Practice Area
briefings

sponsored content graciously presented by AccessData Group

Who is Guarding Your Digital Back Door?

Dropping the 'hammer' on security threats with Rapid Detection and Resolution

The Changing of the Old Guard

The question is no longer if your network has been breached, but the number of times you have been unknowingly breached and the extent of the damage already done. It is no big secret that cybersecurity threats have evolved dramatically over the past few years. As a result of this evolution it is imperative that an organization be able to establish in real-time if a threat is part of a disruptive-attack or a cyber-crime. Today's generation of 'black-hat' hackers (cyber-criminals) are technically sophisticated, stealthy, and laser-focused on maximizing their financial gains by exploiting an organization's weaknesses. And with today's news outlets willing to publicly shame an organization at just the hint of a possible breach, a reputation can be irreparably damaged in minutes. With many breaches (data thefts) literally going unnoticed until a customer's personal information or credit/debit card numbers are found already for sale on the Internet black market — businesses are now realizing that older, manual, less informed approaches of dealing with breaches are no longer tolerable.

Several recent high-profile cyber-crimes illustrate the devastating impact modern threats can have on businesses. Target Corporation is perhaps the most recent well-known example of a "for profit" breach that was skillfully planned and executed. Experts hypothesize that the responsible malware was likely inserted in Target's network months before the actual event, and was tactically triggered at a time when it could intercept and steal the most customer data possible. There are numerous other examples.

The Organizational Response

There are some very important steps that an organization has to be able to take when a breach has occurred. These activities are intended to halt the damage, provide accurate details about what has been compromised and what data is at risk. These activities on their own do not improve the overall security posture. The steps are driven out of a need to 1) know the extent of the intrusion and 2) stop or mitigate it. This allows management to make public statements that accurately reflect what has occurred with some assessment of overall impact. This may sound simple, but during real events, most organizations are not able to respond in a timely or accurate manner.

A large part of the reason why the organizational response is often delayed or inaccurate is that a valid assessment requires many diverse tools and groups to work together effectively. Typically, these response teams include IT, legal, compliance, audit, management, and outside

Don't just respond to cyber threats.
Eradicate them with **ResolutionOne**™.

In an era of continuous compromise, prevention alone isn't good enough. Today's omnipresent threats require Continuous, Automated Incident Resolution (**CAIR**™) to detect compromises, cyber attacks and the advanced persistent threat (APT) as they happen, resolving them through integrated threat intelligence, forensics and automated IR. **ResolutionOne**: the first CAIR platform that truly eradicates cyber threats.

AccessData®

Learn more at
www.accessdata.com/resolution

counsel. There may be others depending on the specific situation. This ad hoc response group is often plagued by a number of issues that limit the ability to respond quickly to the security event, such as:

- Different language and terminology
- Lack of a consistent set of information to inform all parties
- Diverse informational needs
- Alert "Fatigue"

In order to maximize the ability to work as a team, and to identify the actual status of the breach, it is essential to have tools and reporting solutions that work across these disciplines. These security event and response tools must have broad coverage, but also the depth to truly ascertain the impact of the breach.

A second and highly important element of moving forward effectively during an event is the need to work quickly. Moving fast requires automation in order to successfully deliver critical information. One of the key aspects of an automated solution is integration with existing security investments to provide context which equates to control of an event. The need for automation extends to the use of threat intelligence information (commercial & open sources, internally generated) to best understand the details of the hack.

The Solution

AccessData Group, Inc. has developed an enhanced solution to transform organization practices from *response* to true *resolution*. The ResolutionOne™ platform enables organizations to understand more quickly — and with greater certainty — what is truly occurring when there has been a breach. ResolutionOne is the first platform to provide Continuous Automated Incident Resolution (CAIR™) that delivers the information and capabilities that are required to detect, analyze, and resolve any security event.

Continuous Automated Incident Resolution (CAIR) Overview

CAIR is a new class of technology platform that is designed to improve organizational response to security events. CAIR comprises the tools to enhance collaboration between multiple organizational groups, and then prioritize an automate many of the traditional IR steps required by kill chain best practices.

CAIR's benefits align with the organizational needs that occur during an event. The most important are:

- **Faster resolution to security events** — Shortening the response time to an event minimizes the potential damage from a breach CAIR provides actionable intelligence and enterprise level visibility in minutes
- **Holistic and integrated security solution** — Many organizations are challenged with multiple point products and a lack of integration when responding to security events. This leads to security alert and analyst fatigue which ultimately increases risk and costs the organization money
- **Reduced communication complexity and overhead** — Information is delivered to all parties. Consistent information is the key to fast, confident event management. The sooner an organization knows exactly what transpired, the sooner public and board level commentary can be made and public confidence restored

As organizations grapple with more frequent and increasingly serious security events, an automated and integrated response process is essential. This new approach stands in stark contrast to the current process for identifying and resolving breaches, which is often dependent on manual tasks, has inconsistent information flows, and is not designed to facilitate real-time collaboration. Reacting to events as they occur is no longer an effective approach to information security.

ResolutionOne Overview

ResolutionOne delivers an integrated platform that enables different security teams to automate many of incident response practices within a unified platform. This enhances real-time collaboration and allows analysts to focus on the threats with the greatest potential risk which leads to an overall reduction in time to resolution for ALL SECURITY EVENTS. ResolutionOne succeeds in delivering these benefits through:

- Cohesive endpoint and network threat analysis for a more complete picture of the actual breach
- Coverage across the enterprise including mobile endpoints providing event playback
- Ability to isolate/remediate compromised endpoints in seconds
- Enhanced use of existing security tools
- Numerous other features to support organizational protection, investigation, and response for cybersecurity issues

The process for resolving an event starts with identification of a threat. ResolutionOne integrates with and enhances a number of real-time security monitoring solutions including FireEye®, HP's ArcSight® and McAfee's NitroSecurity®. ResolutionOne takes these alerting technologies one step further, by reducing the volume with context based prioritization and secondary threat scoring.

AccessData's ThreatBridge™ threat analysis engine is a core component of ResolutionOne and the market's first agnostic library for threat intelligence. ThreatBridge aggregates and normalizes threat intelligence from commercial, open source and internally generated IOCs. Then it prioritizes the threat information while indicating real (or valid) alerts amongst the hundreds or thousands of alerts that might have otherwise been ignored. Once a threat is validated using ThreatBridge, the ResolutionOne platform can automatically remediate and isolate the compromised systems. Because the ThreatBridge analysis engine examines both network and endpoint activity, organizations can immediately determine the scope and breadth of an attack. This unique and holistic application of threat intelligence simultaneously fortifies an organizations threat library by automatically appending to the library as new variants are detected. The platform effectively becomes the repository for all of the key threat and security intelligence. The engine supports an organizations' transformation to proactive threat hunters.

As more laws and compliance directives are issued that focus on cybersecurity and the impact of an intrusion, the need to reduce the time and complexity resolving a breach increases. This may be required by law enforcement, compliance bodies, corporate counsel, and other external entities. Further, these capabilities aid general information governance activities of the organization and provide a mechanism of replying to external demands.

Key Benefits of ResolutionOne

ResolutionOne was developed with a focus on the actual cybersecurity landscape in organizations today, and the need to move beyond older, manual and reactive response to security events.

A recent study by the Ponemon Group, a renowned security research firm, details some of the most troubling issues common in organizations today. Key findings that showcase how older response approaches are lacking include:

- 86% of the organizations say that detection takes too long
- 85% say that there is little ability to prioritize various incidents, making response difficult to gauge
- 74% mention that there is little if any integration among the many security products that are currently used
- 52% believe that remediation takes too long

This adds up to a process that is not intelligent, facile, and responsive to the organization.

An additional section of the Ponemon study looked at issues that impact incidence response. Again, some of the most important findings were startling. Among them:

- 55% of the respondents do not believe that the internal team has the expertise to effectively investigate and remediate sophisticated attacks
- Only 25% of the respondents are currently using a next-generation security solution, defined as being able to remediate cyber attacks, not only to identify

Given the findings of the Ponemon study, the value of a platform like ResolutionOne, which provides a more comprehensive and capable solution when a security event occurs, is clear.

Summary

The demands placed on an organization's security event response process have increased and expanded dramatically from both internal and external constituents. On top of that the general public, after very public and costly breaches, is now paying much more attention as well. Today, organizations require a security event *resolution* process that can ascertain the facts of the breach quickly and remediate the event.

ResolutionOne provides a new approach to identifying, managing, and resolving to security events. Most important, it meets the demands for faster identification of the threat, quicker remediation, and clarity about the attack's impact on systems and data. Defense driven security is no longer effective or practical. Detection and *resolution* is optimal, proven and necessary. **PAB**