CLOUD-BASED

Cyber Detection and Response

A white paper to introduce the concept of cloud-based cyber detection and response services, and show how external Service Providers can offer significant benefits in the race to keep cybercriminals from accessing enterprise data

Stratejm

Office: 888.876.0504

Email: info@stratejm.com

Website: www.stratejm.com

About this Whitepaper

Systems and networks are being attacked every day – there is no shortage of cybercriminals who are ready to take advantage of every weakness. Newer technologies such as the Internet of Things, wireless phones, analytics systems and cloud computing make achieving strong security more difficult than ever before.

The do-it-all-yourself prevention-based approach used by many organizations is neither workable nor efficient in the Internet world. New tools and techniques are needed to contain costs while minimizing loss or damage.

One emerging security strategy uses “security as a service” to share the costs, to improve detection quality and to ensure incident responsiveness. For many enterprises, fast detection and rapid response have become just as important as prevention-by-design. Choosing cloud-based managed services for both threat detection and response planning can be very effective, especially when in-house security expertise and tools are either outdated or missing.

This whitepaper introduces the concept of cloud-based cyber detection and response services, and shows how third party service providers can offer significant benefits over an in-house solution.

Contents

Introduction

In an ideal world, cybercrime would be almost non-existent and breaches would not be in the news as often as they are today. Since absolute protection is not achievable in practice, the ability to rapidly detect and react to cybercriminal activities continues to be a basic goal and requirement for most organizations.

In fact, security incidents have never been as visible or dangerous as they are in today's online, consumer-oriented world. Security and privacy failures have led to severe difficulties for many enterprises - theft of information, disruption of operations and destruction of assets can have very significant financial and reputational consequences.

The large number of data breaches is ample evidence that the challenge of security has yet to be met (see the box on this page). Strong security is generally considered to be a critical success factor in the fast-emerging digital enterprise transformation.

A dramatic shift is also taking place in the IT industry itself. Many traditional in-house IT functions are being re-deployed as shared cloud services and are being managed by external service providers. Cloud computing, personal mobile devices, app stores and the many "things" of IoT have brought cyber security out of the technical backrooms and onto the C-suite's and Corporate Board's agendas.

In this whitepaper we look first at a basic cyber security lifecycle**,** then examine critical cyber detection and response services and finally discuss the benefits of cloud-based managed services. Suggestions are offered for adopting Cybersecurity-as-a-Service as a strategy.

The complex challenges of security

For security professionals, security is like a never-ending whack-a-mole game. Intruders pop up everywhere, they are hard to find and they are almost unpredictable. Even "whacking" threats as they appear does not ensure strong protection forever.

Security experts must be innovative and must use the best available tools if they want to keep up with today's cybercriminals, especially when access is both mobile and global and when operating budgets are limited.

IT security for systems of record (back office systems such as accounting) has traditionally been relatively static. The implied strategy was isolationism - keep the systems separate using a walled garden approach. Unfortunately, this doesn't work for newer systems of engagement that are web-scale, public-facing and online 24/7 – these systems have no fixed edges to serve as walls.

More recently, defense-in-depth security has been deployed for greater protection. The system's design includes point-in-time security functions but cannot anticipate every new exploit (or even vulnerabilities such as software bugs).

It is now well-recognized that systems cannot be permanently "immunized" against all possible future threats or exposures. The major challenge then is how rapidly you can detect and respond to security events.

Examples of major breaches:

- 2015: Ashley Madison – more than 25Gb of company data stolen and leaked, including user details.
- 2016: US Internal Revenue Service – the information of more than 700,000 individuals was exposed, including social security numbers and other personal information.
- 2016: Yahoo - 500 million email accounts were hacked in 2014 but the hack was not discovered until 2016 as part of an internal investigation.
- 2016: Dyn – Distributed denial of service attack that involved tens of millions of discrete IP addresses infected with a botnet.

The Breach Level Index indicates that more than 5.3 billion records have been lost or stolen since 2013.

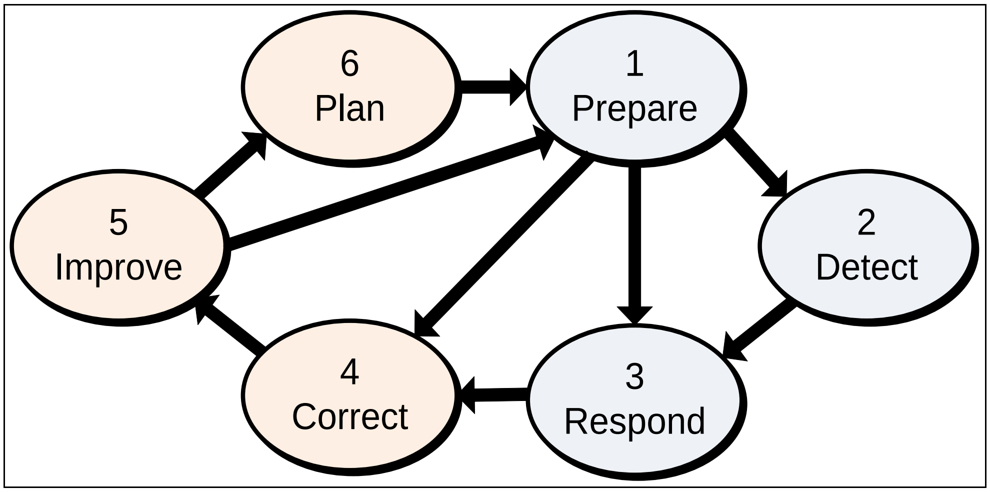

Figure 1: A cyber security lifecycle

A cyber security lifecycle

Cyber security can be described as a six-step lifecycle, as is illustrated in Figure 1. The essence of the lifecycle is the traditional Boy Scout motto - be prepared.

For security, this is not as easy as it sounds!

The security lifecycle can be divided into two parts that correspond to first reacting to an event and then responding to it.

The first three steps aim to stop an attack:

1. ***Prepare your defense*** – Being prepared involves three important activities: tracking your IT assets; identifying vulnerabilities and threats; and collecting relevant industry intelligence to avoid re-inventing the "wheel" for security engineering;
2. ***Detect security events*** – System monitoring combined with a knowledge base and qualified expert analysis is needed for "smart" detection; the process includes collecting relevant data, quickly identifying unusual events and then validating the incidents;
3. ***Respond to stop the incident*** – An effective response will stop an attack and neutralize the intruder as quickly as possible;

The other three steps help to restore normal operations and incorporate the lessons learned:

4. ***Correct the damage*** – Damages resulting from an attack should be assessed, losses identified, data restored and assets repaired;
5. ***Improve knowledge and understanding*** – Learning about cybercriminal motivations and methods should be a continuous process, leading to design improvements and better response preparations;
6. ***Plan improvements*** – Improvements to protection should be based on the lessons learned.

One important concern is where to acquire the expertise to use threat intelligence and to prepare workable responses. For many organizations, there is a shortage of security experts on staff.

Prevention alone is not enough

Prevention alone is now considered to be a failed strategy for most IT environments. The results have been poor at best even though up to 80% of enterprise security budgets are often spent on prevention.

To keep intruders out, the "prevention by design" model relies on techniques such as network segmentation, firewalls and even physical isolation.

This approach has been found lacking for various reasons:

- Security components such as antivirus software, network firewalls, intrusion prevention systems, and access management are increasingly complex to deploy and expensive to integrate and maintain;
- The number of access points is growing exponentially (e.g., IoT sensors, tablets, smartphones, cars, etc.), thereby greatly increasing the threat landscape and the cost of access control;
- Most major breaches are due to insiders having their legitimate elevated access credentials stolen, with data then being exfiltrated without detection;
- Integration of disparate applications is increasing, often including links between organizations, which makes prevention-based tactics even more difficult to deploy;
- Expert personnel who understand the many technologies and vulnerabilities are increasingly scarce; and
- Unfortunately, cybercriminals are more sophisticated and agile than ever before, especially as the stakes get higher and the pace of change increases.

For most organizations, the best overall strategy is to be "more proactive about reacting." This can be achieved by:

- Using industry threat intelligence data to understand what's happening and what's going on before it hits your system;
- Actively monitoring systems and collecting data in real-time as well as historically; and
- Planning in advance to provide rapid, coordinated responses to every incident and all intruders.

Security program models

There are three common, but not mutually exclusive, security operating models:

- ***In-house security support*** – a security centre of excellence takes responsibility for all aspects of planning, organizing, operating and managing the organization's security lifecycle processes;
- ***Managed security services (MSS)*** - a model defined by Gartner as *"*outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services. MSSPs use high-availability security operation centers to provide 24/7 services"; and
- ***Managed detection and response services (MDR)*** – Gartner recently defined a new market sector that they have named "Managed Detection and Response". MDR services "fill that critical security skills gap by providing expert detection and remediation services to deal with today's increasingly complex threats. Private businesses and public companies will find it challenging to deal with these threats alone."

As long as systems and networks have vulnerabilities and cybercriminals remain innovative, no single approach will be enough and security will continue to be a never-ending story.

Cyber detection and response services

The SANS Institute 2016 Incident Response Survey indicated that:

> "Of the 591 respondents to qualify and take the 2016 SANS Incident Response Survey, approximately 21% cited their time to detection, or "dwell time," as two to seven days, while 40% indicated they could detect an incident in less than one day. Conversely, 2% of organizations reported their average dwell time as greater than one year. Survey participants reported that 29% of remediation

events occur within two to seven days, while only 33% occur in less than one day."

These kinds of delay have become unacceptable with the speed of business these days.

A new goal for security managers is to track security performance using service metrics, especially when a Service Level Agreement with an external provider is involved. Two of the important security service metrics are:

Mean Time to Detect (MTTD):
The time between occurrence of a breach and its detection; and
Mean Time to Remediate (MTTR):
The time between breach detection and breach neutralization and repair.

This moves the focus from prevention-by-design to fostering excellence in event anticipation, industry awareness, rapid detection and fast response. This also requires larger investments in advanced cyber security capabilities such as data aggregation, analytics, data science, machine learning and threat intelligence sharing.

Both the customer and the provider have roles to play in achieving excellence in security management. However, the customer is ultimately accountable for results, with the providers supplying expertise, tools and best practices.

Figure 2 illustrates the key functional elements of a Cyber Detection and Response model.

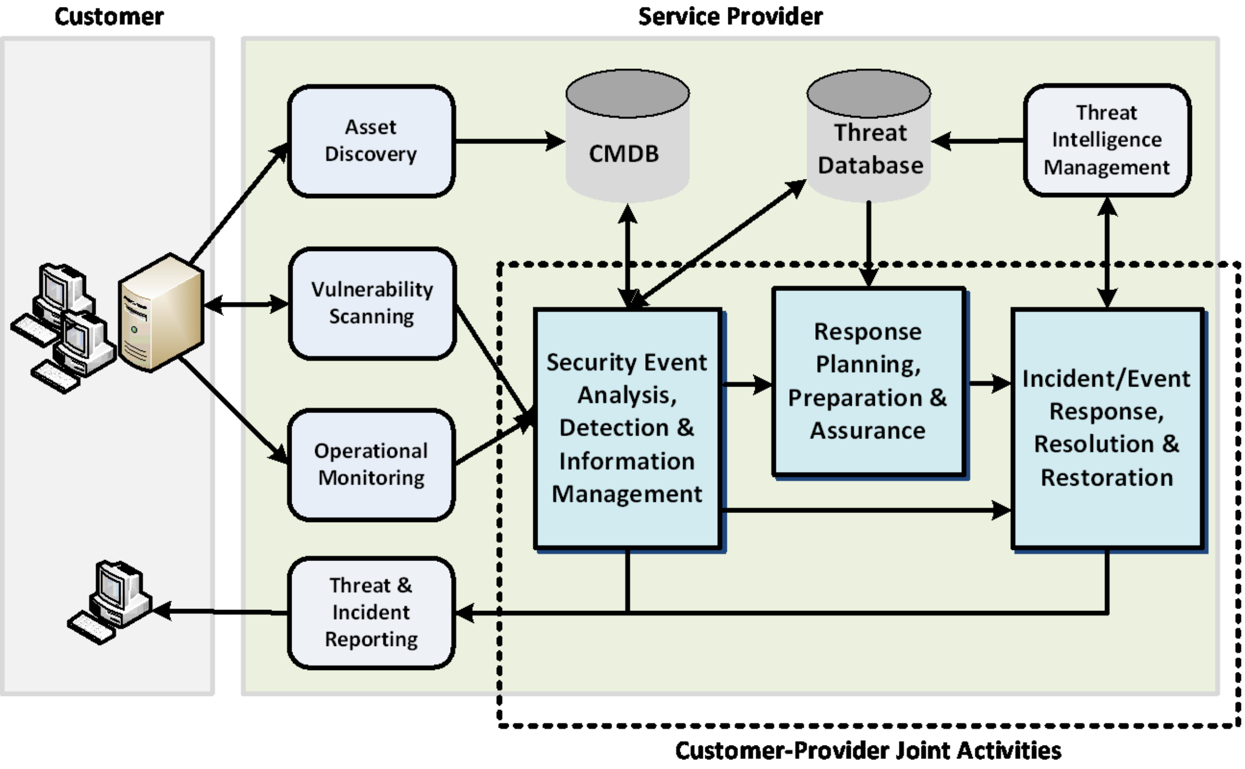
Customer
Service Provider
Asset Discovery
CMDB
Threat Database
Threat Intelligence Management
Vulnerability Scanning
Operational Monitoring
Security Event Analysis, Detection & Information Management
Response Planning, Preparation & Assurance
Incident/Event Response, Resolution & Restoration
Threat & Incident Reporting
Customer-Provider Joint Activities

Figure 2: Cyber Detection and Response - functional components

Functions that are typically included in a Cyber Detection and Response service include:

1. ***Asset discovery and data collection***

   Knowing what assets need to be secured and their vulnerabilities is an important first step in any security program. A customer CMDB is a good starting point if it is up-to-date; otherwise an asset discovery process would need to be invoked.

   IT assets include the physical and virtual resources at all levels of the IT stack, from physical wiring to applications and data objects. Existing protection data (e.g., backup, replication and disaster recovery data) can be used as part of an asset scan. Details about configurations, operations, owners, relationships and known vulnerabilities are all extremely useful for smart security.

2. ***Vulnerability scanning and evaluation***

   Security readiness can be improved through an ongoing process to identify and track vulnerabilities. Since many IT components are used widely, vulnerability data can be shared among organizations. Two broad categories of vulnerability are:

   - ***Known issues*** for which a solution is available, such as unpatched software or older devices;
   - ***Inherent weaknesses*** that can be exploited, such as unencrypted links or weak authentication practices.

   Knowing your system's vulnerabilities is key to being prepared for attack. It also allows scarce resources to focus on where they would be most useful.

3. ***Threat intelligence***

   It's difficult to prepare for attacks when you don't know what's coming at you. Other companies' experiences can be invaluable when trying to understand cybercriminals and for preparing your own defenses.

   Threat intelligence data can save a lot of time and energy, especially when a provider can use the information for multiple users.

   There is also a major advantage if the data can be filtered to suit each customer's situation. Examples of external threat intelligence include the reputation (IP - addresses and domains), malware characteristics, attacker tactics, attack details, etc.

4. ***Operational monitoring***

   Monitoring is useful only if it collects data that can generate security alarms and help with response and repair processes. Security data can be extracted from original data (such as raw log messages), from processed data (averages, summaries, etc.) and from correlated data (i.e., from multiple device logs).

   Potential sources for security data include device event logs, performance data and other indicators of compromise (filenames, hashes, IP addresses, hostnames, processes, services, Windows registry entries, etc.).

   Security monitoring can be implemented by the customer, a managed service provider, or both using:

   - Monitoring appliances on the network;
   - Integration with IT Service Management systems; and
   - Data extracted from applications and filestores.

5. ***Security analysis, detection and information management***

   A lot of configuration and security data can be collected from historical records but may also be needed on a realtime or near realtime basis.

   Modern "big data" analytics and business intelligence techniques can be applied to security event analysis. Smart detection services should be situational and context-aware, with quick response whenever incidents are detected.

A security event analysis combines intended configurations, discovered configurations, directory data and threat intelligence to generate alerts, notifications and reports. Although there should be no limits on the amount of data that can be ingested and processed, good information management practices need to be used. This would include purging, archiving and summarizing historical data over time.

6. ***Security response preparation and execution***

Rapid detection provides little or no advantage if an effective response and recovery capability is not in place. A well-defined incident response process ensures that the enterprise is well-prepared to handle incidents efficiently and effectively.

The essence of an excellent security response is to:

- Anticipate incidents and prepare a response plan before an incident occurs;
- Contain the problem by isolating the attacker and by quickly determining the extent of the damage;
- Remove the active elements so that no further damage can be done; and
- Restore normal operations by recovering data and software or replacing damaged components.

Comparison to in-house security

Security is a necessary cost for almost anyone who uses a computer, but it is especially important for organizations that allow direct customer access or use third party services. Actual costs will vary considerably – from as little as the cost of antivirus software to the complexity of a full enterprise-wide defense-in-depth implementation. Security expenses may also include significant staffing costs.

One option for cost control is to use managed security services. The managed "Cyber Security-as-a-Service" approach uses cloud-based systems that share common functions to reduce the overall cost.

The chart on Page 9 examines the differences in the costs of in-house security versus a Cyber Detection and Response service.

Actual savings achieved will, of course, depend on many other factors including your purchasing power, your location and the availability of suitable services.

Steps you can take now

Marc Andreesen's statement in 2011 that "software is eating the world" was certainly correct. Today's applications for the IoT embed software in almost every physical object, from street lights to shoes to animals (e.g., cows with fitness bands).

There will be no shortage of things that need to be secure. Cisco estimates 50 billion Internet endpoints by 2020. All it takes is one unsecured endpoint or one unsuspecting person to potentially compromise an entire IoT ecosystem.

Unfortunately, software defects often lead to vulnerabilities, as is demonstrated by Microsoft's Patch Tuesday. Unintended functionality, poor design, incorrect implementation, and a lack of regular maintenance are just a few of the security-related software concerns. A security breach, much like a physical disaster, can lead to severe business continuity problems.

Considering all the complexities, a managed service approach may be the best fit for your security policies, budgets and systems requirements. The first question, of course, is how do you get started.

Cost Component	Description	Cost Element	
		In-house security organization	Cyber Detection and Response Service
Asset discovery	A process to discover, catalogue and track hardware, software and data assets that need to be secure	Significant investment in management systems and possibly agent software; expertise in security operations and management is required	Discovery system will already be implemented; may use appliances on the customer site; expertise shareable by customers
CMDB database	A database that captures information about IT assets, characteristics and relationships	May be combined with management systems if available	Could use customer systems as data source; may also be deployed in multi-tenant services
Threat Intelligence database	A collection of data from external sources with correlation to internal assets	Interfaces and external subscriptions required; expertise needed to use the data	Standard on-demand system shared by providers; expertise to use data would be shared by multiple customers
Vulnerability scanning and analysis	Periodic testing for weaknesses and evaluation of potential exposures	Expertise and tools must be acquired	Standard on-demand system and support expertise
Security monitoring and analysis	Monitoring must be available 24/7/365 and evidence analyzed to validate security status	Dedicated expert(s) and systems required to evaluate and react to alarms	Intelligent SIEM systems can be made available; experts would always be available to all customers
Alerting/Reporting	Portals and interfaces to the customer to display events and status	Custom in-house interfaces may be required	Standard interfaces are available as required
Incident response management (planning, execution, recovery)	Process for managing responses to incidents and attacks	Internal ITSM processes would apply; expertise required for planning and execution	Pre-defined processes and shared experts would be available

Five steps that will help you establish a Cyber Security-as-a-Service solution are:

Step 1: Document your GRC (governance, risk, and compliance) policies and practices. Identify any constraints that might preclude a managed service (including public cloud policies and any data storage restrictions).

Step 2: Identify any existing asset catalogues and databases – you must have some records. If these are incomplete or outdated, you will need an asset discovery service.

Step 3: Consider doing a test of Cyber Detection and Response services to evaluate provider processes and current vendor relationships. Your provider may have a free trial and should offer services on a subscription basis with little or no capital funding for equipment or software.

Step 4: Select a suitable partner to provide the security services and develop a Service Level Agreement that meets your specific needs. This will include role statements, service descriptions, quality specifications, and possibly performance penalties. Remember, however, that you are ultimately accountable for security so make sure your vendor management processes are well-defined and managed.

Step 5: Begin planning for providing access to your in-house data sources and/or providing interfaces to your operational monitoring and detection systems. There will be many stakeholders involved in this!

Finally, as a general guideline, don't try to do everything on your own! The security battle is best fought by collaborating with other organizations and by sharing your knowledge and experience, not by attempting to work in isolation.

About the author

Don Sheppard P.Eng. is a Senior Consultant with ConCon Management Services of Toronto, Ontario. He has been a consultant and advisor to IT managers for more than thirty years. Don has participated in the development of various ISO standards including the OSI Security Architecture and, more recently, the Cloud Computing Reference Architecture. Don developed service descriptions and facilitated threat risk analyses for a large government project. Don is also an active blogger for IT World Canada.

About Stratejm Inc.

Stratejm has developed Canada's first cloud-based Cyber Security-as-a-Service offering, enabling enterprise customers to solve security problems in a secure, intuitive and cost-effective manner. Time-to-value is optimized and the enterprise is under no obligation to purchase new hardware or software. Stratejm's security platform is backed by a state-of-the-art Threat Intelligence Centre that is staffed by security professionals. Call 1-888-876-0504 or email to info@stratejm.com for further information.