MSOC+

MANAGED SIEM

FROM:

ABAXIO

WHAT IS SIEM ?

The underlying principle of a SIEM system is that relevant data about an enterprise's security is produced in multiple locations and aggregated into a single point of view. Highly efficient searching coupled with automated and manual response facilitates significantly faster response times, and the spotting of trends and patterns that are out of the ordinary. SIEM combines SIM (security information management) and SEM (security event management) functions into one security management system.

A SEM system centralizes the storage and interpretation of logs and allows near real-time analysis which enables security personnel to take defensive actions more quickly. A SIM system collects data into a central repository for trend analysis and provides automated reporting for compliance and centralized reporting. By bringing these two functions together, SIEM systems provide quicker identification, analysis and recovery of security events. SIEM systems also allow compliance managers to confirm they are fulfilling an organization's legal compliance requirements.

A SIEM system collects logs and other security-related documentation for analysis. Most SIEM systems work by deploying multiple collection agents in an hierarchical manner to gather security-related events from end-user devices, servers, network equipment as well as specialized security equipment like firewalls, antivirus and intrusion prevention systems. The collectors forward events to a centralized management console, which performs inspections and flags anomalies.

The final, and critical step which is still not offered by most competing solutions, is the direct and automated communication from the SIEM system back to the firewall(s) providing for a range of automatic and/or manual responses such as automatically blacklisting of the threat-emanating IP address or quarantining the hosting network IP address.

GROWING RELIANCE ON SIEM

Until just a few years ago, because of our assumptions that the cyber criminal was on the outside breaking in, security defense correctly focused on the perimeter – the firewall. To compare the proliferation of spyware (i.e.: the criminal breaks in) vs. phishing (i.e.: the victim "reaches out" to the criminal) in 2010 vs. 2014, see Figure 1 (below):

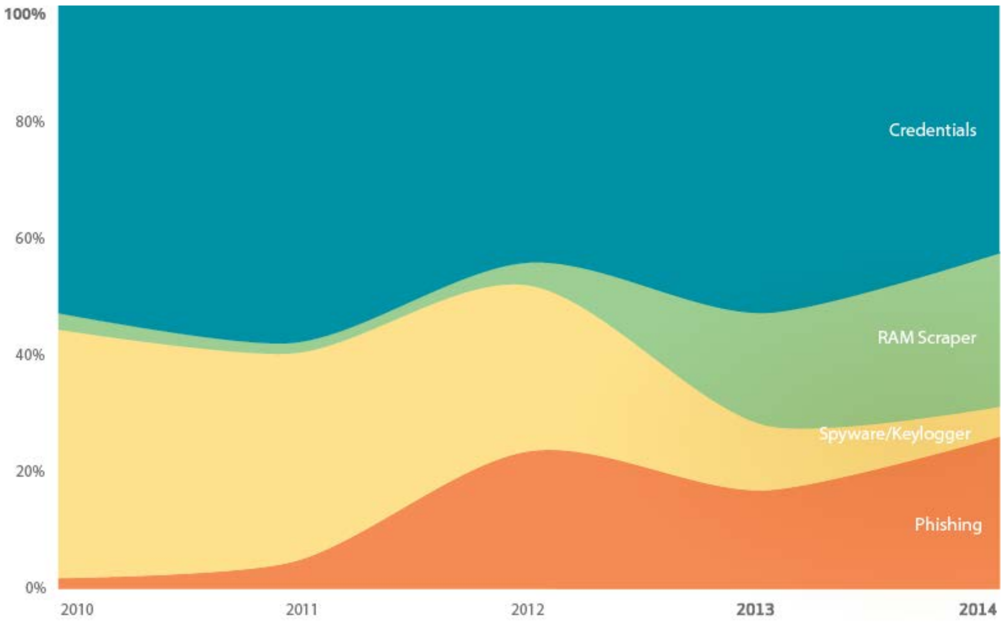

Figure 1. Significant threat actions over time by percent.

Source: Verizon 2015 Data Breach Investigation Report

Especially with the increasing prevalence of phishing schemes, the attack zone has moved away from the firewall and onto the desktop. As such, security experts no longer assume the criminal is breaking in from the outside. As a result, the focus has shifted from a firewall's intrusion prevention to time-to-respond after detection.

To further illustrate this idea, watch a short (15 minute) video recording in which Levi Staal, presenting live to Illinois' Technology Executives Club, neatly summarizes the paradigm.

SIEM'S CRITICAL SUCCESS FACTOR: SPEED

According to the Verizon 2015 Data Breach Investigation Report, "in 60% of cases, attackers are able to compromise an organization within minutes."

Figure 3 highlights one of the primary challenges to the security industry, contrasting how often attackers are able to compromise an organization in days or less (orange line) with how often defenders detect compromises within that same time frame (teal line). Until today, the proportion of breaches discovered within days falls well below that of time to compromise. Even worse, the two lines are diverging over the last decade, indicating a growing "detection deficit" between attackers and defenders.

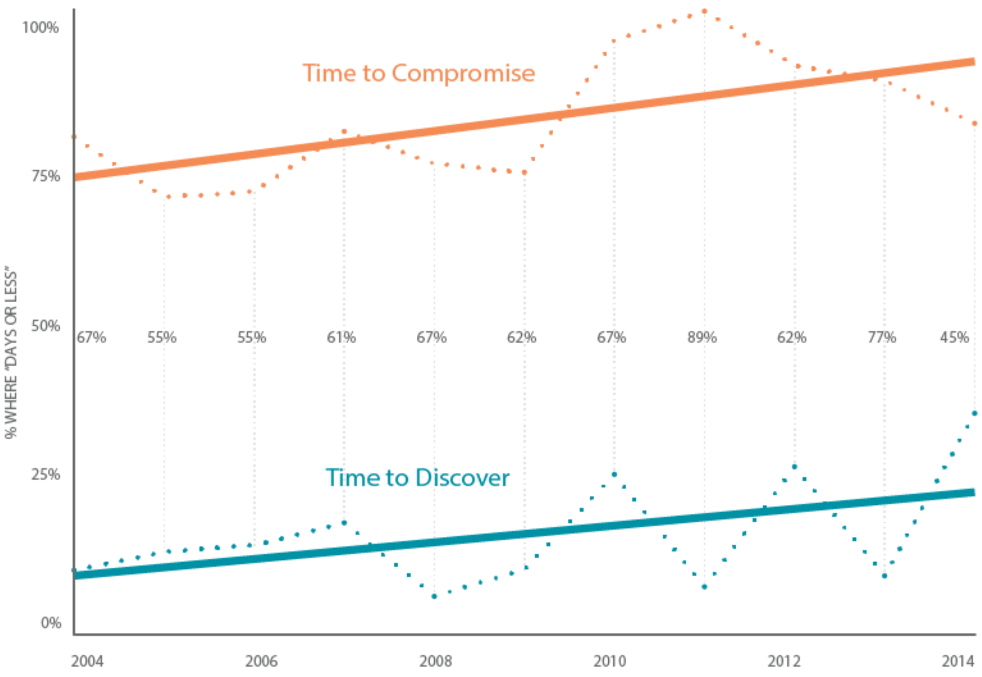

Figure 3.
The Defender-Detection Deficit

Source: Verizon 2015 Data Breach Investigation Report

Some good news: last year boasted the smallest deficit ever recorded and the trend lines appear a bit more parallel than divergent. We'll see if that's a trick or a budding trend for the coming year.

WHY ABAXIO?

MSSPs have an enormous advantage in the near-term analysis. The upfront cost of rolling out a functional Security Operations Center are almost entirely eliminated by the fact that the MSSP's infrastructure and staff are already in place – all the MSSP needs to do is adapt their existing resources to the client's particular needs.

But that's just the beginning. Abaxio has taken SIEM to the next level with MSOC+, its *hosted* **SIEM-as-a-Service.**

MSOC+ is an end-to-end solution using a combination of proprietary and off-the-shelf software and hardware to deliver a *hosted* SIEM solution currently unmatched in terms of price and degree of automated response.

MSOC+ is also *unique* that it is the only hosted SOC service which is backed by up to $500M in coverage by our A+ rated underwriter against a hack, breach or network downtime.

SPEED

Using both standard and proprietary software, Abaxio reduces the time-to-respond of its Security Operations Center (SOC)'s from an average of 30 minutes to less than one minute for 80% of all 'actionable' security events.

This (a) reduces the impact of any potential breach, and (b) reduces our reliance on human intervention, (c) lowers our break-even cost, and (d) increases reliability.

PRICE

Abaxio prices its Managed SIEM service at less than half that of competing services such as Masergy and Onshore.com.

Rhino Security Labs recently published a study analyzing the price differential between in-house vs. managed SIEM. Their bottom line conclusion was as follows:

SECURITY OPERATIONS CENTERS: IN-HOUSE vs. MANAGED SECURITY*

	In-House	MSSP	✓ Abaxio
Upfront Costs**			
One-time MSSP fees		$ 32,000	$ 25,000
Hardware and software one-time purchases	$ 466,000		
Total Capital Expenditure	$ 466,000	$ 32,000	$ 25,000
Operational Cost Breakdown, 3-Year Outlook**			
Annual MSSP fees		$ 525,000	$ 300,000
Incidental MSSP costs		20,000	-
Software License Renewals / Upgrades	255,000		
Vendor / Specialist Contractor Fees	65,000		
Management Costs	295,000		
Training & Certification	34,000		
Asset Depreciation / Replacement	175,000		
SOC Analyst Salaries & Benefits (2x FTE 24x7)	550,000		
Misc. Operating Expenses	8,500		
Total Operational Costs	$1,382,500	$ 545,000	$ 300,000

* Published by Rhino Security Labs 2015

** Figures are averages drawn from actual RFPs generated by Rhino Security Labs.

Common sense might suggest that MSSPs will have a stronger lead in short-term scenarios, while a longer scenario can favor the in-house approach, but unfortunately this is rarely the case in practice. Prevailing conditions in the technology industry in general, and the cybersecurity industry in particular, tend to favor the MSSP approach even over ten-year timescales. Factors such as the rapid evolution of technologies and the ensuing pace of obsolescence, the difficulty of staff retention, talent shortages and the accompanying cost for employers, and the changing nature of cybercrime itself all tend to weight the scales against long term investments in infrastructure.

WINNING ARCHITECTURE

Abaxio's lower price points are a reflection of important advantages of its architecture vs. its competition, including:

- 100% Hardware-less solution (for the client)
- Tighter integration between the firewall and aggregation software using proprietary software
- Abaxio has developed a unique, proprietary training program for our SOC personnel. We have more than 25 fully-credentialed, highly trained security technicians in our off-shore facility on call 24x7.

MEET THE CEO:

Levi is a senior Cyber Security and Risk Management executive with over 20 years of experience in all aspects of security and privacy program architecture, design, management, and operations. His experience spans Financial Services, Government, Healthcare and other industries and includes business continuity, risk management, program planning, application and software security, security assessments and audits, and security operations. He built and leads Abaxio Corp., a global managed security services provider with offices in the United States and Canada, specializing in SIEM as a Service, and Business Continuity. He has been the principal advisor to many Fortune 500 and government clients on cyber security strategy, responsible for securing their critical information assets for e-commerce transactions, sensitive health records, and classified military communications. Levi is a graduate of Boston University's Questrom Graduate School of Business with a Masters Degree in Management Information Systems.

Levi has published several articles on security topics, such as application security, security operations, and secure system design. He is a frequent speaker on effective security techniques at security symposiums, conferences, and CIO forums.

Security Clearance(s): CSIID ("Protected & Classified" Canada Department of Public Works, non-current)

Certifications: Licensed (Cyber Security) Commercial Lines Insurance Producer IL #16990974

Organizations: Founding Member – Chicagoland Chamber of Commerce Cybersecurity Task Force.

Levi was previously CEO of HostGeneral.com, an international, high performance hosting conglomerate consisting of five brands.

In addition to his work with Abaxio, Levi is acting Chief Technology Officer for several Single and Multi- Family Offices (SFO/MFO). Levi is also Managing Partner of Benchmark Cyber Partners, a Chicago-based full service commercial lines insurance agency that partners with Abaxio specializing in Network Security & Privacy Liability ("Cyber") Insurance.

NEXT STEPS:

Let's talk!

For more information about MSOC+, Abaxio's managed SOC services, please contact:

Louis Allan, Vice President Channel Sales
admin@abaxio.com
773-575-6800