WHITEPAPER

Best Practices: Cybersecurity & Critical Incident Response.

OnPage Corporation
www.OnPage.com

Best Practices: Cybersecurity Compliance & Critical Incident Response.

"Never Miss a Critical Alert!"

January 30, 2016

TABLE OF CONTENTS

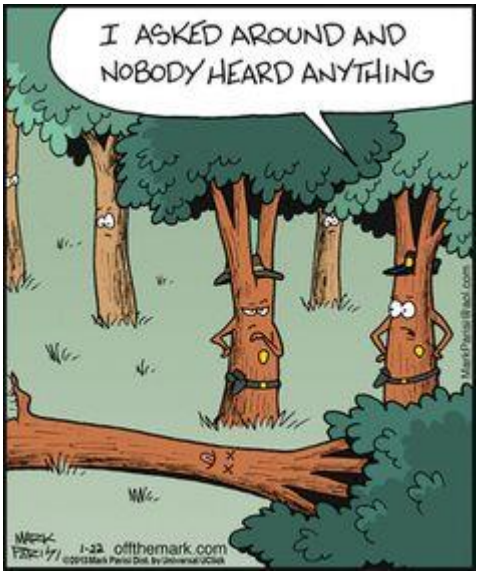
INTRODUCTION **3**
BACKGROUND **4**
DATA BREACH **5**
MOBILE THREATS **6**
SECURITY TIPS **7**
BEST PRACTICES ..... **8 & 9**
THE ONPAGE SOLUTION **10**
TESTIMONIALS **11**
REFERENCES / RESOURCES ..... **12 & 13**

Incident Response: "If a Tree Falls in the Forest…"

Incident Detection & Response is a growing challenge – security teams are often understaffed, the attack surface for intruders is expanding, and it's difficult to detect stealthy user-based attacks.

Corporations worldwide, large and small, are investing billions to protect their network infrastructure, customer credentials and data. Security monitoring and reporting isn't about if an attack will occur, it's about when and how quickly you will react to every event.

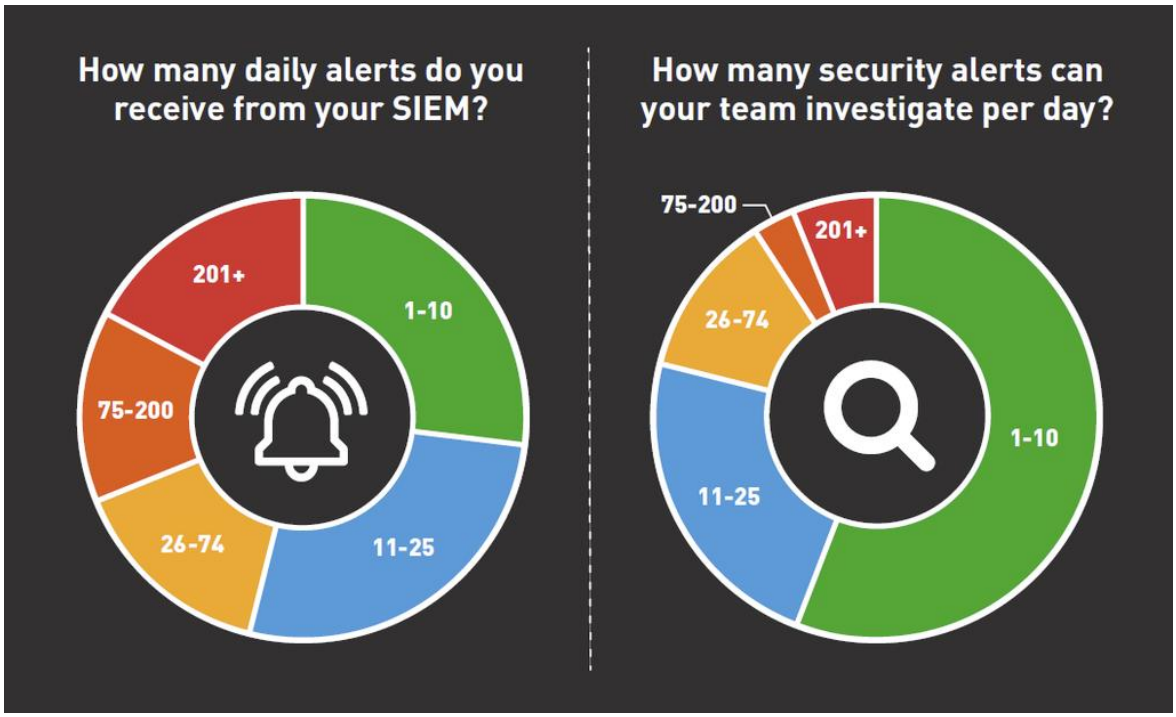
The following contains a variety of insights into the current state of cybersecurity incident response. It will address how threat exposure management relates to your business, what you can do about it and how the OnPage Intelligent Round-Trip Alerting system is a vital part of your overall RMM (remote monitoring management / SIEM (security information and event management) solution. Also included are valuable security tips, current information and infographics from respected industry sources.



The Event: "Did Anyone Hear the Tree Fall?"

Your Critical Event Messages are NOT reaching the right people in real-time!

Your team has implemented a costly Security Information and Event Management System (SIEM). Daily alerts are coming in 24/7 and slow resolution times are creating SLA complaints.



SOURCE: **Rapid7**

Cybersecurity, RMM, and SIEM solutions are costly for every business, large or small. Make sure that your chosen platform meets the regulatory compliance requirements for your specific industry.

OnPage delivers Critical messages Real-Time with escalation and failover.

Is Your IT infrastructure Secure?

SOURCE: **Solarwinds**

Mobile security threats IT should know:

When it comes to mobile security threats, IT has more to deal with than just risky, malicious apps.

Mobile malware, device breaches, lost or stolen devices, cloud service risks, leaky apps exposing enterprise data, mobile compliance, and malware aimed at enterprise assets are examples of typical security threats IT must confront.

The emergence of enterprise mobility has made it a lot more complicated for organizations to maintain compliance with government and industry-specific regulations.

Even if mobile malware isn't yet a major concern for enterprises, a few basic countermeasures can go a long way. Disabling side loading of Android apps, monitoring and quarantining jailbroken or rooted devices, establishing minimum OS versions, and keeping devices and apps up-to-date can deter most of today's mobile malware threats.

Security Tips:

SOURCE: **Solarwinds**

Best Practices:

Securing critical data, servers and users is an ever increasing challenge facing businesses.

User activity monitoring is one of the ways businesses can meet security and data protection requirements.

1. **Monitor Applications with Access to Data**

Applications are great. They give your business the tools it needs to function and be productive. But they also put your sensitive data at risk. When IT security attempts to protect critical information, it usually involves putting up firewalls and building your infrastructure around the data you want to protect. Then you give applications access to this data. When hackers look to steal your data, they won't try to hammer their way through your firewall, they'll look for the least secure system with access to the data they need.

2. **Create Specific Access Controls**

Once your IT network is secure, you need to be very careful about who you give the keys to the kingdom to. Ideally, it shouldn't be anyone. By creating specific access controls for all of your users you can limit their access to only the systems they need for their tasks and limit your sensitive data's exposure.

3. **Collect Detailed Logs**

For a complete record of what goes on in your systems – both for security and troubleshooting purposes – you should collect detailed logs and report data. This is especially the case for applications that don't have internal logging. By adding tools that can log the activities of these applications you will be able to plug any security holes those applications may create.

4. **Maintain Security Patches**

When cyber-criminals are constantly inventing new techniques and looking for new vulnerabilities, an optimized security network is only optimized for so long. When Home Depot's POS systems were hacked last summer, they were in the process of installing a security patch that would have completely protected them. To keep your network protected, make sure your software and hardware security is up to date with any new antimalware signatures or patches.

Best Practices (cont.):

5. Beware of Social Engineering

All of the technical IT security you implement can't take the place of common sense and human error. Social engineering tactics have been used successfully for decades to gain login information and access to encrypted files. Rogers Communications recently faced a major breach when a hacker called an employee pretending to be the IT department and was able to get the employee's log-in information. Attempts like this one may come from phone, email or other communication with your users. The best defense is to…

6. Educate and Train Your Users

No matter how gifted, your users will always be your weakest link when it comes to information security. That doesn't mean you can't limit this risk through regularly educating your users on cyber security best practices. This training should include how to recognize a phishing email, how to create strong passwords, avoiding dangerous applications, taking information out of the company, and any other relevant user security risks.

7. Outline Clear Use Policies for New Employees and Vendors

To strengthen and clarify the education you give your users, you should clearly outline the requirements and expectations your company has in regards to IT security when you first hire them. Make sure employment contracts and SLAs have sections that clearly define these security requirements.

8. User Activity Monitoring

Trust but verify. While well trained users can be your security front line, you still need technology as your last line of defense. Insider Threat Detection Solutions allows you to monitor users to verify that their actions meet good security practices. If a malicious outsider gains access to their log-in information – or if an insider chooses to take advantage of their system access – you will be immediately notified of the suspicious activity.

9. Create a Data Breach Response Plan

No matter how well you follow these best practices, you might get breached. In fact, nearly half of organizations suffered a security incident in the past year. If you do, having a response plan laid out ahead of time will allow you to close any vulnerabilities and limit the damage the breach can do.

10. Maintain Compliance

Regulations like HIPAA, PCI DSS and ISO offer standards for how your business should conduct its security.

The Missing Link is OnPage!

Investing in Cybersecurity? OnPage ensures Critical Alerts get to the right person securely with Real-Time Incident Management! Intelligent Messaging, Escalation Schedules & Audit Trails are easily integrated into your existing Remote Monitoring Software. OnPage will plow through the noise and prioritize the most crucial alerts.

Cybersecurity Compliance:

- OnPage is fully compliant with Data Security Regulations and guidelines for both IT and healthcare professionals. OnPage security protocols are designed "out-of-the-box" to comply with the most common regulations such as HIPAA, PCI, DSS and SOX. Corporate data security is assured.

Cloud-Based Priority Alerts:

- Agile Security

Shorten Incident Lifecycle:

- OnPage is vital to an effective event response program.

Global Coverage:

- Major Corporations, and Blue Chip Organizations Worldwide trust OnPage.

Audit Trails:

- Mandatory for Security Regulations

Cost Effective & Fast Integration with popular RMM software:

- Easy installation and quick deployment.

Real-Time, Round-Trip Notification:

- Includes custom escalation protocols and failover.
- Situational awareness of the IT Ecosystem & Infrastructure.

On-Call Management:

- Intelligent Routing of On-Call Personnel.

Testimonials:

Arkansas Electric Chooses OnPage for Cybersecurity Intrusion Compliance.

"OnPage solved a mandatory requirement we had in our data center for regulatory cybersecurity compliance. To cover physical or cyber intrusions, we have OnPage notifications sent out to the group on an on-call rotation for incident response."
~ Philip Huff – Director of IT Security Compliance.

***

One of the Nation's Busiest Data Centers Chooses OnPage for IT Communication, Cyber Security Compliance and Priority Alerts.

"The OnPage smartphone system gets the correct technician's attention quickly every time. Needless to say we would never go back to the old style obsolete standalone pagers again and we're happy to recommend OnPage to our colleagues."
~ Doug Goss – Chief Engineer

***

Model N Revenue Management Cloud Solutions praise for OnPage.

"I went to the Apple App store and found OnPage. The app worked extremely well. I've never missed a page and every time a page comes through, I am able to easily distinguish the tone. As an IT professional, I would highly recommend this app for mission critical systems."
~ A. Gouyang - Server System Admin

References:

Resources:

TechTarget:

- http://searchnetworking.techtarget.com/feature/The-fundamentals-of-availability-monitoring-tools
- http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM
- http://searchmobilecomputing.techtarget.com/tip/Three-mobile-security-threats-IT-should-know
- http://searchmobilecomputing.techtarget.com/news/4500270274/IT-in-the-gutter-with-mobile-compliance

RAPID 7

- https://www.rapid7.com/resources/infographics/images/Rapid7-IDR-survey-infographic.pdf
- https://www.rapid7.com/resources/infographics/state-of-incident-detection-and-response.html
- https://www.rapid7.com/company/news/press-releases/2016/rapid7-research-study-finds-compromised-credentials-top-concern.jsp

Solutions Review

- http://solutions-review.com/security-information-event-management/files/2015/11/SolarWinds-Infographic.jpg
- http://solutions-review.com/security-information-event-management/2015/11/12/4-essential-steps-to-avoid-security-breaches-an-infographic/

SC Magazine

- http://www.scmagazine.com/the-new-80-20-rule-for-data-center-cybersecurity/article/397220/

Deloitte

- http://www2.deloitte.com/content/dam/html/us/analytics-trends/2016-analytics-trends/pdf/analytics-trends.pdf

Observe IT

- http://www.observeit.com/blog/10-best-practices-cyber-security-2015

OnPage Knowledge Base:

- Solarwinds Integration
  - http://onpage.com/wp-content/uploads/2015/05/OnPage_Tech_Tips.pdf
- Arkansas Electric Case Study: Cyber Security Compliance
  - http://onpage.com/wp-content/uploads/2015/08/Arkansas-Electric-Cooperative-Case-Study_V2.pdf
- IT Alerts: How to Improve Responsiveness
  - http://onpage.com/wp-content/uploads/2013/11/IT-Alerts_-How-To-Improve-Responsiveness1.pdf
- Data Center Case Study: Chief Engineer Doug Goss
  - http://onpage.com/wp-content/uploads/2015/08/Doug-Goss-Case-Study_V3.pdf

FOR MORE INFORMATION

OnPage Corporation
460 Totten Pond Road
Waltham, MA 02451
781-916-0040

Never Miss a Critical Alert!