
WHITE PAPER

exabeam

# STREAMLINING INCIDENT RESPONSE OPERATIONS WITH ORCHESTRATION AND AUTOMATION

Not so long ago, large-scale data breaches were novel and somewhat revolutionary, in that they changed perceptions consumers held of affected companies and shaped buying habits. But today such breaches are commonplace. Almost every week another national retailer, government organization, or multinational corporation is in the news for having exposed consumer data through a data breach.

Repeated exposure to mega-breaches may have desensitized the masses, but the consequences from them are as damaging as ever. For example, consider the now-infamous Target and Home Depot breaches, each costing hundreds of millions in insurance proceeds, legal fees, and credit monitoring reimbursement.[1] And this doesn't even begin to factor in the reputational damage suffered by these household brands.

Such attacks show no sign of abatement. Data from sources such as Verizon's Data Breach Investigation Report (DBIR) show the opposite—that is, a steady increase of such occurrences over time. DBIR data from 2010 – 2017 shows that data breaches have seen a 22% average growth rate. Another study surveyed 1,100 IT security personnel, finding that 79.2% of respondents believed their corporate network had been successfully compromised by a cyberattack within the past 12 months.[2]

Two takeaways from the myriad of similar statistics are available:

- The threat is growing
- Investments in preventative security solutions (e.g., firewalls, 2FA) haven't solved the problem

Security leaders must adopt attacker mentality—that the latter will find ways past fortifications. Thus security efforts need to continually focus on detecting and quickly responding to advanced threats.

## SLOW, INCONSISTENT RESPONSE IS STILL THE NORM

Effective response measures prevent minor security incidents from becoming major data breaches. By stopping attacks early, organizations have the opportunity to limit the impact of any given event. Unfortunately, incident response (IR) teams charged with handling security alerts and investigating incidents are overwhelmed and understaffed.

On average, a 2016 BakerHostetler[3] report estimates it takes 50 days for companies to detect, investigate, and contain security incidents. With the myriad of tools available to security analysts, why does it take so long to respond? The numerous reasons include:

- **An Overwhelming Workload** – In most SOCs, analysts face workloads that are impossible to complete. Given their available resources, it's often not feasible to address every alert received. Instead they attempt to identify those posing the highest risk to their organization and focus on them. This means that some potentially high-risk incidents may slip through the cracks.

- **Overly Manual Investigations** – The standard incident investigation process is to query and pivot through a SIEM to gather evidence, then assemble it into an incident timeline. Each query may take hours and yields only a portion of the evidence, so investigations often take days or weeks to complete.

- **A Myriad of Tools** – Throughout the process of investigating and handling incidents, IR analysts engage a wide array of security and IT infrastructure tools to access data and take corrective actions. Alternating between systems slows their workflow and hinders productivity. For example, investigating a phishing email may entail switching between a threat reputation service, an email security solution, and a sandboxing tool.

  If such interactions could be gathered into a single interface, analysts would be able to operate more efficiently.

1. http://www.digitaltransactions.net/news/story/Expenses-From-the-Home-Depot-and-Target-Data-Breaches-Surpass-_500-Million
2. CyberEdge Threat Landscape Report 2017
3. BakerHolsterIter 2017 Data Security Incident Response Report

- **A Skills Shortage** – Perhaps most importantly, there is a far reaching and well recognized cybersecurity talent shortage. A recent McAfee report states that by 2019, half of all security openings will be vacant[4]. Being unable to fill out their teams, SOCs increasingly operate with skeleton crews, exacerbating the problems already mentioned.

Exabeam Incident Responder (EIR) was developed from the ground up to tackle these issues by improving staff organization, optimizing processes, and automating the work IR teams perform. EIR amplifies the ability of SOC teams to respond to threats, vastly improving their productivity.

## MODERN INCIDENT RESPONSE SOLUTIONS—KEY FEATURES

### TICKET MANAGEMENT

Incident management often relies a ticketing system or a case management tool. This provides a centralized user interface for tracking the status, owner, and evidence related to security investigations.

In many organizations, security teams are forced to use a legacy ticketing system owned by the IT team. This results in the comingling of security incidents with basic IT tasks, such as “Create a user account” or “Troubleshoot Wi-Fi issues,” rather than “Respond to ransomware outbreak affecting a dozen endpoints.”

Exabeam Incident Responder (EIR) was developed from the ground up to tackle these issues by improving staff organization, optimizing processes, and automating the work IR teams perform. EIR amplifies the ability of SOC teams to respond to threats, vastly improving their productivity.

To truly enable security teams, organizations should provide SOCs with a purposeful incident management system—separate from that of the IT admins. Now armed with a dedicated case management tool, IR teams would be free to customize it to better conform to their own information and workflow types.

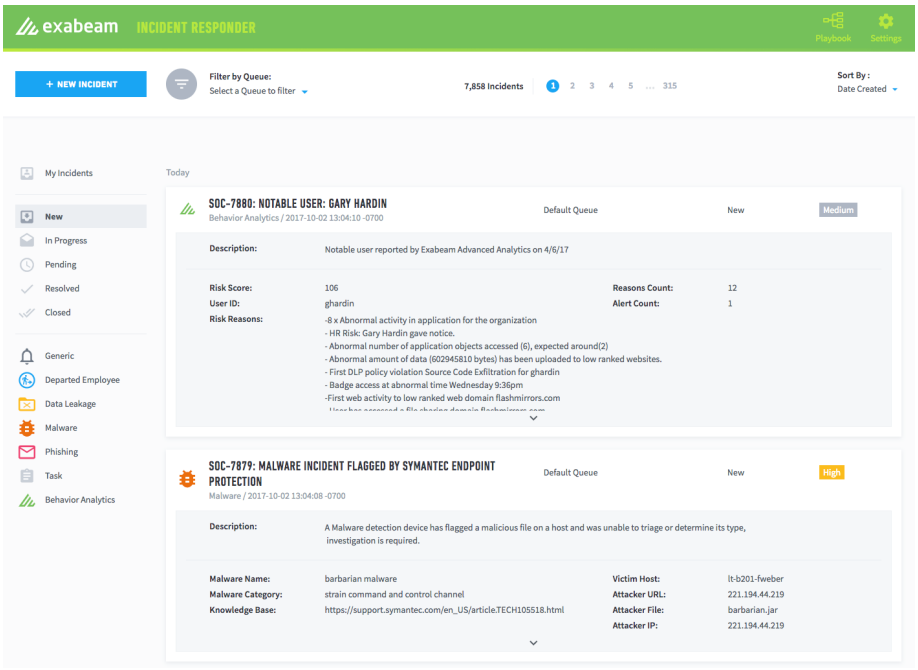



Figure 1. Incident Responder’s fully customizable incident management system.

information and workflow types. Enter Exabeam’s Incident Responder. Its UI is fully customizable—all workflows, fields, statuses, and values can be easily tailored to meet individual security team needs.

Moreover, Incident Responder is context aware, such that it automatically recognizes specific incident types it has ingested. In your role as an analyst, it then presents you with the most relevant information about any incident type. For example, a malware event might display its variant name, victim host, and attacker URL, while a phishing occurrence would highlight such items as the To:, From:, and Subject: lines.

4. Hacking the Skill Shortage Report, McAfee, 2016

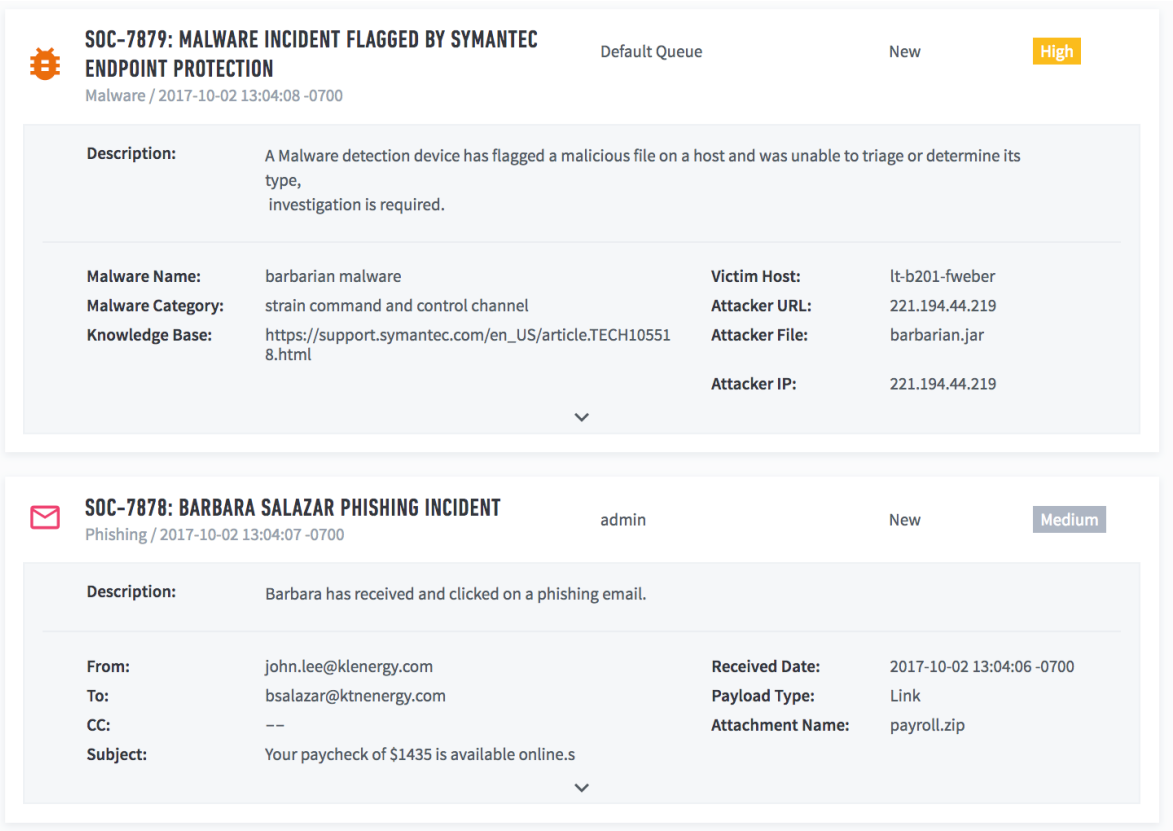
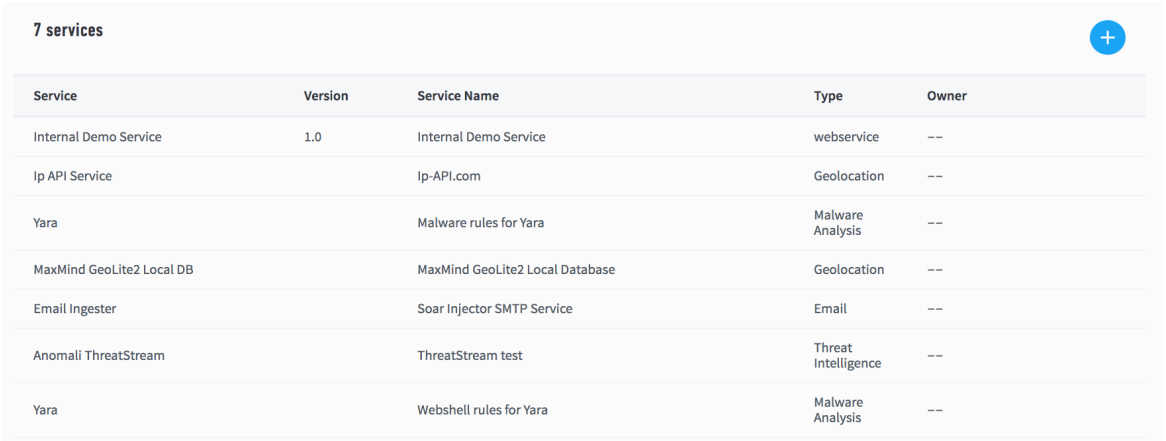



Figure 2. Contexual awareness helps Incident Responder automatically determine incident types and display relevant information.

## SECURITY ORCHESTRATION

Switching to yet another tool for investigation or to take corrective action—logging in, finding the correct tab, copying and pasting information, etc.—wastes time that could otherwise be applied to moving an incident closer to resolution. Connecting and coordinating all security across your organization's entire infrastructure, security orchestration uses prebuilt, bi-directional APIs to enable a single, centralized UI to run actions in other tools or poll information from them. Leveraging this capability, Exabeam Incident Responder programmatically runs actions from a single screen, reducing productivity lost to "swiveling chair syndrome." And it provides turnkey support for many popular security solutions.




| Service | Version | Service Name | Type | Owner |
|---|---|---|---|---|
| Internal Demo Service | 1.0 | Internal Demo Service | webservice | -- |
| Ip API Service | | Ip-API.com | Geolocation | -- |
| Yara | | Malware rules for Yara | Malware Analysis | -- |
| MaxMind GeoLite2 Local DB | | MaxMind GeoLite2 Local Database | Geolocation | -- |
| Email Ingester | | Soar Injector SMTP Service | Email | -- |
| Anomali ThreatStream | | ThreatStream test | Threat Intelligence | -- |
| Yara | | Webshell rules for Yara | Malware Analysis | -- |

Figure 3. External services configured for use by Exabeam Incident Responder.

Exabeam Incident Responder offers prebuilt connections to all popular security and IT infrastructure tools used by organizations such as yours; this renders obsolete the script use to achieve automation.

The following table compares the traditional script-based approach to automation using security orchestration.

| Traditional Scripting | Security Orchestration with Exabeam IR |
|---|---|
| Requires basic coding background | Uses a point-and-click interface accessible to junior talent (e.g., interns) |
| Requires API key script inclusion | Automatically performs API key management |
| Scripts must be written for each action or step in a process | Has hundreds of prebuilt actions that can be selected from dropdown menus |
| Complex tasks may require many scripts | Complex tasks can be handled with playbooks comprising many actions |

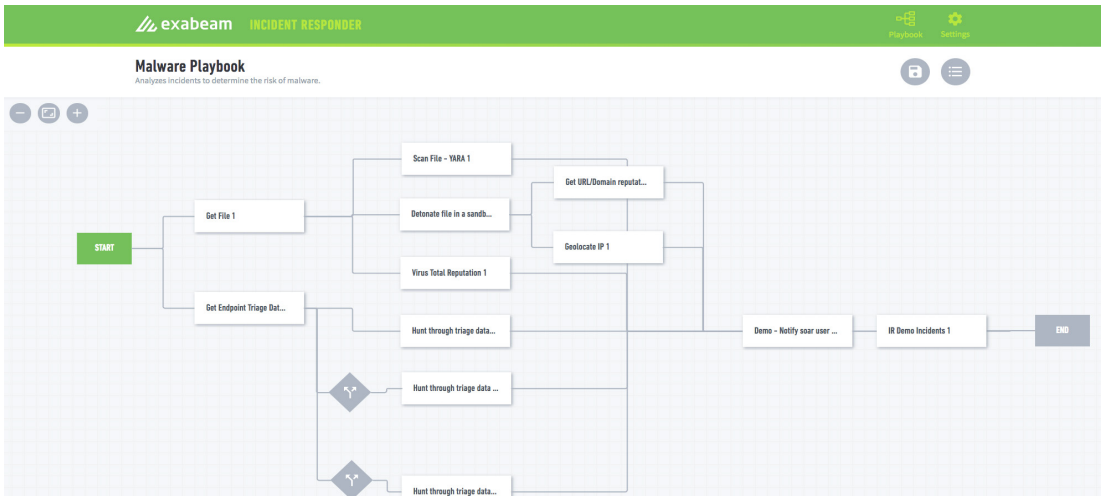
The combination of incident management and security orchestration yields a powerful platform upon which to build incident response automation. Yet true productivity gains come from the addition of another key feature to EIR—response playbooks.

## RESPONSE PLAYBOOKS

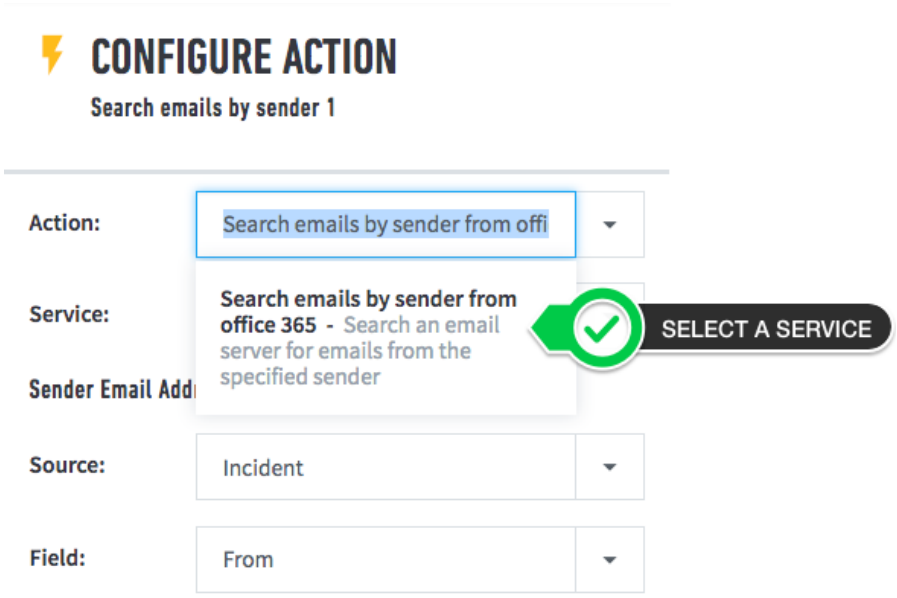
You may be well aware that seasoned security analysts (often called ”ninjas” due to their finely honed skill set) provide a disproportionately high amount of value in present-day SOCs. Such level 3 and 4 analysts are usually the most familiar with the tools used by the organization and they’ve had greater exposure to a wider variety of threats over time. They’re typically responsible for leveraging their experience to create best practices, as well as response plans that codify standard operating procedures for handling specific threats. Such step-based response plans, or playbooks, help train junior staffers to learn how to effectively investigate, contain, and mitigate disparate threats.

Further, present-day IR automation solutions make use of response playbooks to standardize and expedite procedures. An IR automation playbook codifies workflows by coupling actions with logic, then—at the push of a button—executes them over API calls.  These response playbooks can be run in a fully or semi-automated fashion, enabling organizations to easily build a 24x7x365, global security team. Without such automation, building an always-on response team can costly and difficult to coordinate due to the limits of human time and energy.

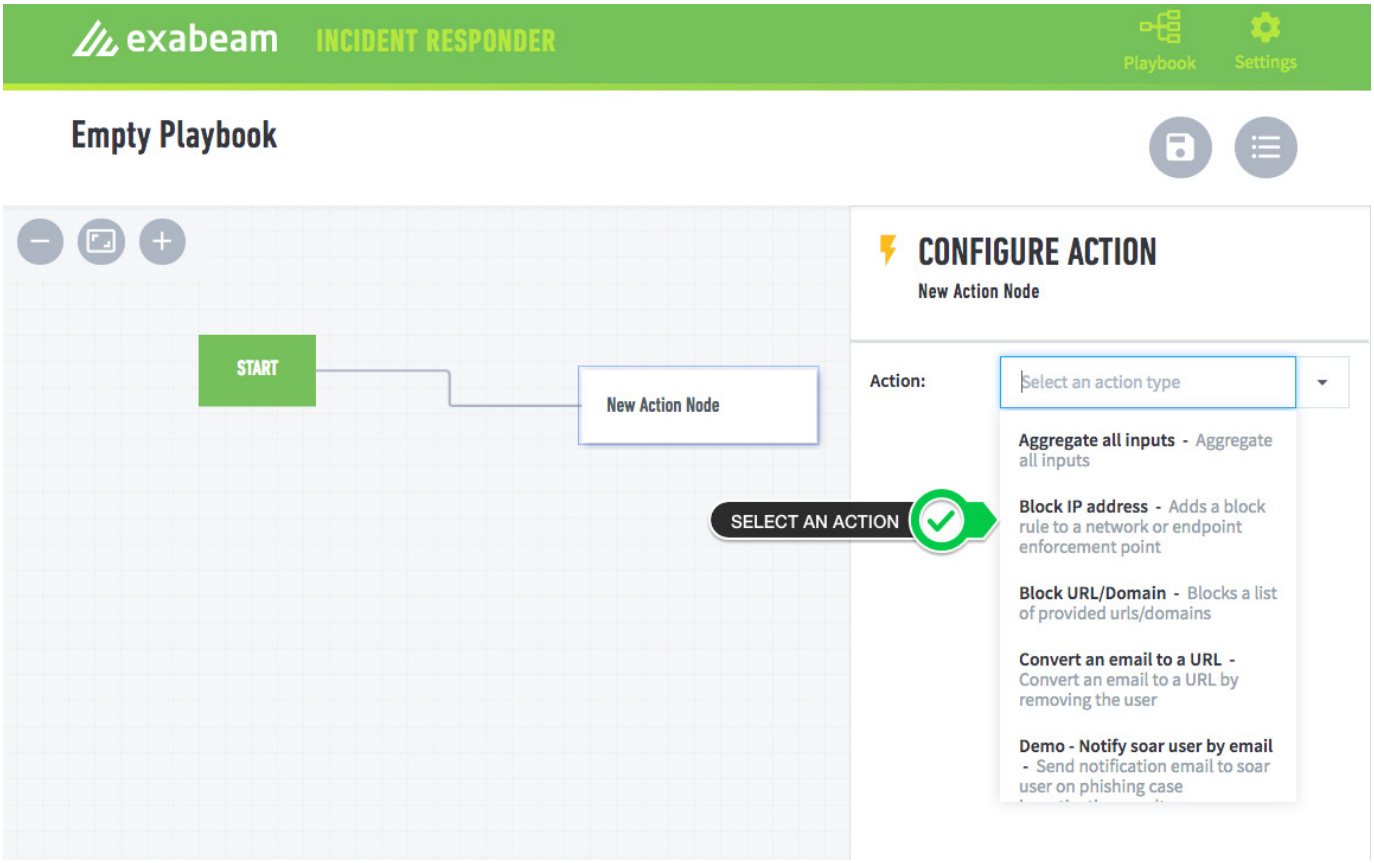
Exabeam Incident Responder ships with numerous prebuilt playbook templates—letting you and your organization quickly respond to such common threats as phishing, malware infection, data exfiltration, and more.



Within Incident Responder, its playbooks serve as templates that you can easily customize to leverage solutions already available in your environment. For each step, you only need select those systems you want to interact with. For example, if a playbook step is to poll an email server, you simply select that server from a dropdown menu.




In addition, Exabeam's Incident Responder ships with a visual playbook editor that lets you easily create your own playbooks from scratch using a point-and-click interface and drop-down menus. This user-friendly approach lets analysts of all experience levels create playbooks to help them automate tasks and boost their productivity.



## WALKING THROUGH AN AUTOMATED PHISHING INVESTIGATION PLAYBOOK

Regardless of company size or industry, Verizon's 2017 Data Breach Investigation Report reports that email-based attacks and phishing are among the top attack vectors exploited by perpetrators according. Being so ubiquitous, many SOCs have staff dedicated to identifying and responding to phishing emails.

In this section, we'll dissect an out-of-the-box, Exabeam IR playbook to learn how orchestration and automation solutions can help amplify your efficiency and improve response KPIs. (Typically this playbook would be run in a semi- or fully automated fashion, then be followed up using a containment playbook.)

We'll then review the results a major public university achieved by implementing the playbook. The goal is to help organizations investigate suspicious emails, to assess whether they're malicious, and how to automatically determine who else received the same emails.

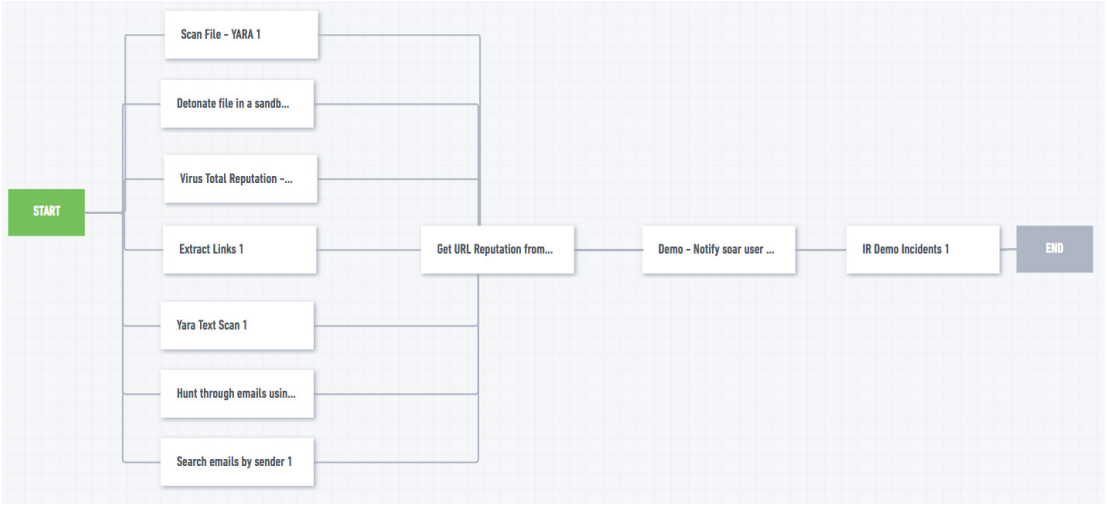



Figure 7. An Overview of the Incidnet Responder's playbook template.

When run, the playbook automatically provides key pieces of information you can use in your investigation, or which you can use in other playbooks to contain the threat (i.e., taking remediative action to prevent future attacks). Once run, results from each playbook action are displayed on separate cards, such that you can quickly browse them in a well-organized fashion.

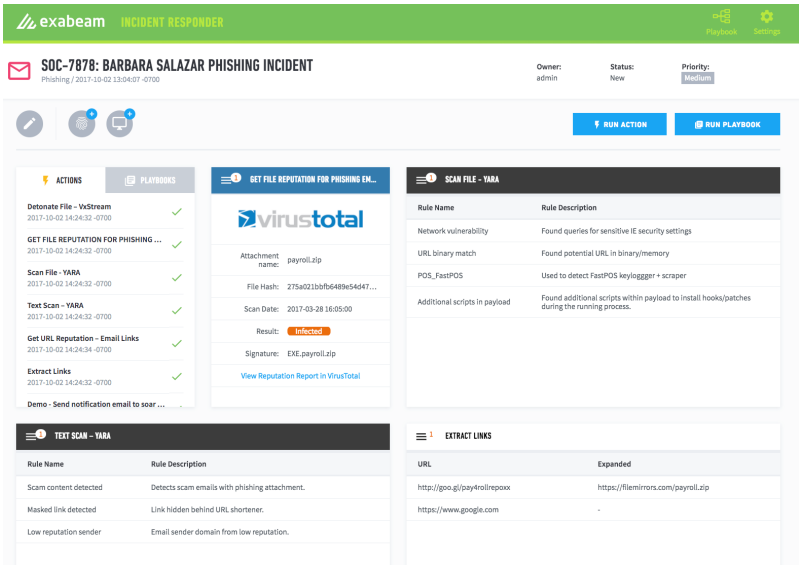


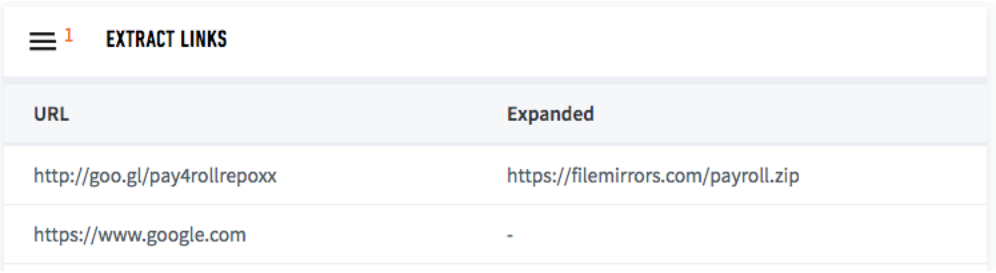

Figure 8 - Playbook information displayed on cards in the workbench.

EIR's phishing playbook functions as follows:

1. **Email-Based Incident Ingestion** – Many organizations already maintain a phishing email alias, to which employees are trained to forward suspicious emails. Incident Responder is unique in its ability to ingest emails, parse them, then automatically transform them into incidents. This lets IR teams seamlessly hook into existing workflows and phishing response processes.

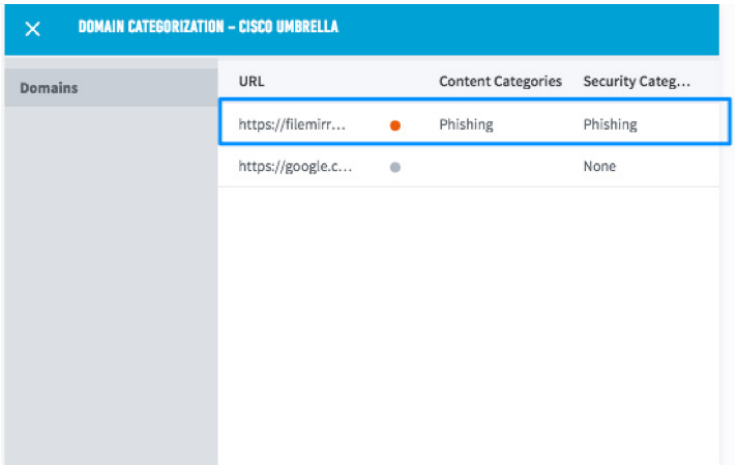
2. **Email Parsing** – EIR parses emails sent to the phishing inbox for relevant information, automatically determines the incident type, then creates an incident. For phishing events, EIR looks for hyperlinks and files that may require analysis, in addition to parsing the email subject and body text. Once parsed, all of this data can be used by other playbook actions.

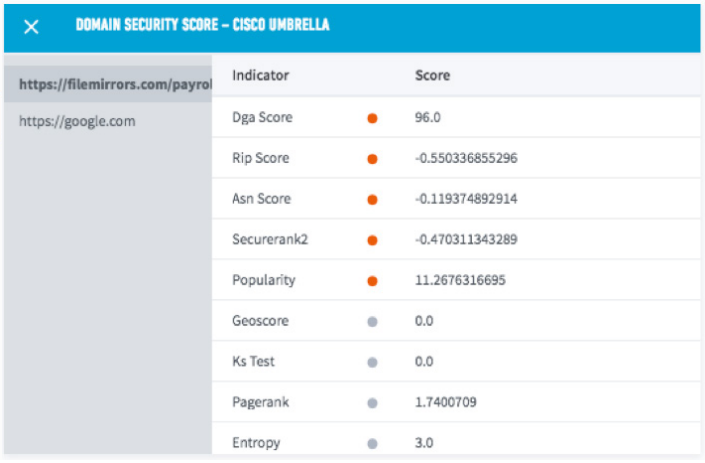
   In this example, the parser found two links—one pointing to Google and the other to `hxxp://goo.gl/pay4roll-repoxx`, which redirects traffic to a ZIP file located at `hxxp://filemirrors.com/payroll.zip`.




3. **Investigating Domains** – The next step is to gather information about the domains discovered above. This playbook is programmed to feed the results of the last step directly into a DNS reputation service (in this environment Cisco Umbrella was used).

   Shown below, the `filemirrors` domain returned potentially malicious results for both its domain categorization and domain security score. In the former, it was specifically classified in the phishing category.



4. **Indicator of Compromise (IoC) analysis using Yara** – The playbook then takes files and text associated with the suspicious email and scans them in Yara to find indicators of compromise (IoCs).

   Here, `payroll.zip` appears to be malicious; it includes a keylogger and memory scrapper. IoCs are highly valuable for subsequent containment and remediation steps, since they provide analysts with information about malware involved in a given phishing campaign and what it may attempt to do to victims.

**TEXT SCAN – YARA**

| Rule Name | Rule Description |
|---|---|
| Scam content detected | Detects scam emails with phishing attachment. |
| Masked link detected | Link hidden behind URL shortener. |
| Low reputation sender | Email sender domain from low reputation. |

**SCAN FILE - YARA**

| Rule Name | Rule Description |
|---|---|
| Network vulnerability | Found queries for sensitive IE security settings |
| URL binary match | Found potential URL in binary/memory |
| POS_FastPOS | Used to detect FastPOS keyloggger + scraper |
| Additional scripts in payload | Found additional scripts within payload to install hooks/patches during the running process. |

5. **Obtaining file reputation** – This playbook also leverages VirusTotal to assess the file reputation of the attachment. The resulting score can be used by future actions and playbooks.

**GET FILE REPUTATION FOR PHISHING EM...**

virustotal

| | |
|---|---|
| Attachment name: | payroll.zip |
| File Hash: | 275a021bbfb6489e54d47... |
| Scan Date: | 2017-03-28 16:05:00 |
| Result: | Infected |
| Signature: | EXE.payroll.zip |

View Reputation Report in VirusTotal

6. **Behavioral Sandbox** – Next, the playbook detonates the suspicious file in a sandbox to observe its behavior, obtain a threat score, and identify any unusual or unexpected network connections.

**BEHAVIORAL INDICATORS – VXSTREAM**

| Name | Description |
|---|---|
| Detected Emerging Threats Alert | 100 |
| Sample was identified as malicious by a large number of Antivirus engines | 100 |
| Sample was identified as malicious by at least one Antivirus Engine | 80 |
| All indicators are available only in the private webservice or standalone version | 80 |
| Sends UDP traffic | 25 |
| Found potential IP address in binary/memory | 25 |
| Malicious artifacts seen in context of a contacted host | 25 |

**DETONATE FILE – VXSTREAM**

PAYLOAD SECURITY

| | |
|---|---|
| Sample Type: | HTML document, ASCII te... |
| Threat Score: | 99 |
| Attachment Name: | payroll.zip |
| SHA-256: | 9335e1404d1aa005456a8... |
| Sample Size: | 7960 Bytes |

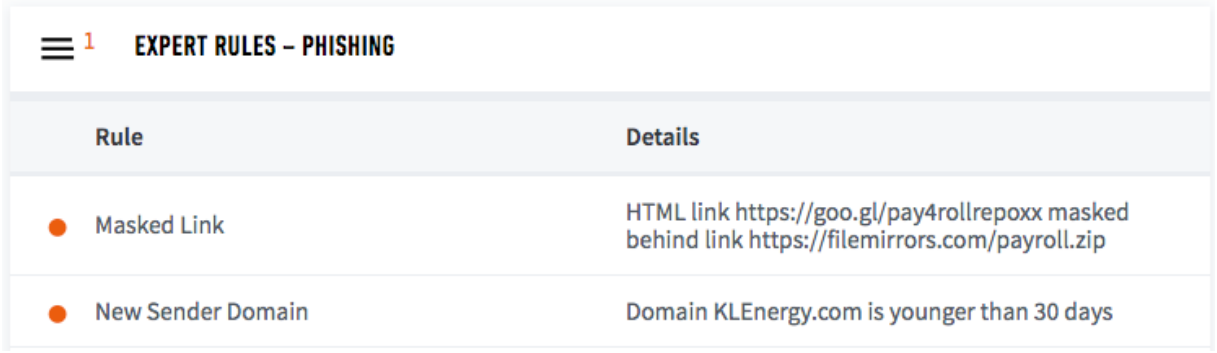
View Detonation Report in VxStream

**EXTRACTED NETWORK INDICATORS – VXS...**

| Type | Network Resource |
|---|---|
| TCP | 192.229.233.16:80 |
| TCP | 205.196.123.9:80 |
| UDP | 84.200.69.80:53 |

7. **Applying Security Expertise** – Incident Responder playbooks leverage the expertise of Exabeam's security research team to create expert rules. These identify potential signals of malicious or suspicious activity, including such items as masked links and algorithmically generated domains.

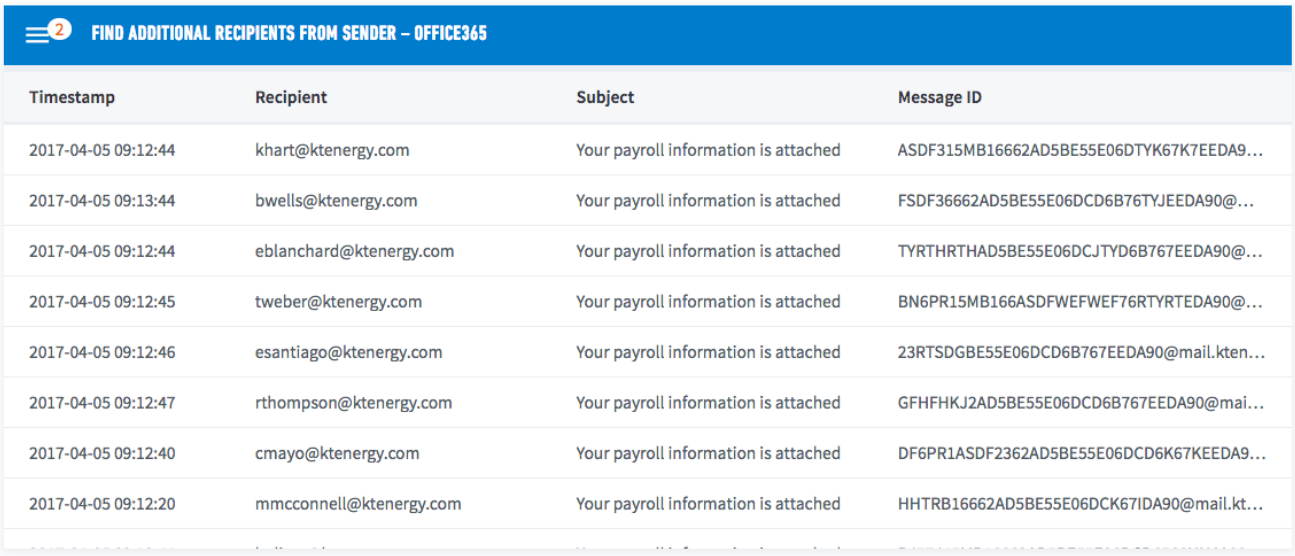
   In this playbook the emails and their contents are scrutinized using these expert rules and, when triggered, the results are presented in the UI.



1 EXPERT RULES – PHISHING

| Rule | Details |
|---|---|
| Masked Link | HTML link https://goo.gl/pay4rollrepoxx masked behind link https://filemirrors.com/payroll.zip |
| New Sender Domain | Domain KLEnergy.com is younger than 30 days |

8. **Finding Additional Recipients** – Should the investigation playbook determine that the suspicious email was indeed a phishing email, it kicks off an additional step to determine who else in your organization received the same email by way of a quick search of Office 365 data.



2 FIND ADDITIONAL RECIPIENTS FROM SENDER – OFFICE365

| Timestamp | Recipient | Subject | Message ID |
|---|---|---|---|
| 2017-04-05 09:12:44 | khart@ktenergy.com | Your payroll information is attached | ASDF315MB16662AD5BE55E06DTYK67K7EEDA9… |
| 2017-04-05 09:13:44 | bwells@ktenergy.com | Your payroll information is attached | FSDF36662AD5BE55E06DCD6B76TYJEEDA90@… |
| 2017-04-05 09:12:44 | eblanchard@ktenergy.com | Your payroll information is attached | TYRTHRTHAD5BE55E06DCJTYD6B767EEDA90@… |
| 2017-04-05 09:12:45 | tweber@ktenergy.com | Your payroll information is attached | BN6PR15MB166ASDFWEFWEF76RTYRTEDA90@… |
| 2017-04-05 09:12:46 | esantiago@ktenergy.com | Your payroll information is attached | 23RTSDGBE55E06DCD6B767EEDA90@mail.kten… |
| 2017-04-05 09:12:47 | rthompson@ktenergy.com | Your payroll information is attached | GFHFHKJ2AD5BE55E06DCD6B767EEDA90@mai… |
| 2017-04-05 09:12:40 | cmayo@ktenergy.com | Your payroll information is attached | DF6PR1ASDF2362AD5BE55E06DCD6K67KEEDA9… |
| 2017-04-05 09:12:20 | mmcconnell@ktenergy.com | Your payroll information is attached | HHTRB16662AD5BE55E06DCK67IDA90@mail.kt… |

9. **Notifying Stakeholders** - The final playbook step is to summarize the results for interested parties—including the victim or other stakeholders. At this point, the investigation is complete. You can decide to run additional playbooks as needed for the purpose of remediation or containment.

## THE IMPACT OF RESPONSE AUTOMATION

Organizations that leverage orchestration and automation solutions as part of their response practices are able to increase response capacity, overcome staffing challenges, and streamline their SOC operations. To understand the impact of such tools, we'll look at the experience of a university that implemented Exabeam Incident Responder to tackle their phishing problem.

### THE CHALLENGE

A major, US-based public university was being bombarded by roughly 700,000 phishing emails per month. Originally the institution implemented a best-of-class email security solution to help detect and block such email. While it was helpful, the university quickly found it was unable to catch 100% of the phishing attempts launched at their faculty and student body.

The emails that weren't blocked by the email security solution were forwarded to a special phishing email box. From there they were manually turned into incidents for review by a full time security team member solely tasked with investigating phishing emails. That person was only able to investigate about 60% of the incidents received in any given month.

### THE SOLUTION

The university implemented Exabeam Incident Responder, using the aforementioned phishing playbook in their SOC workflow. This brought much needed automation to its phishing email investigation.

### THE RESULT

By deploying EIR's automated response, the university was able lower the dedicated email investigation headcount by half. The productivity gain now enabled it to investigate and respond to 100% of the phishing incidents, thereby eliminating the possibility of overlooking a high-risk incident due to capacity issues. Additionally, this freed up time for the SOC team to tackle non-phishing projects.

## CONCLUSION

It's often the case today that SOC analysts are never able to address all the alerts being thrown at them. But by using security orchestration and automation tools, organizations can greatly increase their ability to investigate incidents more quickly and more thoroughly. Orchestration and playbook-based workflow automation provides them with the possibility of addressing their entire mountain of work, while potentially requiring fewer man-hours to do so. This reduces the chance that a high risk alert or incident slips through the cracks.

IR automation enables SOCs to do more with less. It also means senior analysts can codify response best practices into playbooks for junior analysts to run. The result is a more consistent response, along with the ability to hire additional junior talent to fill open SOC positions.

For more information, please visit http://www.exabeam.com, or send email to info@exabeam.com.