Reducing Risk and Accelerating Time to Remediation with Security Analytics

WHITEPAPER

1440Security

Table of Contents

The Role Of Analytics In Security

Cyber attacks are a complex and growing problem with significant financial and legal implications. Executives at the highest levels are under scrutiny about security posture and their response to a breach from stakeholders, regulators and consumers. For some companies – it's a potential matter of survival.

This paper explores emerging cyber security trends, the challenges they present, and how security analytic techniques can help reduce risk. It also discusses how Managed SIEM service providers can help organizations better identify, contain, investigate, and resolve incidents faster.

Cyber attack threat is large and growing

Cyber crime is reaching epidemic proportions as the cost of cyber attacks skyrockets. Juniper Research predicts that cyber crime costs will reach $2.1 trillion globally by 2019.[1] This is an increase of nearly 400% over 2015 costs – which had already quadrupled from 2013 costs. What's worse, some experts estimate that as much as 75% of total global security breaches occur in the United States.[2] According to the Ponemon Institute's 2016 Cost of Data Breach Study, the average total cost that U.S. organizations paid per data breach increased 7% year over year from $6.53 million to $7.01 million. This equates to an average cost of $221 for each U.S. lost or stolen record containing sensitive and confidential information.[3] In 2015, IBM estimated that their customers were attacked an average of 16,856 times a year. This equated to 46 attacks every day — or nearly two attacks every hour. And even though most were not successful, on average, nearly 2 attacks were successful each week.[4]

While most data breaches continue to be caused by criminal and malicious attacks, these breaches also take the most time to detect and contain. As a result, they have the highest cost per record because the longer it takes to detect and contain a data breach the costlier it becomes to resolve.[5]

And this is just the tip of the iceberg. Most cyber crime goes undetected, particularly industrial espionage where access to confidential documents and data is difficult to spot.[6] In fact, some experts estimate that 80% of cyber crimes go unreported globally due to a lack of awareness of the crime, inability to report it, embarrassment on the part of individuals, or fear of consumer backlash on the part of businesses.[7]

Small and medium sized businesses are big targets

Companies of all sizes are at risk from cyber attacks. While large banks, retailers, and federal agencies get lots of negative press when they are hacked, small to medium size business (SMB) are also at risk – perhaps even more so than large companies. In fact, the last five years have shown a steady increase in attacks targeting small businesses with 43% of all reported 2015 cyber attacks worldwide targeting businesses with less than 250 workers.[8] In addition, other studies show that only 20% of SMBs report cyber attacks on their computer networks. Thus, the percentage of small businesses attacked is probably much higher. Given the likelihood of attack coupled with the high average cost per security breach, a single incident could easily put a small company out of business.[9]

Why target SMB companies? Cyber criminals steal business information to do things like take employee and customers' personally identifiable information (PII) and create fake identities which are then used to deplete bank accounts, launder money, and commit insurance fraud. These criminals also steal intellectual property, hijack websites, and use stolen data to attack other businesses. They even ransom critical data, demanding a financial payoff for the return of valuable information.

Cyber criminals target small and medium sized companies because they are easy to hack. Most smaller businesses don't have the technical/financial resources or security expertise to protect themselves against cyber attacks.

Security is a "Must Have" Cost of Doing Business

53
million security events per average company per year[11]

12
new cyber crime victims created per second[12]

80%
of cyber crime is committed by organized crime syndicates[13]

50%
of data breaches caused by malicious or criminal attacks[14]

64%
more security incidents found in 2015 than in 2014[15]

43%
of global cyber attacks target companies with fewer than 250 employees[16]

80%
of small businesses do not have basic cyber attack response plan[17]

They typically lack data encryption capabilities, anti-phishing email protection, security event log analysis and off-site backups of their data and websites. And even though they are a highly-targeted entity, 80% don't have a basic cyber attack response plan.[10] Security is no longer a "nice to have" capability for SMBs, it's a "must have," fundamental cost of doing business.

Attacks are increasingly sophisticated and ever-changing

Per the FBI, cyber intrusions are becoming more commonplace, more dangerous, and more sophisticated. Fraud is no longer just the activity of an occasional hacker. Experts estimate that 80% of fraud schemes are committed by organized crime syndicates.[18] These crime rings view cyber crime as highly profitable, low-risk, and easy means of obtaining millions of dollars in cash. What's more concerning, the technical capabilities, professionalism, and global reach of these criminal entities are now equal to those of many large organizations, even governments.[19]

The growing sophistication of criminal capabilities combined with ubiquitous usage of mobile, cloud and online technologies and the introduction of new, "smart" devices that belong to the Internet of Things (IoT), means security threats will continue to increase and the attack types and vectors will continue to proliferate.[20] As businesses look to offer a wider range of benefits and optimize operational performance, more devices are being created with Wi-Fi capabilities and sensors to relay information over the Internet and communicate with each other and with corporate networks. And many of these devices and capabilities are being created in a security vacuum — something cyber criminals will exploit as more companies and consumers adopt interconnected systems and products. The mobile and IoT threat to corporate networks is significant (e.g. potential theft and malicious use of personally identifiable information, payment card holder data, critical infrastructure, business systems, point of sale devices, etc.). Companies need tools to help them better protect themselves and adapt to ever-changing security threats.[21] [22]

> **55%**
> of companies that experienced a data loss could not identify for certain what data was stolen.
>
> - Ponemon Institute Report

Security Challenges Increase Risk

Businesses today are responsible for managing a large and growing number of systems and devices resulting in an enormous amount of security data which must be analyzed. This data is collected from diverse application logs, network security events, vulnerability management data, host-based anti-malware tools, and endpoint security tools among other things. However, most companies either lack the security expertise or don't have enough IT staff or budget to adequately analyze and act upon all this data. According to the SANS Institute, 30% of companies could not even tell if they had been breached in 2016.[23] Security personnel are overwhelmed and as the number and sophistication of cyber attacks increases, vulnerabilities are missed and companies are exposed.

Lack of security skills impedes threat detection and remediation

The biggest challenge to detecting and remediating security risks is a shortage of security skills.[24] In the US alone, more than 209,000 cyber security jobs were unfilled in 2015, with job postings up 74% over the past five years and demand for positions like information security professionals expected to grow by 53% through 2018.[25] In a recent report from Vanson Bourne, 82% of companies reported a shortage of cyber security skills with one in three saying the shortage makes them prime hacking targets and one in four saying it has led to reputational damage and the loss of proprietary data due to cyber attacks.[26] A lack of available, adequately trained personnel exacerbates the already difficult task of managing cyber security risks. A strong security posture requires a highly skilled security workforce.

Overwhelming amounts of security data from multiple sources make timely identification of threats difficult

In addition to security staffing challenges, today's companies are overwhelmed by the amount (petabytes) and pace (hundreds of thousands of events per second) of security data from logs, network metadata, flow data, events, and alerts.[27] As more cloud and IoT offerings are added, the amount of security information and events captured from devices and systems will increase and worsen an already tenuous situation.

Humans alone cannot manually keep up with the amount of data needing to be assessed. Automated security analytics are needed to help keep pace with the growing volume of data and sophistication of attacks. A recent report from Verizon found that 84% of successful attacks on IT infrastructures compromised their targets within hours and 74% of attacks were not discovered for weeks – and sometimes not for months, even years.[28] Likewise, the Ponemon Institute estimates that the mean time to identify a breach is 256 days, while the mean time to contain it is 82 days.[1] Attacks happen quickly – which is one reason they are so difficult to detect – and why automated security analytics that help filter extraneous noise and provide actionable insights are so important.

Dispersion of attack data across the infrastructure complicates attack detection and prevention

Attack data is often spread across many different network devices, servers, application logs and endpoints.[29] Not only does this make it difficult to analyze a breach in progress, it hinders the ability to assess its impact. In a recent Ponemon Institute report, 55% of companies that experienced a data loss could not identify for certain what data was stolen. Improving the speed of detection and analyzing the impact of an attack are key drivers to adopting security analytics.[30]

Inconsistent data and false findings impact ability to address critical security issues

IT and security personnel need to focus on the highest-level security issues (that present the most risk) yet inconsistent security data and false findings can degrade their ability to do this. Security data comes from a variety of sources in a wide range of formats. It needs to be aggregated and correlated into a unified view or dashboard, then evaluated to weed out false alarms and determine true issues.

While the vast majority of security events can be designated as “noise,” or extremely low priority traffic, companies need automated methods to help them quickly analyze and prioritize security events to determine which events need the most immediate attention.[31] In addition, false findings can waste limited resources and increase the amount of attack damage. For example, false negatives can make a company overlook vulnerabilities, which not only leaves security flaws in place but reduces the likelihood that the company is even aware of the issue. Alternatively, false positives present security issues that do not in fact exist, which can waste valuable time and resources trying to find or fix something that can’t be found.

Fig. 1 - Attack data is often spread across many different network devices, servers, application logs and endpoints.

Security Analytics Dramatically Reduce Risk

Protecting against today's rapidly evolving threat landscape requires broad and deep visibility across your IT environment. Threats arrive from many vectors and evidence of their existence can be found in data from a variety of sources. Security analytics use multiple, layered techniques that enable organizations to better detect, prioritize, respond to and neutralize emergent cyber threats (including more advanced threats) and comply with regulatory requirements. How? By complementing existing security controls and applications while gaining visibility into threats and risks to which organizations are otherwise blind.[32]

Machine analytics automate and broaden security scrutiny to keep pace with threats

Due to the speed of cyber attacks, time is of the essence when evaluating security data. Unfortunately, evaluation time is limited due to the amount of data that needs analysis and the speed at which it is generated. Machine-based analytics help already overwhelmed security personnel keep pace by automatically and continuously reviewing relevant data to look for malicious activity. Using machine learning, these analytic tools can recognize and understand patterns, seasonal trends, and anomalies within the data; learn from each instance what is a normal behavior and where the outliers are to identify potential problems; and then prioritize threats for follow up.[33] [34]

Baseline analysis establishes normal behavior and highlights suspicious deviations

Baselines are used to establish a pattern of normal activity within a monitored environment so that potential threats or deviations from the norm can be more quickly and easily detected. As data moves across an IP network, baselines define things like source and destination computers, length of transmission time, amount of data typically transferred and which applications are involved. Once baselines are established, data is continuously collected and evaluated to refine normal activity parameters and to identify deviations that may indicate potential threats. For example, deviations such as the use of unknown or unauthorized source or destination computers or increases in transfer times or data amounts may indicate an active attack. These deviations could mean that a server has been highjacked and is now participating in a botnet or that sensitive data is being stolen, or other malicious behavior in underway. Alternatively, deviations to an existing baseline may simply indicate a change in normal behavior. The inclusion of a new business partner or the launch of a new service offering could cause previously unknown servers to show up or network traffic flows to change, which would simply require an update to the existing baseline. Unfortunately, cyber criminals are aware of baseline analysis and may slowly increase their activities over long periods of time to avoid detection and trick organizations into accepting anomalous behavior as normal. That's why baseline analysis is just one of many techniques required for a multi-layered approach to security analytics.[35]

Signature analysis and threat data feed matching quickly identify known threats

Strong security requires a combination of ongoing, analytical techniques to identify threats accurately and quickly. One methodology is to compare the security data collected to characteristics of known threats. For example, some threats, such as malware, can have a unique string of bits or a unique binary pattern known as a signature, (think of a fingerprint) that can be used to detect and identify the presence of malicious code. Another thing to look for is known bad behavior, such as attempting to use a default password to log into a system or using commands out of normal sequence during an application session. Sophisticated machine-based analytics can look for these types of signatures and patterns to identify known threats.[36]

Another methodology is to constantly compare threat data feeds (ongoing streams of data related to potential or current threats on worldwide basis) to aggregated log data and search for matches which may indicate a potential issue. Sources of threat data feeds include free indicator feeds, paid feeds, bulletins, internal intelligence gathering and strategic partnerships. (Some organizations in the network security community, including SANS and CERT, make open source threat data feeds freely available.) The data provided in these feeds should use STIX™ (Structured Threat Information eXpression), a structured XML programming language for describing cyber threat information so it can be shared, stored, and analyzed in a consistent manner for seamless integration and faster analysis.[37]

> Strong security analytics require a continuously evolving, multi-layered methodology to keep pace with constantly changing security threats.

Like signatures, these feeds include information on major threat characteristics such as the IP addresses, URLs, and DNS names used by malicious websites engaged in phishing and malware attacks. However, just as with baseline deviations, a threat data feed match doesn't always indicate malicious activity. For example, a match to a malware URL may be caused by multiple systems in a shared virtual hosting environment sharing a single URL where most systems are legitimate and only one system is serving malware. Likewise, a match to a phishing URL could simply indicate an accidental misspelling in a browser or email address bar. Nonetheless, a match does indicate that the activity may be suspect and should be investigated.

Security event correlation reveals hidden relationships and advanced threats

Security event correlation is a machine-based analytical technique for bringing separate but related items across security events (such as authentication, access to services and data, and output from point security tools such as Intrusion Detection Systems (IDS) or antivirus software) together in a meaningful way to identify obscure relationships. By looking for common attributes across disparate events and linking these items together in a more meaningful way, event correlation turns random data points (that alone would not indicate a potential threat), into useful security information to give a more accurate view of what is happening across the organization. Cyber criminals rarely attack only one location. They silently infiltrate and attack multiple systems at multiple times – with each mini compromise helping them make progress towards the final goal. Event correlation analytics can help combine these separate transgressions into a more holistic view to better understand the operational aspects of advanced attacks, help stop these attacks if they are still underway, and determine the extent of damage they may have already caused.

Threat prioritization expedites remediation of high priority targets

The number of security events and alerts generated daily is overwhelming and organizations simply do not have the bandwidth to investigate them all. To enable overworked security resources to weed out extraneous noise and focus on the most critical issues, a potential threat should be prioritized based on its likelihood of success (including the risk the threat poses because of an organization's known vulnerabilities) and its potential impact to the organization. That said, every organization is different and needs to determine the specific criteria for threat prioritization that makes the most sense for their situation.[38]

As a rule of thumb, the greater the chance that an attack will succeed, the higher it should be ranked on the prioritization list. While it isn't easy to determine how successful a threat may be, a good place to start is with understanding existing vulnerabilities. For example, if an organization has known issues with unpatched devices or unsecured remote access, threats that target these areas should be given higher priority as they are more likely to be successful. Other indicators include how long has the attacker been inside the perimeter and how far has the attack penetrated. The longer the attacker has been inside or the deeper the penetration, the higher the threat should be prioritized. Achieving administrative privileges on valuable hosts is another good indicator of a potentially successful attack and one that should be given high priority.[39] Finally, understanding the type of attacker may give some indication about the level of sophistication and resources available to support the attack. Is the attacker a state-sponsored entity engaged in espionage; a hactivist making a political statement; a competitor looking for a business advantage; or a criminal looking for financial gain? The more serious the attacker profile, the higher the threat should be prioritized.[40]

Just as a higher chance of a threat's success indicates a higher priority ranking, the amount of damage a threat can cause also warrants a higher prioritization. Unfortunately, it's difficult to gauge the potential impact of a specific threat unless you know what asset the threat is targeting – and this is frequently not known until it's too late. For attacks that are just starting or are in progress (e.g. an attack is attempting unauthorized access to a remote employee laptop), chances are it is far from the ultimate goal and has less of an immediate impact, therefore it may have a lower priority. If an attacker has achieved administrator privileges and is attempting to access a database containing customer credit card information, it's likely that the attacker is attempting to steal this data and the threat should be given high priority given the high cost of customer notification and remediation. Another factor in determining potential impact is the type of attack. For example, a distributed denial-of-service (DDoS) threat could stop a vast majority of critical processes and might be given higher priority. Likewise, if a particular attack might be successful and could enable additional attacks that are more costly, then the attack might be given a higher priority.

Search analytics accelerates time to security

Machine-based analytics help automate the analysis of huge amounts of data as well as the detection and prioritization of threats, but computers alone can't do it all. Search analytics are also needed. Although they're manually performed by people, search analytics that use automated tools to support complex queries and deliver results quickly can dramatically improve time to security. How? Tools such as dashboards with drill-down features and advanced visualization techniques can provide a consolidated view of information (a single pane of glass) where data from all sources in the network such as logs, network flows, and IP packets from diverse devices and applications has been normalized into a common format. This not only saves time, it helps security personnel better understand what is going on so that issues can be escalated and preventative measures taken.

These search-based security analytics should also provide analysts with the ability to interact, query, and depict a large volume of both real-time and historical data in a wide variety of ways to make more informed decisions and better manage overall risk. Given the speed at which attacks can cause damage, real-time analysis of security data is critical so that potential threats can be escalated and steps taken to immediately neutralize them and minimize damage.[41] Likewise, historic information is especially helpful for forensic investigation of incidents that have occurred so that the organization can learn from them and take steps to remedy such situations.[42]

> …real-time analysis of security data is critical so that potential threats can be escalated and steps taken to immediately neutralize them and minimize damage.

Consolidated, graphical views and visualization techniques augment threat analysis and productivity

Because a single data source may not provide sufficient information to understand an attack, one of the most important aspects of security analytics is integrating data from different devices and applications across the extended enterprise into a centralized console. For example, a security analyst may need to synchronize network packet

Fig. 2 - Graphical Views and Visualization Enable Fast Exploration of Issues.

data with application log data and endpoint device data to get a comprehensive picture of the steps used to execute an attack. Instead of having to run several reports separately and then go back and forth between the results, dashboards can enable security analysts to automatically run and refresh multiple reports, displaying the results immediately in a cohesive, graphical and easy-to-understand format. This insures that analysts are reviewing the most recent data in the most time efficient manner to help reduce threat impact.[43] These consolidated views along with robust visualization methods can help organizations perform complex analysis and improve remediation productivity as well as reconstruct timelines and conduct forensic investigations. Advanced visualization techniques that depict contextual correlations can help analysts gain deeper security insights. These techniques not only show the data in an intuitive, graphical format, they enable analysts tointeractively manipulate the data to streamline security event analysis.

Drill-downs enable fast exploration of potential issues

Drill-downs help analysts quickly determine if a trend or event is of interest without having to run additional reports or manually search for more information. They enable analysts to simply select an item of interest, such as a dot on a map or a piece of pie chart, and obtain more details about that item. Then, after viewing the details, they can dive into more detailed information or quickly return to the original view. Drill downs should provide a wide range of views, depending on the amount of detail and level of information needed.[44]

Multiple search capabilities help locate the right information instantly

To ensure accurate and meaningful insights, many types of security information and event management search capabilities should be used. For example, an analyst might need to see all recent activity involving a specific element of the network such as a particular user ID, IP address, or website. Alternatively, they might need to retrieve events meeting a more detailed set of criteria such as attempted access to a particular type of information such as earnings reports or

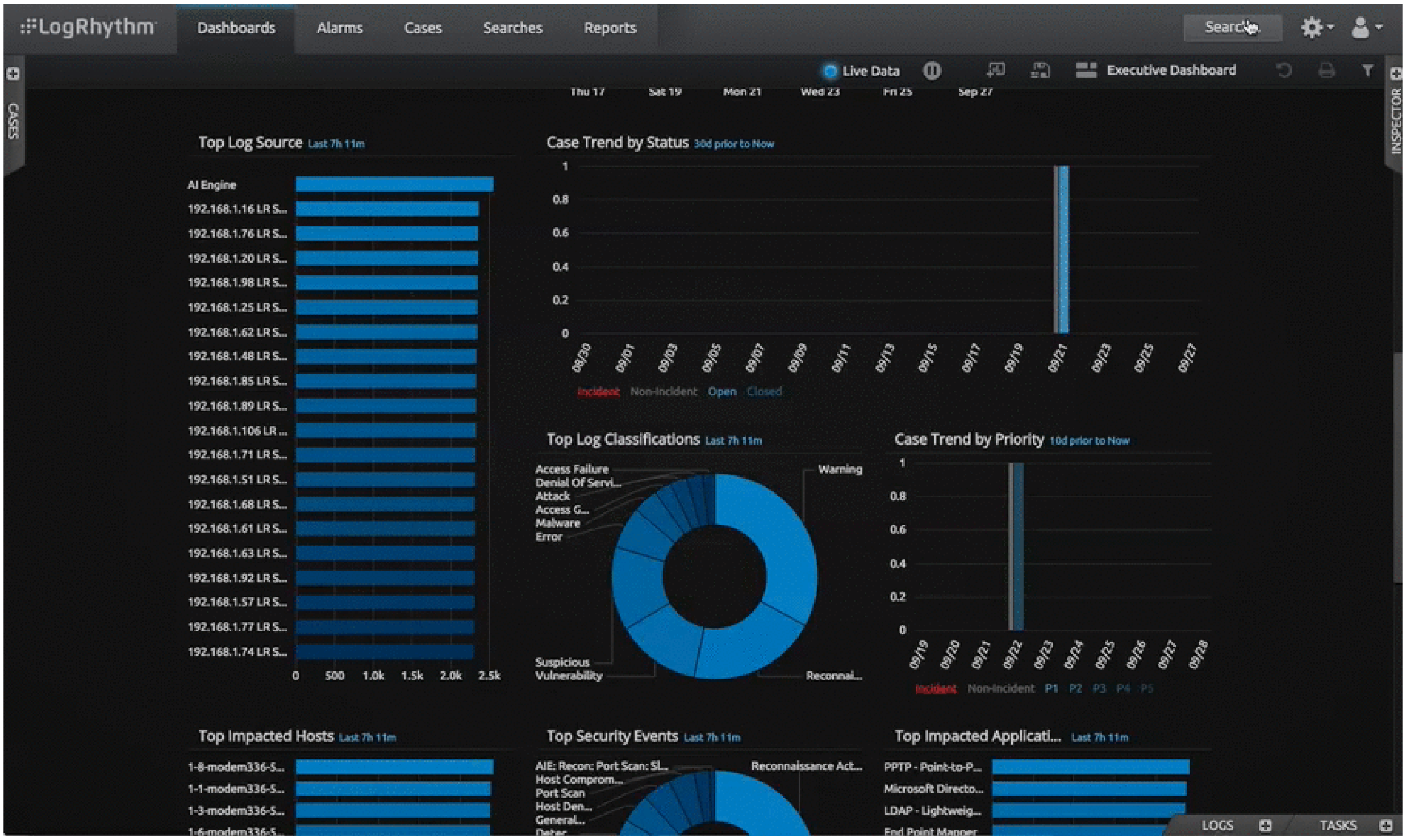

Fig. 3 - Actionable Intelligence at a Glance

personally identifiable employee information. Search-based analytics should support non-linear needs of security analysts who may pivot from query to query as they investigate individual security events and/or anomalous behavior across systems, networks, and user activity. They must also support the analysis of structured and unstructured data to enable analysis of historical security trends over long periods of time.[45]

Actionable intelligence streamlines security remediation

Companies need automated alerts that notify security and IT administrators when certain criteria have been met but they also need these alerts to go a step beyond and make actionable suggestions on how to investigate or correct the issue at hand. This requires highly-trained analysts to review all incidents and filter out some of the “noise” (e.g. reduce false positives) and distill into actionable information. Managed Security Service Providers (MSSP’s) do this by pulling the logs for the event in question and providing customers with incident information so they’re ready to start an investigation immediately upon receipt of an alert. Plus, in most cases, the alerts include data that shows customers what they need to do rather than instigating a long, detailed investigation before action can be taken. This reduces risk and provides faster time to security by enabling your staff to prioritize and focus on the most important security issues first rather than waste time tracking down false positives.

Managed SIEM Service Providers Help Accelerate Time-to-Value

MSSP's offering Managed SIEM help companies efficiently address their most pressing security issues by detecting, prioritizing and neutralizing cyber threats and by helping them meeting compliance requirements. They can do this in a manner that significantly reduces the time required to detect and respond to threats which enables organizations to neutralize these threats before they cause a damaging cyber incident or data breach. When powered by the LogRhythm Security Intelligence Platform, they can collect, classify and contextualize petabytes of machine and forensic data from across extended IT and operational environments. We then continuously and in real-time apply automated machine analytics to this contextualized data to detect cyber threats while providing robust forensic analytics and centralized search capabilities that enable customers to rapidly investigate and respond to threats.

Managed SIEM Can Help:

- Maximize your ability to block threats to reduce risk
- Identify and neutralize threats before a breach occurs
- Reduce compliance costs
- Remove complexity from security operations
- Stay protected 24x7x365 while lowering operational costs
- Leverage industry leading technology on premise or in the cloud
- Ensure critical security infrastructure stays up to date

Multiple deployment options and a 24/7 security operations center deliver flexibility

Managed SIEM service providers that have a 24/7 Security Operations Center (SOC) and a variety of implementation models can deliver flexibility and expertise beyond what SIEM resellers can offer. For example, you can purchase the solution and have it installed on your premises yet still have have 24x7 security event monitoring. Using "SIEM as a Service" can simplify security operations and remove management complexity. Outsourcing to a trusted partner who is focused exclusively on security enables companies to focus on what they do best – and not worry about the security of their systems.

Security expertise augments existing staff and investments

Security talent is hard to find and harder to keep. MSSP's with long-term LogRhythm certified deployment engineers on staff can enable better monitoring and fine tuned analysis to help keep up with and correlate incident data to identify and prevent.

Regulatory compliance reporting simplifies adherence

Depending on the industry, regulatory compliance and reporting can be burdensome with significant penalties in place for non-compliance. With MSSPs, security administrators can demonstrate that proper security controls are in place and functioning correctly to mitigate the risk of breaches (and avoid penalties).

About 1440 Security

Keeping up with today's rapidly evolving threat landscape requires skillsets that are hard to find. Whether you need help complying with standards or simply want the peace of mind from having a team of security experts on your side, we help companies keep up with today's demands through a wide range of security services built on industry leading technology. Our Every Minute™ Security Operations Center manages the LogRhythm SIEM platform, whether deployed in your datacenter or ours, and provides 24x7x365 advanced threat detection and response services to neutralize potential security threats while facilitating compliance with various security standards.

Learn more

Click here to learn more about how 1440 Security delivers best-in-class security analytics.

Contact us today to see what we can do for you.

Resources

[1] Juniper Research, “Cybercrime will Cost Businesses Over $2 Trillion by 2019” press release, May 12, 2015, https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

[2] Gemalto Breach Level Index, http://breachlevelindex.com/assets/Breach-Level-Index-Infographic-H1-2016-1500.jpg

[3] IBM and Ponemon Institute, “2016 Cost of Data Breach Study: United States, June 2016, https://www-01.ibm.com/marketing/iwm/dre/signup?source=mrs-form-2039&S_PKG=ov49599

[4] http://www.cbs.com/shows/csi-cyber/news/1003888/these-cybercrime-statistics-will-make-you-think-twice-about-your-password-where-s-the-csi-cyber-team-when-you-need-them-/

[5] Ponemon Institute, “2016 Cost of Data Breach Study: United States, June 2016"

[6] Forbes, “Cyber Crime Costs Projected To Reach $2 Trillion by 2019,” Steve Morgan, January 17, 2016, http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#79c27e573bb0

[7] CBS, “These Cybercrime Statistics Will Make You Think Twice About Your Password: Where’s the CSI Cyber team when you need them?” March 3, 2015, http://www.cbs.com/shows/csi-cyber/news/1003888/these-cybercrime-statistics-will-make-you-think-twice-about-your-password-where-s-the-csi-cyber-team-when-you-need-them-/

[8] Symantec, ” Attackers Target Both Large and Small Businesses,” 2016, https://www.symantec.com/content/dam/symantec/docs/infographics/istr-attackers-strike-large-business-en.pdf

[9] Fox Business, “Cyber Attacks on Small Businesses on the Rise,” Elizabeth MacDonald, April 27, 2016, http://www.foxbusiness.com/features/2016/04/27/cyber-attacks-on-small-businesses-on-rise.html

[10] Fox Business, “Cyber Attacks on Small Businesses on the Rise,” Elizabeth MacDonald, April 27, 2016, http://www.foxbusiness.com/features/2016/04/27/cyber-attacks-on-small-businesses-on-rise.html

[11] IBM X-Force® Research, “2016 Cyber Security Intelligence Index”, 2016.

[12] Symantec Internet Security Threat Report, 2014, April 2014, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

[13] United Nations Office on Drug and Crime, Comprehensive Study on Cybercrime, February 2013, www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[14] Ponemon Institute, "2016 Cost of Data Breach Study: United States, June 2016", http://www-03.ibm.com/security/data-breach/

[15] IBM X-Force® Research, "2016 Cyber Security Intelligence Index", 2016, www.ibm.com/security/data-breach/cyber-security-index.html

[16] Fox Business, "Cyber Attacks on Small Businesses on the Rise," Elizabeth MacDonald, April 27, 2016, http://www.foxbusiness.com/features/2016/04/27/cyber-attacks-on-small-businesses-on-rise.html

[17] Fox Business, "Cyber Attacks on Small Businesses on the Rise," Elizabeth MacDonald, April 27, 2016, http://www.foxbusiness.com/features/2016/04/27/cyber-attacks-on-small-businesses-on-rise.html

[18] United Nations Office on Drug and Crime, Comprehensive Study on Cybercrime, February 2013, www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[19] Security Info Watch, "Coping with the increasing sophistication of cybercrime syndicates," Steve Durbin, September 22, 2016, http://www.securityinfowatch.com/article/12260502/coping-with-the-increasing-sophistication-of-cybercrime-syndicates

[20] PWC, "Key findings from the Global State of Information Security® Survey 2017," http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/assets/gsiss-report-cybersecurity-privacy-possibilities.pdf

[21] Experian, "2016 Third Annual Data Breach Industry Forecast," 2016, http://www.experian.com/data-breach/2016-data-breach-industry-forecast.html

[22] NBC News, "Hack to the Future: Experts Make 2016 Cybersecurity Predictions," Keith Wagstaff, January 2, 2016, http://www.nbcnews.com/tech/internet/hack-future-experts-make-2016-cybersecurity-predictions-n486766

[23] SANS Institute, 2016 SANS Security Analytics Survey, Dave Shackleford, December 2016, https://www.sans.org/reading-room/whitepapers/analyst/2016-security-analytics-survey-37467

[24] SANS Institute, 2016 SANS Security Analytics Survey, Dave Shackleford, December 2016, https://www.sans.org/reading-room/whitepapers/analyst/2016-security-analytics-survey-37467

[25] Peninsula Press, "Demand to fill cybersecurity jobs booming," Ariha Setalvad, March 31, 2015, http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/

[26] IInformationWeek, "Cyber-Security Skills Shortage Leaves Companies Vulnerable," Kelly Sheridan, August 1, 2016, http://www.informationweek.com/strategic-cio/security-and-risk-strategy/cyber-security-skills-shortage-leaves-companies-vulnerable/d/d-id/1326463

[27] Forrester, Market Overview: Security Analytics Platforms, May 4, 2016, https://baydynamics.com/content/uploads/2016/05/Market_Overview_Security_Analytics_Platforms.pdf

[28] Verizon, "2013 Data Breach Investigations Report," April, 2013, www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

[29] TechTarget SearchSecurity, "Introduction to security analytics tools in the enterprise," Dan Sullivan March, 2015, http://searchsecurity.techtarget.com/feature/Introduction-to-security-analytics-tools-in-the-enterprise

[30] TechTarget SearchSecurity, "Introduction to security analytics tools in the enterprise," Dan Sullivan March, 2015, http://searchsecurity.techtarget.com/feature/Introduction-to-security-analytics-tools-in-the-enterprise

[31] TechRepublic.com, "How Big Data is changing the security analytics landscape," Brian Taylor, January 2, 2014, http://www.techrepublic.com/blog/big-data-analytics/how-big-data-is-changing-the-security-analytics-landscape/

[32] Gartner Group, "Demystifying Security Analytics: Data, Methods, Use Cases," RSA Conference 2016, Session ID: AIR-T09, Dr. Anton Chuvakin, February 29, 2016, https://www.rsaconference.com/writable/presentations/file_upload/air-t09-demystifying-security-analytics-data-methods-use-cases-final.pdf

[33] InfoSecIsland.com, "What Elements Are Needed for Security Analytics Success?" Mike Paquette, August 23, 2016, http://www.infosecisland.com/blogview/24812-What-Elements-Are-Needed-for-Security-Analytics-Success.html

[34] TechTarget SearchSecurity, "Introduction to security analytics tools in the enterprise," Dan Sullivan March, 2015, http://searchsecurity.techtarget.com/feature/Introduction-to-security-analytics-tools-in-the-enterprise

[35] LogRhythm, "Definitive Guide to Security Intelligence and Analytics," Karen Scarfone and Steve Piper, November 1, 2016, https://logrhythm.com/definitive-guide-to-security-intelligence-and-analytics/

[36] Webopedia.com, "Virus Signature," 2017, http://www.webopedia.com/TERM/V/virus_signature.html

[37] TechTarget SearchSecurity, "Introduction to security analytics tools in the enterprise," Dan Sullivan March, 2015, http://searchsecurity.techtarget.com/feature/Introduction-to-security-analytics-tools-in-the-enterprise

[38] LogRhythm, "Definitive Guide to Security Intelligence and Analytics," Karen Scarfone and Steve Piper, November 1, 2016, https://logrhythm.com/definitive-guide-to-security-intelligence-and-analytics/

[39] LogRhythm, "Definitive Guide to Security Intelligence and Analytics," Karen Scarfone and Steve Piper, November 1, 2016, https://logrhythm.com/definitive-guide-to-security-intelligence-and-analytics/

[40] Carnegie Mellon University, "Implementation Framework – Cyber Threat Prioritization," Troy Townsend and Jay McAllister, September, 2013, http://www.sei.cmu.edu/about/organization/etc/citp-cyber-threat-prioritization.cfm

[41] Forrester, "Market Overview: Security Analytics Platforms," Joseph Blankenship, May 4, 2016, https://baydynamics.com/content/uploads/2016/05/Market_Overview_Security_Analytics_Platforms.pdf

[42] Bloor, "The requirements of a security analytics platform," Fran Howarth, May 2, 2013, http://www.bloorresearch.com/analysis/requirements-security-analytics-platform/

[43] LogRhythm, "Definitive Guide to Security Intelligence and Analytics," Karen Scarfone and Steve Piper, November 1, 2016, https://logrhythm.com/definitive-guide-to-security-intelligence-and-analytics/

[44] LogRhythm, "Definitive Guide to Security Intelligence and Analytics," Karen Scarfone and Steve Piper, November 1, 2016, https://logrhythm.com/definitive-guide-to-security-intelligence-and-analytics/

[45] IDG Network World, "Defining Big Data Security Analytics," Jon Oltsik, April 1, 2013, http://www.networkworld.com/article/2224394/cisco-subnet/defining-big-data-security-analytics.html