esentire®

We've Been Breached– Now What?

Rapidly Mitigate Attacks and Minimize Business Risk with Embedded Cybersecurity Incident Response

An eSentire White Paper

www.esentire.com | @esentire | sales@esentire.com

Table of Contents

Executive Summary

Most of the cybersecurity industry focuses on attack prevention. While this is hugely important, every threat cannot be prevented, and if your company has been breached prevention is no longer of any value.

When a cyber attack unfolds, you need to stop it, limit the damage, and restore normal business operations as fast as possible. Doing this quickly and confidently requires specialized expertise. Unfortunately, it's not easy to find practical, cost effective help for mitigating a successful cyber attack. Mitigation services exist, but they are often geared to large enterprises and can be extremely expensive for midsize companies.

There are plenty of "cyber attack checklists" available, and most of them offer the same advice, which centers on setting up plans and procedures that can be followed when an attack happens. While checklists are helpful, more is needed.

This white paper introduces the concept of Embedded Cybersecurity Incident Response (CSIR). As part of an Active Threat Protection framework, this mitigation approach is the quickest and surest way to minimize cyber attack damage and re-secure operational systems.

Embedded CSIR augments advanced preparation checklists by directly addressing the three key elements that come into play as a cyber attack spreads:

1. Bringing resources to bear upon the crisis
2. Obtaining the precise information required for remediation
3. Maximizing the speed of incident resolution

In times of war, embedded journalists are attached to military units, where they are presumably able to provide more accurate first-hand reports.

Embedded CSIR is based on a similar notion – that the best way to fight a cyber attack is with specialized resources that have already been operating in "embedded mode" within a company's IT group. This approach is far less expensive yet more effective than calling in high profile security experts (who know little about your company) after a crisis has already erupted.

With Embedded CSIR, cyber attacks are understood more quickly and remediated faster than is possible with a non-embedded approach.

This white paper concentrates primarily on the technology issues of eradicating the cyber threat, repairing infected systems, and restoring operations to normal. Business-side issues are equally important, but are beyond the scope of this paper.

The Incident Response Challenge

Two companies of the same size and operating with similar IT resources can have identical advance cyber attack preparation checklists. Yet, when faced with the same breach condition, one is only starting remediation efforts while the other has resolved the incident. One minimizes economic loss while the other remains exposed.

What makes the difference? One company has implemented an Active Threat Protection™ framework, which includes Embedded CSIR, while the other company is relying on a traditional remediation approach.

Cyber attack response plans are crucial, and in our scenario both companies have one. A lot of up-front thinking and documentation is needed to create a thorough response plan, but the payoff comes from having a roadmap to follow when a cyber attack erupts inside the network. Most checklists outline very similar steps, which go something like this:

- Identify your response team
- Prepare mitigation plans for different cyber attack categories
- Determine internal and external communication procedures
- Assemble the tools and resources needed to deal with the attack
- Implement remediation procedures
- Evaluate results and improve cyber defenses accordingly

These are excellent guideposts, but a company can compile a very good plan without having an optimized incident response process.

The three key areas to optimize are resources, information, and speed. To understand the challenges, let's look at a typical cyber attack response scenario.

Figure 1: Stages of Cyber Attack Response

Cybersecurity authorities agree that specialized assistance is needed to successfully handle a serious cyber attack. Very large enterprises have in-house experts, but most mid-size companies don't, and often they do not have pre-arrangements with a managed security services provider (MSSP) that includes the provision of expert help in the event of an attack. So they follow the traditional steps shown in Figure 1.

Call for help

It usually takes some time before the IT staff recognizes that the cyber attack is one they do not have the expertise to combat. During that time, various solutions are attempted but to no avail. When it is apparent that help is needed, a security services provider is called in.

Before work commences, agreements have to be signed. Of course this is the point of least leverage for the victimized company, and often the cost of expert remediation services is very high, but our focus at this stage is on time, not cost.

Analyze

Analysis doesn't start immediately. Security services providers who do remediation work require their preferred infrastructure tools for analysis and mitigation. Often, hardware has to be shipped and installed, and only then can in-depth incident analysis begin.

The hired experts must first familiarize themselves with the company's network and application infrastructure. After that, research typically relies upon aggregated log data that the victimized company hopefully has. Time required for understanding the source, nature, and scope of the attack depends to a large degree on the quality of available data.

Remediate

When the threat has been thoroughly analyzed, a remediation plan can be implemented and eventually the systems will be restored to an operational state.

Limitations

This traditional scenario reveals troubling problem areas that interlock with each other. First, precious time is required for all of these activities, which are done sequentially. During this time, the cyber attack can continue to spread – unless operational systems have been shut down – but in that case the business itself is held hostage and losing money as the clock ticks.

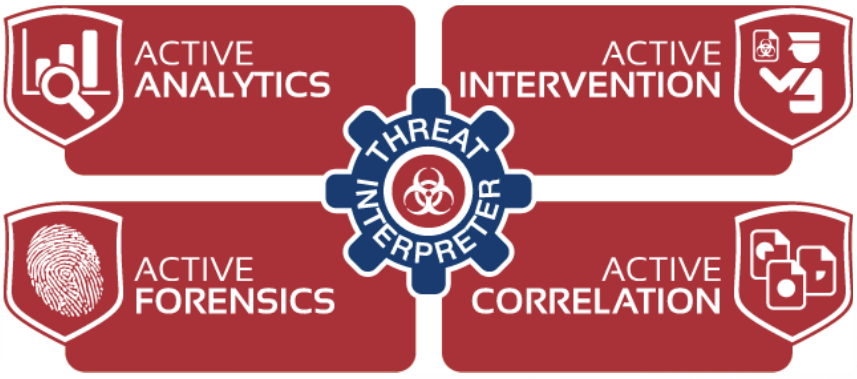
In many industries, the ability to transact business depends upon online system availability. The longer remediation takes, the greater the impact to the bottom line.

A second challenge is getting good information. Even experts are limited by the quality of information available to them. Too often the cyber trail has gone cold because little actionable information is present.

A third challenge is the security analysts' understanding of the victimized company. A certain amount of the money being paid for remediation is actually being used to get the experts up to speed on the company's network and internal systems.

Embedded CSIR and Active Threat Protection

Embedded CSIR is based on Active Threat Protection principles. It is integral to an Active Threat Protection platform such as eSentire's Network Interceptor™, which we will use for purposes of illustration in this white paper.



A key Active Threat Protection concept is that security automation by itself doesn't solve security problems; security analysts are always needed. With a solution such as Network Interceptor, these experts are "embedded" and continuously involved with the client company, not just when an attack happens.

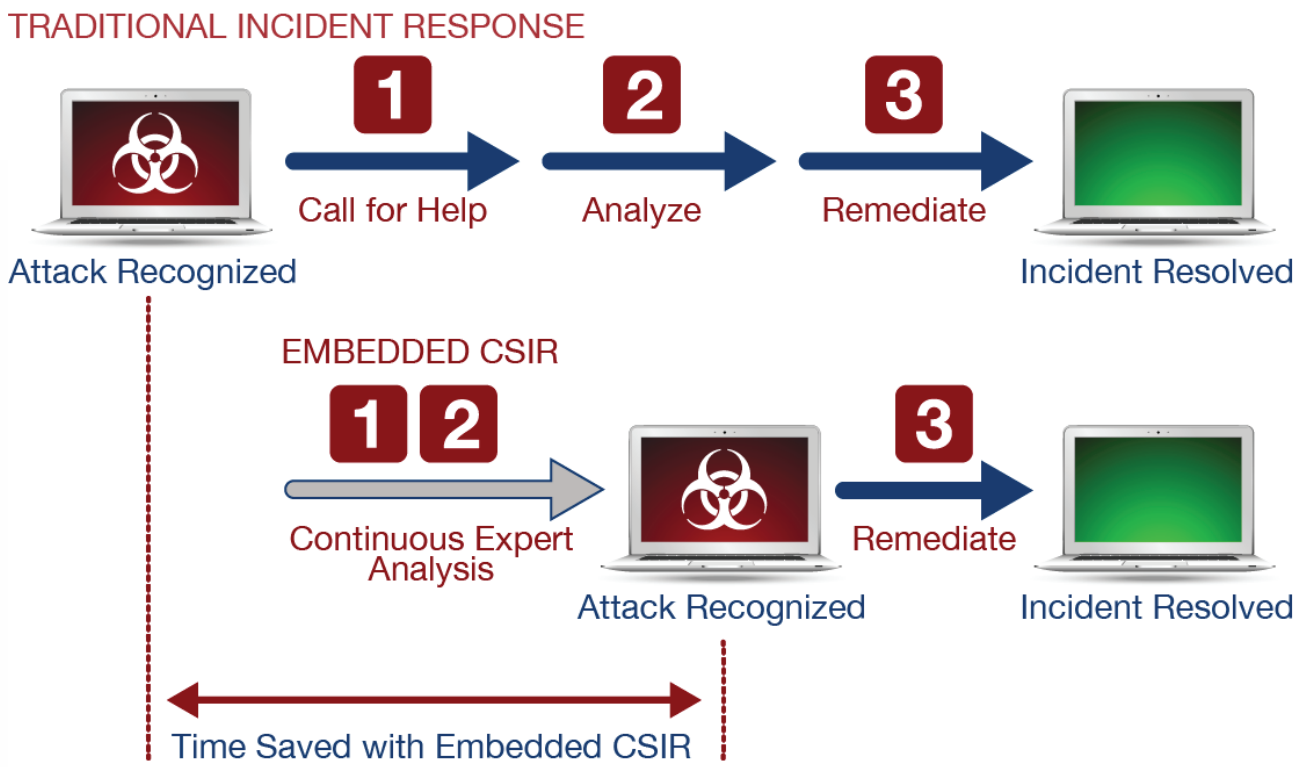
Cyber attacks are inevitable. While Network Interceptor prevents most attacks, it isn't a prevention-only solution. It has specific capabilities designed for those times when a cyber attack has succeeded in breaching a client's network.

It's an important philosophical point. Solutions that solely focus on prevention offer no help when prevention has failed. Active Threat Protection recognizes this, and delivers seamless tools and services such as Embedded CSIR that speed the remediation process.

How Embedded CSIR Works

The primary objective of Embedded CSIR is collapsing the time it takes to remediate a cyber attack. Figure 2 shows how this is accomplished.

Figure 2: Collapsing Remediation Time with Embedded CSIR



With Embedded CSIR, there is no call for help. Security analysts are already there, continuously keeping watch over the client's network. They utilize Active Analytics data and Active Forensics tools to examine any event that indicates a potential threat.

True attacks are recognized sooner, before they have time to proliferate. Remediation time is greatly shortened because there is no hardware to ship to the client site (it's already there), and no read-in time needed for the security experts (they already have intimate understanding of the client network and application infrastructure).

In effect, phases 1 and 2 are being done continuously, before an attack is detected. Remediation is accelerated because the client wastes no time in attempts to resolve the attack without expert help. With Embedded CSIR, experts – who are already working on remediation by the time the client is notified – discover the attack.

Keys to Making Embedded CSIR Successful

Simply having access to cybersecurity expertise doesn't mean you have an effective Embedded CSIR program. Many organizations quickly bring in security experts during a crisis, but they end up wasting time and money while the business is paralyzed – because the threat remains unmitigated for too long. Companies that succeed with Embedded CSIR get incredibly fast incident remediation because they take three crucial steps:

Move to Active Threat Protection

Legacy MSSPs provide security analysis and event notifications, but they do not provide incident response as an "embedded" aspect of their services. It is either unavailable or provided as an extra-cost service in the event of an attack.

Active Threat Protection is a more comprehensive approach, combining technology and services that address the entire spectrum of cybersecurity – from monitoring and analysis all the way through to final remediation of any attack that the company suffers.

Embedded CSIR is integral to Active Threat Protection. It is seamless with regular monitoring, analysis, and alerting services. The same experts who will help remediate an attack are already embedded into daily security surveillance operations and are familiar with the company's network, applications, and business traffic profile.

Establish active analytics capabilities

Most MSSPs and automated security products rely on aggregated data obtained from system and device logs. While extremely valuable, this data is "after the fact" information and there is always a critical time gap after events happen but before their log data can be aggregated.

Active Analytics refers to technology that is deployed on the network wire, which enables real-time event monitoring. It also has the ability to detect suspicious behaviors, which means it can identify previously unknown, zero-day threats.

Active Analytics reduces the time between the commencement of an attack and its recognition, enabling experts to get involved more quickly, before log-based security tools are even aware that an incident has occurred.

Deploy active forensics tools

The speed with which security experts uncover the source, nature, and scope of a cyber attack – and then go on to remediate it – directly depends on the information and analytical tools they have at their disposal.

Active Forensics is a "big data" resource of network events and a toolset designed for expert security analysts. Some of its features are:

Active forensics database

A repository of network event data that is a broader and richer source of valuable information for security systems and analysts. It is a key resource that integrates and extends the capabilities of traditional security systems, but more importantly it arms security analysts with better data – which in turn leads to more accurate diagnosis of cyber attack details.

Intelligent threat interpreter

This dashboard-based facility applies software algorithms to the Active Forensics Database, eliminating false positives and highlighting events that truly need attention. This enables security analysts to concentrate on the real threats instead of wasting time on events that turn out to be benign.

Network event traceability

This advanced tool is like having a record/rewind button on the network: a series of related events can be traced back to their origins to reveal actionable information that is otherwise unobtainable. It enables analysts to quickly pinpoint the source of a cyber attack. Without it, even highly capable experts take much longer to diagnose the cyber attack's cause.

Companies that take these steps optimize Embedded CSIR. Because it is a seamless aspect of an Active Threat Protection service that is already in place, and is enabled by Active Analytics and Active Forensics, cyber attacks are detected sooner and mitigated more quickly than with other approaches.

Embedded CSIR and Advanced Preparation

Embedded CSIR doesn't eliminate the need for advanced cyber attack preparation, but it does make response plans easier to implement in practice.

When initially working with Network Interceptor clients who want Embedded CSIR services, eSentire facilitates development of a cyber attack preparation plan, complete with prearranged policies for response actions in the event of specific attack scenarios. For example, we document different actions for a malware intrusion versus a suspected insider compromise.

eSentire also helps form a readiness baseline with its Enterprise Vulnerability Assessment, and in the event of any cyber attack client systems are not considered restored until an assessment confirms that the threat has truly been neutralized.

One might think that Embedded CSIR would be expensive, due to dedicated security analysts being involved even before an attack commences. But in reality, Embedded CSIR is very cost effective and certainly far less expensive than the alternative.

In short, there is nothing wrong with traditional cyber attack preparation activities and checklists – in fact, they are vitally needed. Embedded CSIR complements advanced planning by optimizing detection and accelerating remediation of cyber attacks.

Conclusion

When under attack, you are at cyber war. You need three key assets to win the battle: resources you can count on, solid information about what you're up against, and speed of action.

Experts agree: there is no way to prevent every cyber attack. All enterprises need tools and resources that will help them to minimize cyber attack damage and return as soon as possible to normal business operations.

Many cyber security companies will help you try to prevent an attack; not many will help you remediate one that succeeds.

Embedded CSIR delivers these capabilities. Surprisingly cost effective, it is the next generation approach to attack mitigation that midsize companies need.

About eSentire

eSentire® is a leader in continuous advanced threat protection solutions and managed cybersecurity services. The company's flagship offering, Active Threat Protection™, challenges legacy security approaches, combining behavior-based analytics, immediate mitigation and actionable intelligence on a 24x7x365 basis. Dedicated security experts continuously monitor customer networks to detect and block cyberattacks in real-time. Protecting more than $2.5 trillion in Assets under Management (AuM), eSentire is the trusted choice for security decision-makers in financial services, healthcare, mining, energy, engineering and construction, legal services, and technology companies. In late 2013, eSentire was named to the Deloitte Technology Fast 50 Companies to Watch and cited as a Canadian Innovation Exchange CIX Top 20 most innovative Canadian company.
For more information visit **www.esentire.com** and follow **@esentire**.

eSentire is named a Gartner 2015 Cool Vendor for Cloud Security Services in the 2015 Cool Vendors report by Gartner Inc.