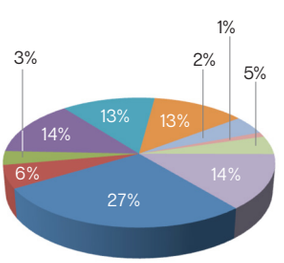

Figure 1:
Incident response engagements by vertical

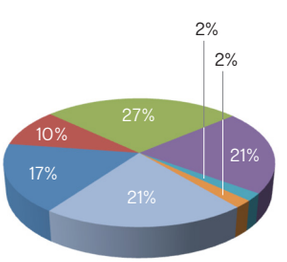

Figure 2:
Incidents by type

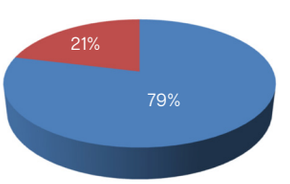

Figure 3:
Incidents by Fortune 500 status

- Healthcare
- Communications
- Software
- Retail
- Financial services
- Accounting
- Telco
- Gaming
- Education
- Manufacturing
- Malware outbreak - previously unknown
- Virus
- Web application attack
- Malware outbreak - known
- Advanced persistent threat
- DDoS
- Application exploitation
- Other
- Fortune 500

Unmatched Global Security Skills Development Experience

CyberWar Games

- 1500+ participants
- 80+ onsite events delivered in 30+ countries
- Trained 16,500+ users in 60+ countries
- Trained well-known cyber vendors, large financials, and 3-letter agencies

Get more information

Incident Response:
symantec.com/incident-response

Cyber Security Services:
symantec.com/cyber-security-services

Emergency response help

Email:
incidentresponse@symantec.com

Call our Incident Response team:
+1 (855) 378-0073

Symantec DeepSight Intelligence Services

Better anticipate and mitigate cybersecurity risk with actionable threat intelligence

New threats are emerging daily, and hostile cyber attacks are on the rise. Traditional security solutions are not always effective when facing advanced attacks. CISOs need a robust threat intelligence program and a clear understanding of the current and emerging threat environment so they can create a proactive and effective defense.

DeepSight™ Intelligence provides a full view of cyber risk for organizations, helping security teams to craft the right strategy for managing cyberattacks, before, during and after they occur. As a cloud-based, cyber threat intelligence platform, DeepSight delivers a timely stream of threat intelligence via a customizable portal and web services to empower security teams and make security technologies smarter.

With a DeepSight threat intelligence program, organizations can put preemptive measures in place to mitigate risks and respond forcefully to targeted attacks. DeepSight™ Intelligence provides both adversary and technical insight that is:

Timely - Intelligence is sourced by continually monitoring adversaries; researching the Dark Web; anonymously collecting real-time threat information from Symantec's installed base of products; and observing attack activity to produce intelligence that is useful before, during, and after an attack.

Relevant - DeepSight analysts focus on providing technology, industry, and geographically organized insights to explicitly address the direct or near-term implications of threats.

Context-rich - The service draws from a variety of intelligence collection sources, including web gateways, emails, endpoints, and by following adversaries around the globe. Using these resources, DeepSight provides rich contextual data on the nature of attacks and their actors, as well as suggested mitigation.

Accurate - Analysts and algorithmically generated deliverables examine the reliability, variety, and quality of sources to minimize errors and ensure quality intelligence.

Gain valuable insights by analyzing the adversary

To better assess the impact and risk from known and unknown threats, DeepSight's Managed Adversary and Threat Intelligence (MATI) research team is strategically positioned around the globe to track over 700,000 adversaries and understand the constantly evolving threat ecosystem. MATI reports provide rich context about an adversary's campaigns and tactics, informing organizations of emerging threats and their associated indicators, as well as attribution and motivation behind cyberattacks.

"Use a commercial threat intelligence service to develop informed tactics for current threats, and plan for threats that may exist in the midterm future."[2]

Gartner, Inc., Market Guide for Security Threat Intelligence Services, Rob McMillan, Khushbu Pratap,
22 October 2015

Cyber Security Services

Adversary Insight

Get tailored answers to unique and specific security questions

DeepSight's Directed Threat Research takes our MATI research one step further, providing tailored cyber threat intelligence reports addressing an organization's specific questions. With DeepSight's vast collection network, skilled analyst and research teams, and unique tools and processes, security leaders can augment their internal capabilities and improve their overall security posture.

Make security teams smarter

DeepSight provides multiple teams with access to comprehensive threat intelligence. Security operations teams received needed context around a threat so they can more quickly detect an advanced attack. Threat and vulnerability teams are armed with timely and accurate intelligence so they can implement proactive controls before an attack occurs. Incident response teams are provided with the details surrounding an attack including who's behind it, their motivations, and their attack tactics to more quickly contain and eradicate the threat before an actual breach occurs.

Leverage a fully integrated solution

A successful cybersecurity program requires a comprehensive strategy and integration across technology and people. Each offering in Symantec's Cyber Security Services portfolio — Managed Security Services for advanced security monitoring; DeepSight™ Intelligence for actionable technical and strategic threat intelligence; Incident Response for fast containment and eradication of a threat; and Cyber Skills Development for strengthening the entire organization's ability to recognize and prevent advanced attacks — is designed to work together and improve the speed and effectiveness of an organization's security program.

Make security technologies smarter

Through the DeepSight API and Datafeeds, we make it easy for an organization's security technologies to consume and query our technical and strategic intelligence. DeepSight integrates with key security solution partners, ensuring a smarter and more automated approach to security. Intelligence available for automation includes vulnerability, network and file-reputation, adversary, campaign, security risk and malcode data.

Get more information

Deepsight Intellligence:
symantec.com/deepsight-products

Cyber Security Services:
symantec.com/cyber-security-services

5/2016 21359232 - BROCHURE OVERVIEW CYBER SECURITY SERVICES

Symantec

Symantec Managed Security Services

Reduce the time between detection and response, and minimize the business impact of an attack with continual advanced security monitoring.

In this evolving cyber landscape, attackers move faster, threat actors are smarter, and the time to detect an attack takes too long. Many companies are struggling to keep up. More than 80 percent of organizations1 believe there is a shortage of security staff necessary to address today's ever-changing threats.

SymantecTM Managed Security Services Advanced Security Monitoring (MSS) extends an organization's internal security operations program by expertly monitoring the environment 24x7 and applying global threat intelligence to detect advanced attacks. Symantec MSS complements the infrastructure already in place and helps security leaders to improve their security operations program and better manage their organizations' security posture before, during, and after an attack.

Work with a designated team for 24x7x365 continual monitoring

Our MSS program provides access to Symantec's world-class team of professionals across our Security Operations Centers and Security Response Centers around the globe. Each client works with the same designated Service Manager and team of analysts and engineers who hold multiple certifications and accreditations, including Global Information Assurance Certification (GIAC) and Certified Information Systems Security Professional (CISSP).

Teams are assigned based on vertical and organization size and work closely with each customer to understand their environment, business goals, and processes. They are available 24x7, actively monitoring the environment and offering insights on malicious activity that can potentially impact each customer's business. This team truly becomes an extension of a client's security team.

Stay focused and pinpoint critical threats

With a deluge of alerts, it can be difficult to know which threats are most dangerous Symantec MSS helps to reduce false-positives and prioritize activity according to each customer's business model and goals. As a result, security teams can focus efforts on the highest priority incidents.

[1] *Michael Suby and Frank Dickson, The (ISC)2 Global Information Security Workforce Study, Frost & Sullivan, April 16, 2015.*

"Armed with a marketplace of exploits, specialized skills and sales opportunities, hackers can easily piece together attacks that circumvent traditional security controls and look like normal behavior to security monitoring tools."

ESG White Paper, SOC-as-a-service for Midmarket and Small Enterprise Organizations, March 2015

Accelerate

See more, correlate more, detect more

MSS teams have unparalleled visibility into the evolving threat landscape. Our analysts are familiar with the tactics, techniques, and procedures (TTPs) of adversaries around the world and will proactively hunt and identify advanced attacks. With access to one of the most comprehensive sources of global threat data in the world, we provide the information customers need to minimize risk and reduce the impact of today's sophisticated threats. When we find a new indicator of compromise across our neural-network and threat intelligence services, we can apply that knowledge across our entire customer base to detect the threat before it can damage multiple organizations.

Reduce operational costs

- Predictable Expense
- Budgetable Cost
- Measurable SLAs

Extend your security team

- Dedicated, GIAC-certified analysts
- 24 X 7 access to counsel
- Automated monitoring

Accelerate detection & response

- Insights from the Symantec GIN
- Context on adversaries and campaigns
- Analytics/retroactive log analysis

Enable compliance

- Assistance with compliance documentation
- Access all security incidents and events
- Monthly report on analysis and actions

Leverage a fully integrated solution

A successful cybersecurity program requires a comprehensive strategy and integration across technology and people. Each offering in Symantec's Cyber Security Services portfolio — Managed Security Services for advanced security monitoring; DeepSight™ Intelligence for actionable technical and strategic threat intelligence; Incident Response for fast containment and eradication of a threat; and Cyber Skills Development for strengthening the entire organization's ability to recognize and prevent advanced attacks — is designed to work together and improve the speed and effectiveness of an organization's security program.

2-7 Carson Zimmerman, Ten Strategies of a World-Class Cybersecurity Operations Center, The MITRE Corporation, 2014.

Considering a do-it-yourself security operations center?

24x7 coverage

must maintain a minimum of analyst coverage at all times

- Two-person integrity is a best practice. [2]
- Multiple analysts can cross-check each other's work.[3]
- Each 24x7 seat requires roughly five FTEs, including fill-ins for vacation and sickleave.[4]
- Assuming a minimum of two filled analyst seats, this roughly equates to 10 FTEs.[5]
- **This is expensive –** $1 million per year.[6]

At least

1.5 – 2 years

Time it takes to fully operationalize a SIEM platform, let alone build a full security operations center. [7]

Symantec Managed Security Services provides

24x7x365 threat monitoring

across all devices in an organization and is operational within days; organizations realize a return on their investment almost immediately.

Get more information

Managed Security Services:
go.symantec.com/mss

Cyber Security Services:
symantec.com/cyber-security-services

5/2016 21359232 - BROCHURE OVERVIEW CYBER SECURITY SERVICES

Symantec™

Symantec Incident Response Services

Respond quickly to credible security threats and incidents with an effective incident response program

Incident preparation has evolved from "if an attack will happen" to "when" — highlighting the importance of a comprehensive incident response program and trusted partners to quickly validate and contain threats. After an attack occurs, security and response teams face immense pressure to assess, respond, and contain a threat while engaging cross-functional stakeholders. When incidents are handled efficiently, the cost, duration, and overall exposure can be decreased, and impact to the business can be minimized. Symantec's Incident Response team partners with organizations to turn a reactionary plan into a repeatable, optimized program. With a powerful response program in place, organizations can react decisively and effectively when a security incident occurs. Better still, they can learn from every attack and proactively defend against the next one.

A programmatic approach to incident response

The time to build a response plan is not during an incident. The time to prepare is now. Advanced planning will lead to more quickly resolved incidents, with less chance of reoccurrence, and more informed stakeholders. Utilize threat hunting services, tabletop exercises, and readiness assessments to set a baseline of the health of the network and employee abilities. With an Incident Response Retainer, organizations benefit from readiness services, prenegotiated terms, and service level agreements (SLAs) to take control of their program and feel confident with their response capabilities.

Programs Needed for Incident Response

Process Stage	Preparation	Detection & Analysis	Containment, Eradication, & Recovery	Post-incident Activities
Services/ Activities	· Incident Readiness Assessment · IR Plan Assessment · IR Program Development · Table Top Exercises · APT Hunting Services	· Incident Triage · Log Analysis · Fly to Sight Incident Handling · Remote Investigation · Network Analysis · System Analysis · Memory Analysis	· Advanced Malware Analysis · Intelligence · Develop & Implement Containment Strategy · Create Recovery Plans · Restore Normal Business Operations	· Summary of Analysis · Recommendations · Customer Board Presentation

"Symantec's offering is a game changer for the way IR services are being charged today both because of flat-rate, predetermined pricing and because they use the learnings from an incident to improve their protection solutions."

Analyst Firm, IDC

"The skills, professionalism and recommendations provided by Symantec's Incident Response team were instrumental in our ability to respond effectively and were the best we have ever experienced."

VP of Information Systems, Large Insurance Company

Integrated

Stay ahead of adversaries with integrated threat intelligence

Incident Response teams have access to one of the world's most comprehensive repositories of threat telemetry — Symantec's Global Intelligence Network (GIN) — and Symantec's DeepSight™ Intelligence research that has been developed by following over 700,000 adversaries around the globe. This intelligence provides incident investigators with critical information to leverage when proactively hunting for advanced threats and when actively responding to an incident. This rich intelligence provides indicator attribution and helps to determine the motives behind an attack while also enabling visibility into vertical-and regional-specific aspects of the threat landscape. This is a critical component to staying abreast of potential methods and modes of attack.

Partner with the cyber insurance ecosystem

To reduce the financial consequences of a breach, many organizations have cyber insurance policies. Symantec works closely with an ecosystem of brokers, insurance carriers, and privacy attorneys to provide customers with the best quality of service as part of their cyber coverage

Comprehensive and integrated solutions for success

A successful cybersecurity program requires a comprehensive strategy and integration across technology and people. Each offering in Symantec's Cyber Security Services portfolio — Managed Security Services for advanced security monitoring; DeepSight™ Intelligence for actionable technical and strategic threat intelligence; Incident Response for fast containment and eradication of a threat; and Cyber Skills Development for strengthening the entire organization's ability to recognize and prevent advanced attacks — is designed to work together and improve the speed and effectiveness of an organization's security program.

Receive top performance and a tailored strategy

- *Experience with incidents across all industry verticals and governments*
- *Extensive experience in public and private sectors including the FBI, U.S. DoD, Y.S. NCIS, U.K. National Cyber Crime Unit, New Scot land Yard Computer Crime Unit, NATO.*
- *Average of 12 years of active investigation experience in the field*
- *Extended team of more than 1,000 security experts around the globe*

Get more information

Incident Response:
symantec.com/incident-response

Cyber Security Services:
symantec.com/cyber-security-services

Emergency response help

Email:
incidentresponse@symantec.com

Call our Incident Response team:
+1 (855) 378-0073

5/2016 21359232 - BROCHURE OVERVIEW CYBER SECURITY SERVICES

Symantec

Ready

Symantec Cyber Skills Development Services

Strengthen cyber readiness across the entire organization to better recognize and prevent attacks

Often, the most obvious attack vector goes unprotected—humans. With Symantec Cyber Skills Development, organizations can raise the security IQ of all employees by addressing challenges faced by each individual. Engaging content and interactive skills challenges vary across technical and non-technical teams, ranging from something as simple as safely working remotely in a coffee shop, to understanding what advanced methods attackers are using to access and pivot across networks.

Materials are kept up to date and relevant to address the latest methods used by today's cyber enemies, and backed by industry leading threat data from Symantec's Global Intelligence Network, organizations can gain confidence that all employees are prepared to thwart targeted attacks.

Strengthen cyber warriors in a virtual battlefield

A soldier would never be sent into battle without live-fire training, so why would a textbook trained IT staffer be expected to go head-to-head with the most experienced attackers? By immersing IT teams in a simulated environment filled with the latest threats and vulnerabilities seen in the wild, they're better prepared to think like the adversary while challenging their skills in a real-world scenario. Symantec's Cyber Security Exercise allows managers to assess the skills of participants, identify functional gaps, and formulate plans to address those gaps with additional exercises or hiring.

By 2020, the security industry will be short 1.5 million information security professionals, with this shortage interestingly cited by half of cybersecurity staff as a key reason for data breaches (48%).

(ISC)²

"Your Cyber Security Exercise changed my life."

Fortune 100 Bank employee who was discovered as a hidden talent, moving from the Helpdesk to the Red Team.

Strengthen

Email inboxes are a hunting ground for adversaries

Email-based attacks targeting employees continue to be the number one entry point into an organization. According to the Anti-Phishing Working Group, there were 106,421 reported spear-phishing campaigns in September 2015 alone1. With the average successful spear-phishing campaign costing an organization upwards of $1.6 million2, companies must face these threats head-on.

Companies are meeting the challenge by conditioning employees to recognize social engineering tactics and to report phishing attacks with Symantec Phishing Readiness. Email templates are built from insights gained through Symantec's DeepSight™ Intelligence, which allow organizations to test employee susceptibility to attacks relevant to various industry verticals. Companies can go one step further and encourage their staff to report spear-phishing activities to IT teams, allowing security teams to do the proper forensics and validate whether a threat exists.

Every employee is responsible

Keeping cybersecurity best practices alive as employees go about their daily routine strengthens the security culture of an organization. Symantec Security Awareness Service addresses the challenges employees face and provides practical solutions with engaging and easily digestible content developed for specific roles, keeping training relevant and immediately applicable. Address problems such as "Creating and Remembering Strong Passwords" and "Working Safely Remotely", while meeting potential compliance and HR requirements.

Comprehensive and integrated solutions for success

A successful cybersecurity program requires a comprehensive strategy and integration across technology and people. Each offering in Symantec's Cyber Security Services portfolio — Managed Security Services for advanced security monitoring; DeepSight™ Intelligence for actionable technical and strategic threat intelligence; Incident Response for fast containment and eradication of a threat; and Cyber Skills Development for strengthening the entire organization's ability to recognize and prevent advanced attacks — is designed to work together and improve the speed and effectiveness of an organization's security program.

1 Greg Aaron, Phishing Activity Trends Report 1st-3rd Quarters 2015, Anti-Phishing Working Group, Dec. 23, 2015.
2 Tara Seals, Spear Phishing Average Cost is $1.6M, Infosecurity Magazine, Feb. 16, 2016.

5/2016 21359232 - BROCHURE OVERVIEW CYBER SECURITY SERVICES

Unmatched Global Security Skills Development Experience

CyberWar Games
- 1500+ participants
- 80+ onsite events delivered in 30+ countries
- Trained 16,500+ users in 60+ countries
- Trained well-known cyber vendors, large financials, and 3-letter agencies

Every employee plays a role in cybersecurity

U.S. companies reported

$40 Billion

in losses from unauthorized use of computers by employees last year.

– Experian Data Breach Industry Forecast

Get more information

Cyber Skills Development:
symantec.com/services/cyber-security-services/cyber-skills-development

Cyber Security Services:
symantec.com/cyber-security-services

About Symantec

Symantec Corporation (NASDAQ: SYMC) is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 19,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2015, it recorded revenues of $6.5 billion.

To learn more go to symantec.com, or connect with Symantec at: go.symantec.com/socialmedia.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA

+1 (650) 527 8000
+1 (800) 721 3934
symantec.com

8/2016 21359232 – BROCHURE OVERVIEW
CYBER SECURITY SERVICES