All too often, security looks more like the cleanup crew after an attack, and less like the centurions standing guard to ensure that nothing bad gets in. In reality, security is a bit of both. How much of each depends on how well you respond to security incidents and whether you leverage them to make your environment more secure.

Intrusions happen. The challenge is knowing when they happen and what specifically to do about them. To quickly and efficiently respond to issues, you need to leverage all the security feeds in your environment to help you plot and visualize activity that might indicate a valid security concern. When a possible issue pops up your security analyst needs to be able to instantly see the context around the user and computer involved.

But that’s only the beginning. Once a security incident is confirmed, what’s the response? Don’t figure it out as you go along. History repeats itself and so do security incidents; they can be categorized and you need to develop corresponding playbooks so that your response is appropriate, complete and consistent.

Without a plan, you will likely address each issue in a one-off manner, with few details, no real context around the incident-related activity, and little insight into what your next steps should be. What’s needed is an incident response plan that outlines both the high-level steps (e.g., quarantine a machine that is infected with malware) and the more detailed steps that help to define the scope of the incident—and further necessary activity. Look for insights from Exabeam throughout this paper.

This whitepaper looks at the top three security scenarios that are ripe with risk to the organization. The paper will discuss, step by step, how to properly respond should these events occur. The top three security scenarios include:

**Exabeam – Security Specialists**

What makes any organization secure is an understanding of how the enemy thinks and acts, enabling the organization to proactively take action to thwart an attack. But in most cases, even with the best defenses in place, the enemy gets inside via email or malware-laden websites—or even worse, is already inside as an employee.

Exabeam’s Security Intelligence Platform provides organizations with data collection, User and Entity Behavior Analysis, and automated incident response, all running in concert to automate detection, alerting, investigation, and response when incidents occur.
Scenario 1: Malware on an Endpoint

In 2017, malware is the #2 preferred attack vector, with 51% of all data breaches including malware as part of the attack\(^1\). And although much of the news focus has been on ransomware (which is considered part of the malware threat), malware that is designed to give external attackers access to your network is a much greater threat. As such, identifying malware infections—and understanding the scope of the infection—as quickly as possible is critical to the security of your organization.

Exabeam Insight – Impact and Spread

You might think that you simply need to be informed when malware is found on a given endpoint so that it can be removed (or the endpoint reimaged). But in practical application, you need visibility into which actions transpired before and after an infection, from both the user and endpoint perspectives. These details provide context around the impact on the endpoint in question (e.g., what’s been installed, which tools were used, which actions were taken) and the spread of the infection (e.g., whether an attacker has moved to another endpoint from the initial foothold). This information helps you to pinpoint both how a machine was infected and whether any additional malicious activity occurred. For example, was the endpoint infected by a user clicking a malicious link or by an external attacker who compromised the endpoint by using elevated credentials that were obtained from another endpoint? Once the endpoint was infected, were any tools used to obtain credentials stored in memory, to continue moving laterally throughout the organization?

Understanding the impact and spread of an infection greatly dictates the proper incident response.

So, which steps should you take to understand the impact and spread of an infection?

Step 1: Define Your Triggers

The first part of your IR plan for malware infections should define the triggers that identify an incident of this type. Your tools should include:

- **AV alerts** – Alerts use traditional malware-centric signature- and heuristic-based detection.
- **Next-gen AV** – In this more system-centric approach, processes, methods, techniques, and procedures indicate malicious intent.
- **Initial EXE launch** – The first time an application is run can indicate malware or hacker tools.
- **Outbound traffic signature** – The use of DNS and specific traffic patterns can be analyzed to identify malicious activity.
- **User reports** – Helpdesk calls around poor performance can be a leading indicator.

Each method requires some level of monitoring, usually by a third-party solution. But by having these tools in place, you can be made aware of a potential infection as early as possible. Typical responses, such as reimaging endpoints or resetting a user’s password, are usually the extent to which organizations go … and then it’s back to business as usual.

But what should you actually do to help ensure that your environment is secure?

Step 2: Quarantine the Endpoint

If you subscribe to “reimage and move on” thinking, you’ve done little more than treat a symptom. You see, the presence of malware itself isn’t the threat; rather, malware is the means by which far more malicious and sinister activity is enabled. So the ability to study the infected endpoint, to determine whether the simple infection is all that has transpired, is critical. Quarantining can be done physically, virtually, or through network segmentation. The endpoint should be isolated so that the malware cannot connect to other endpoints and is not accessible from the Internet. However, the endpoint does need to be accessible to IT, to facilitate the investigation portion of the incident response.

\(^1\)Verizon, Data Breach Investigations Report (2017)
Step 3: Investigate the Source and Scope of the Infection

After isolating the endpoint, you need a solid understanding of exactly what has transpired. Is this a single infection that went no further than the endpoint? Or is it merely the first discovered infection in a massive compromise that has embedded itself across your network?

To find out, you need to answer several questions across two aspects: the user and the endpoint. Simply looking at one or the other isn’t enough; it’s the combination of the two that paints the picture of what malicious actions have transpired, the risk the organization faces by this specific infection, and whether the scope extends beyond the identified endpoint. Questions should include the following:

• What has this workstation’s user been doing? As is appropriate, find out how the workstation endpoint was infected. By looking at the activity of the user account most associated with the endpoint, you can identify how the malware came in, and possibly whether steps were taken to make its presence persistent and stealthy.
  
  Prior to infection – Review downloaded files, visited sites, and incoming email from first-time senders, to provide context around how the system became infected.
  
  After infection – Look for abnormal or questionable programs that were executed, /runas account switches in command lines, and outgoing email, to see which additional actions were taken. Also determine whether the primary user’s behavior has changed since the system was infected—a potential indicator that the user account has been compromised in addition to the endpoint.
  
• Which users have logged on to this endpoint? Identify the users that have used the endpoint recently, to provide context around the data, applications, and systems with which they interact. This action gives IT insight into where you need to look next.

• Have any privileged users logged on to this endpoint? Although particularly important with servers, this question needs to be addressed for all endpoints. Attackers who use malware to gain entry use tools that scrape credential artifacts from the memory of accounts that have previously logged on to the endpoint in question. This approach enables attackers to gain access to additional systems on your network. Understanding the privileged accounts that have logged on recently gives IT insight into which resources and systems might have been compromised.

• What have privileged users with previous logon sessions been doing since intrusion? This is the next step from the previous question. A review of user activity across any and all systems for any privileged accounts that were used on an infected endpoint needs to be done. See whether anything out of the ordinary indicates the malicious use of compromised credentials.

• What has this endpoint been doing? Because some malicious actions are technically handled by the OS and not the user (depending on the tools that are used), it’s important to have visibility into which connections, communications, transmissions, and so on involved the endpoint:
  
  Internal network connections – With which other internal endpoints has this computer initiated communications?
  
  DNS queries – Which Internet domains have been queried? Do they indicate the use of domain-generation algorithms? Are they consistent with command and control traffic within TXT record DNS queries?
  
  Website URLs – Which domains has the endpoint visited that are not in the Alexa top 1M sites? Would any URLs fall into suspicious categories? Are any uncategorized?
  
  Outbound connections by process – Which processes are attempting outbound connections, and are any out of the ordinary?
  
  Process lineage – Malware can spawn other processes that would otherwise look normal, so knowing what is responsible for every launched process is important.
  
  Registry changes – Would any entries (such as RunOnce values) help establish malware permanence?
Exabeam Insight – What if the Endpoint Is a Server?
All the previous investigative direction should be equally utilized if a server is compromised. But because a server is far more likely to have privileged users and to host valuable data, it’s even more critical to quickly investigate all user logons, as well as the user and endpoint activity mentioned previously.

Step 4: Analyze the Infection

You can gather a ton of information from the previous step—so much so that you might find plenty of false flag activity. For example, you might find that a machine infected with ransomware also had a process run for the first time on the very same day. Does that mean it’s malicious? Without context, it’s impossible to tell.

What’s necessary is to take the user and endpoint evidence that you find, and look for similar evidence on other users or endpoints. Comparing to peer groups is a fast and effective way to do so, as peers who perform the same job functions tend to have the same applications, privileges, and so on as that of the user and the endpoint.

You want to establish what’s normal for your users and endpoints, and what’s an outlier that requires further scrutiny. That first-run might be found only on machines that are infected with the same ransomware, indicating that the attack surface within your network is much wider than the single user or endpoint. But if the same process is commonly found on uncompromised machines, you can rest assured that it’s benign—and move on to your next piece of evidence.

At the end of your investigation, the goal is to have some new insight into how the malware came in, which tactics it used, how it spread (if applicable), and how it functions. Then you’ll take that information to the next step, to improve your organization’s security stance.

Step 5: Prevention

The answer to preventing further malware attacks isn’t to simply update the definitions on your AV. The answer is found in taking the evidence from your investigation and applying the specific details about how the infection made its way inside, enabling you to take preventative actions to improve security:

• **Block the infection vector** – Which patches, security policies, and firewall settings should be continually updated?

• **Block malicious outbound connections** – Command & control (C&C) connections are a necessary part of arming malware. Which specific URLs, domains, and protocols should be clocked to prevent this type of traffic?

• **Network IDS for intraconnections** – Are the specific types of connections that should be monitored, and potentially blocked, made internally between systems?
Exabeam Insight – Making Sense of All the Data: Before, During, and After

All the detail mentioned here is valuable in trying to identify the source, existence, and scope of a malware infection. But manually collecting and analyzing all this data is pretty much impossible in any realistic timeframe. You’d need a way to compile all the audit data around processes, logons, network traffic, protocol use, and so on, requiring countless programs and searches to gain meaningful and actionable intelligence.

Exabeam’s behavior-based security intelligence begins with collecting all pertinent data for both the user and the endpoint, along with alerts from integrated security solutions. Then, Exabeam analyzes all activity and alert, and provides a visually intuitive way of seeing all activity as a timeline (shown in the following figure).

Activity considered anomalous along the timeline (such as the Symantec detection of a Trojan at the bottom of the image) is highlighted on the right side, complete with relevant details such as suspicious external VPN logins and remote access sessions (as shown in the following figure), likely performed by an attacker. This information provides insight into which actions led up to an infection, and which activity occurred afterward.

Quickly making sense of the massive amounts of data that are involved with even a single malware infection is the difference between stopping an attack in its tracks and giving an attacker full access to your entire network.
Scenario 2: Successful Phishing Attack

It isn't difficult to fool a user who isn't vigilant 24/7. After all, they're thinking about their job—not whether an email is a phishing attack. That's probably why 66% of malware in 2016 was installed via a malicious email attachment\(^1\). Attackers are finding sophisticated ways to increase their success rates: impersonating users within the company, using social engineering, and finding multistep ways to infect machines, bypassing security solutions that are intent on detecting them. It's no wonder phishing remains a powerful means of attack today.

So which steps should be a part of your incident response plan?

### Step 1: Identify and Analyze the Phishing Email

Because the assumption is that the user has fallen prey to an attack (which has likely resulted in a malware infection), it's first important to identify the email responsible for the attack. Is this a spear-phishing attack, which might target only select users, or have other users received the same email?

Analyzing the phishing email is about discovering details that will form a preventative response against future attacks (more on this later). Pertinent details include links, attachments, attachment-detonation behaviors (you'll need a virtual sandbox in which to detonate attachments), the sending email server, and the reputation of the sender, the sending domain, and the domains used in the links.

**Exabeam Insight – Automating Phishing Investigation**

As you consider the details you would gather in a phishing scenario, you can begin to see how the actions to identify an attack and to prevent further similar attacks take a consistent form. You can create a playbook of sorts—and then automate the set of actions you need to take.

\(^1\)Verizon, Data Breach Investigations Report (2017)
Phishing attacks generally have two endgames. Either social engineering is used to fool the user into providing credentials, such as an email that indicates “Your Office 365 password has expired; please reset it here”, or links and attachments are used to facilitate the installation of malware. In a malware-related compromise, refer to the previous scenario for the steps to include in your incident response, using the email as the inflection point of your investigation.

But in the case of credential theft, answer these questions to understand the impact of the attack:

- **Were the user’s credentials compromised?** In cases like the Office 365 password example, the answer to this question is generally yes.

- **On which access points of Internet presence can the credentials be used?** The answers include OWA, your VPN, Office 365, and other federated clouds. If you use Active Directory Federation Services or Azure Active Directory Sync, your on-premises Active Directory is also at risk.

- **Is the user’s email account now being exploited?** With compromised credentials, attackers can target other employees by posing as the initially compromised account, in an effort to infect other machines with malware. Analyzing outbound email for anomalies, attachments, and so on should be part of your investigation.

**Exabeam Insight – Compromise in the Cloud**
If an attacker tricks a user into providing credentials to, say, Office 365, the attacker might never need to access the internal corporate network. Rather, the attacker can simply navigate SharePoint Online to obtain whatever valuable data is accessible. Because most organizations lack visibility into access of their cloud-based resources, this kind of compromise can have the most negative impact.

As with malware infections, you can use collected investigative evidence to take preventative measures that can limit your organization’s exposure to another attack:

- **Blocking at your gateway or next-gen firewall** – You can deny specific links or the base URL here.

- **Blocking at the email server or scanner** – You can block specific senders, domains, attachment types, and so on here.
Scenario 3: Departing Employee

Insiders are one of the greatest threats to an organization. They already have access to valuable data, and data theft by an employee can be the most difficult activity to spot; 81% of insider threats take months or years to detect\(^1\). Departing employees can be particularly tricky, as they might have motive (financial, emotional, or personal)—and certainly have opportunity—to take information, work product, and even intellectual property with them. Research shows that 59% of employees, whether leaving an organization voluntarily or involuntarily, say they take sensitive data with them\(^2\).

Typically, when an employee leaves voluntarily, most organizations’ actions are limited to identifying and disabling accounts and escorting the employee from the building. In essence, the employee departure isn’t seen as a security incident.

But because of the risk of these employees taking information, every employee departure should be treated the same, regardless of whether the departure is voluntary. Here’s why: If someone’s leaving to take on a similar role at a new company and gives proper notice, they might have been planning the leave for weeks or months—and might take some of their work product with them to make the transition easier. And although termination of an employee may seem unexpected, most employees know that they aren’t doing a good job and prepare for an exit in much the same manner.

So which steps should you take?

Step 1: Get Possession of Physical Devices

The company needs to reclaim every device that contains or provides access to company information. This includes laptops, phones and tablets, tokens, keys, badges, and vehicles.

Step 2: Identify All Used Accounts

Every account used by the employee should be disabled upon their departure. These accounts should include both on-premises systems and cloud applications.

Step 3: Look at Before and After Behavior

To gain visibility into whether company data has been taken, you need to look at the employee’s behavior around one of two points in time. For an employee leaving voluntarily, the point in question is when they give notice. It’s imperative to look at their behavior not just after notice is given (i.e., the timeframe between when notice is given and their departure date), but in the days and weeks leading up to the date of notice. For the employee being terminated, it’s purely a before play, with their termination date as the inflection point.

Watch several types of behaviors for clues of data theft:

- Access of unusual systems
- Access of unusual buildings or rooms
- Increased information access or consumption
- Increased sending of email
- Abnormal use of applications or processes
- Use of programs like WinZip
- Access of removable media
- Large data transfers
- Execution of privacy cleaners

---

\(^1\) Verizon, Data Breach Investigations Report (2017)

Look for abnormalities that deviate from the work the employee normally does. For example, if there is a large uptick in the amount of uploaded web traffic for a given user, they might be copying data to a cloud-based storage service such as Dropbox. You need to think like a thief, and look for user or endpoint evidence that might indicate the improper use of company resources to exfiltrate data.

This approach is perfect for low-level users, but what about for privileged users?

If the departing employee is a privileged user, you should look for other specific actions that more fit the employee’s level of access. Regular users are relatively unsophisticated and will simply copy files to a USB drive, or email a file to their Gmail account. But privileged IT users understand how they might be caught, and will take steps to hide their tracks. So expand your scope of activity to monitor:

- All account maintenance
- The setup of back-door accounts
- Abnormal activity around the assets and data that the employee’s specific privileges allow
- The clearing or disabling of any audit logs on applications or systems to which the employee has access
- Any account creation or firewall rule changes

Exabeam Insight – Going Back in Time

As soon as you know an employee is leaving, keep a closer eye on them. IT needs visibility into patterns of access that indicate an abnormality. Remember, employees normally access information as part of their job, so the simple use of those privileges isn’t necessarily malicious in intent. Instead, look for changes such as an increase in activity (e.g., copying 10 times more data than usual), odd times of activity, or the use of applications or websites that were previously never used.

Take the example of a developer named Gary. Exabeam’s Incident Responder is watching every action that Gary or his endpoint performs. Pulling in activity from other systems—such as your building’s security system and GitHub—you can easily see that Gary has begun his work day about 3 hours earlier than usual and is pulling down an unusually high amount of data from his software-development platform.

This visibility extends back in time to before Gary put in his notice, enabling security teams to review his activity to ensure that data hasn’t been taken prior to the time he gave notice.
Building the Right Incident Response Plan

Security incidents like the ones covered in this paper are not just possible, but probable. Given the risk each one presents to the organization, the proper response plan needs to incorporate a means of detection and go well beyond cleanup. Rather, the plan should seek to understand why the incident happened, how it happened, and what can be done to mitigate it from happening again.

To accomplish these goals, your response plans needs to incorporate monitoring and analysis of both the user and the endpoint, looking at activity both before and after the incident in question. By incorporating data gathered from many sources (e.g., user, endpoint, building, applications), you can intelligently leverage this information to both focus your response efforts and reduce future risk.

About Exabeam
Exabeam provides security intelligence and management solutions to help organizations of any size protect their most valuable information. The Exabeam Security Intelligence Platform uniquely combines unlimited data collection at a predictable price, machine learning for advanced analytics, and automated incident response into an integrated set of products. The result is the first modern security intelligence solution that delivers where legacy security information and event management (SIEM) vendors have failed. Built by seasoned security and enterprise IT veterans from Imperva, ArcSight, and Sumo Logic, Exabeam is headquartered in San Mateo, California. Exabeam is privately funded by Lightspeed Venture Partners, Cisco Investments, Norwest Venture Partners, Aspect Ventures, Icon Ventures, and investor Shlomo Kramer.

About Randy Franklin Smith
Randy Franklin Smith is an internationally recognized expert on the security and control of Windows and AD security. Randy publishes www.UltimateWindowsSecurity.com and wrote The Windows Server 2008 Security Log Revealed—the only book devoted to the Windows security log. Randy is the creator of LOGbinder software, which makes cryptic application logs understandable and available to log-management and SIEM solutions. As a Certified Information Systems Auditor, Randy performs security reviews for clients ranging from small, privately held firms to Fortune 500 companies, national, and international organizations. Randy is also a Microsoft Security Most Valuable Professional.