ESG Enterprise Strategy Group | Getting to the bigger truth.™

Technical Review

Exabeam Security Management Platform

Date: May 2019 **Author:** Tony Palmer, Senior Validation Analyst; Alex Arcilla, Validation Analyst

Abstract

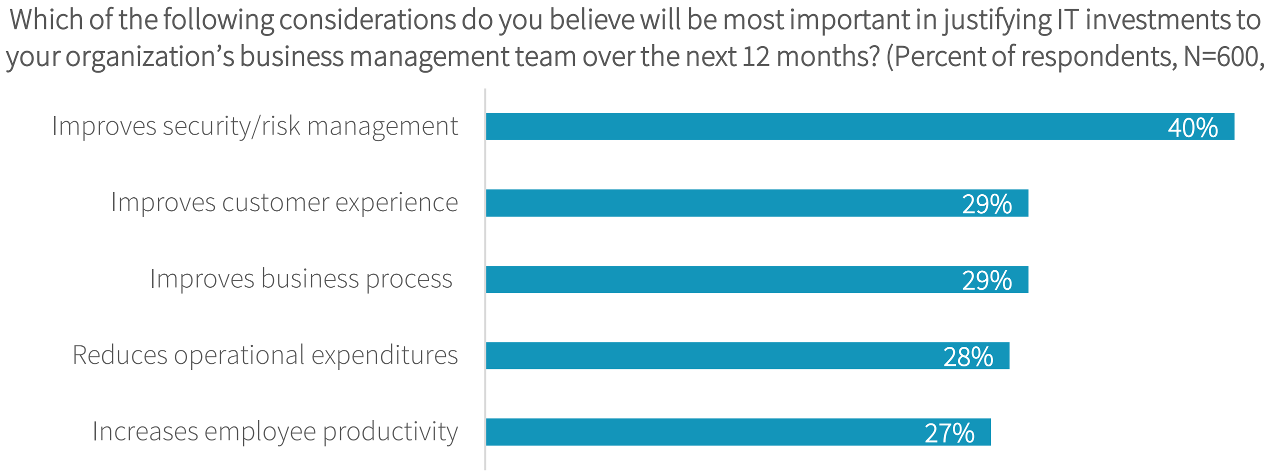
This ESG Technical Review documents hands-on testing of the Exabeam Security Management Platform (SMP), Exabeam's modern security information and event management (SIEM) platform. We focus on how Exabeam Cloud Security Services, Data Lake, Advanced Analytics, Entity Analytics, Incident Responder and Case Manager empower security operations center (SOC) and incident response (IR) analysts to be timelier and more effective in responding to threats and attacks.

The Challenges

In ESG's *2019 Technology Spending Intentions Survey*, 40% of respondents noted that improving security and risk management capabilities is one of the considerations they believe will be most important in justifying IT investments during the year (see Figure 1).[1] Fifty-eight percent of respondents stated that they will increase their cybersecurity spending in 2019 over what they spent in 2018, showing that this area continues to be top of mind for organizations in light of ongoing high-profile data breaches and ransomware attacks.

One challenge that continues to plague IT organizations is overcoming the lack of in-house cybersecurity skills. ESG research reveals that 53% of respondents note this as one of their areas with significant skill gaps. With the ever-growing amount of data that SOC and IT personnel must analyze to uncover and resolve threats quickly, keeping skill sets up to date remains difficult. The skills gap threatens the ability of organizations to implement budgeted cybersecurity projects, and organizations will need to consider investing in developing skills and seeking products that improve operational efficiency.

Figure 1. Most Important Considerations in Justifying IT Investments—Top Five Responses



Source: Enterprise Strategy Group

To address this skills shortage, it is critical that an organization have tools and processes that allow it to bring new SOC and IR analysts onboard quickly, with less training time. This requires tools that will correlate activity across the attack surface—covering endpoints, networks, cloud services, and users—to detect threats, allowing analysts to focus on threat hunting,

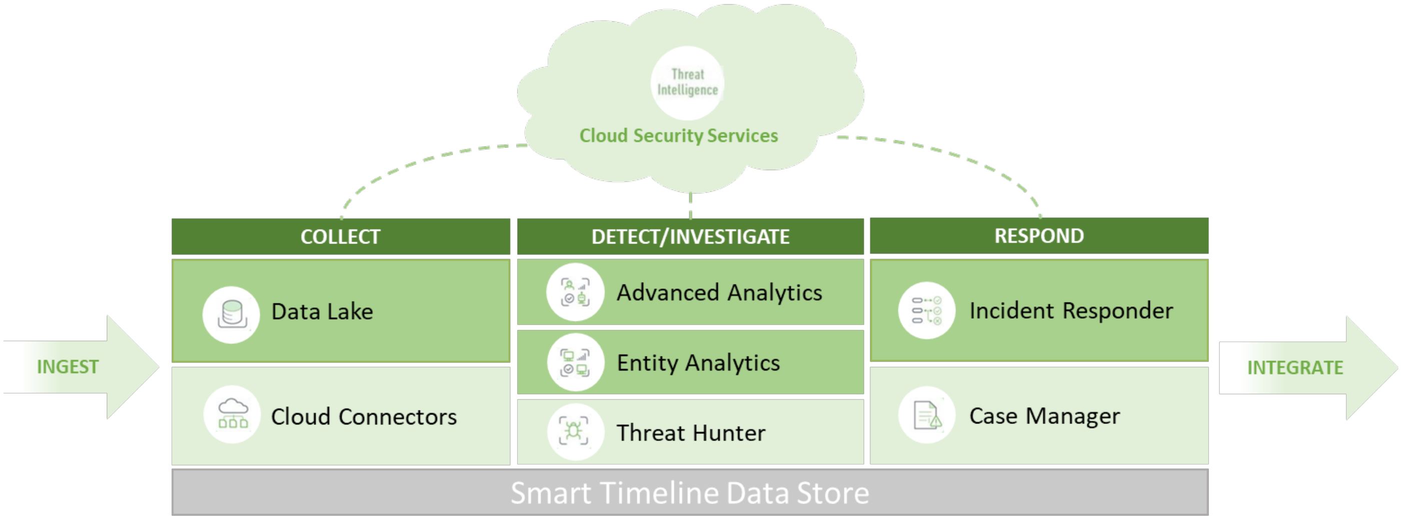
[1] Source: ESG Research Report, *2019 Technology Spending Intentions Survey*, February 2019. All ESG research references and charts in this technical review have been taken from this research report unless otherwise noted.

identification, and resolution. Additionally, these tools will incorporate security analytics that will educate analysts on recurring threats and assist in automation through playbooks for timelier incident response.

The Solution: Exabeam Security Management Platform

The Exabeam platform is built on a modern, scalable, big data infrastructure, and uses data science, machine learning, and behavioral modeling for advanced analytics designed for comprehensive insider and entity threat detection. Exabeam Advanced Analytics and Entity Analytics provide insider threat detection, tracking anomalous behavior and lateral movements within an organization while monitoring cloud services, machines, devices, and IoT assets. Automated incident response and case management are employed to enable teams to respond to security incidents rapidly and with less effort. The foundation of the platform is the Exabeam security Data Lake designed to store all event logs at a predictable flat price. The Exabeam enterprise SIEM solution is designed to allow security teams to focus on quickly identifying and responding to security threats rather than manually analyzing the sea of data logs their environment generates. Figure 2 shows how these tools fit into Exabeam's overall solution.

Figure 2. Exabeam Security Management Platform



Source: Enterprise Strategy Group

Organizations are now collecting data generated by endpoint, network, IoT, and security devices from both internal networks and the cloud. The user and application activity can result in petabytes to be processed. Organizations may incur increased log collection, storage, indexing, and search costs unexpectedly. To address the ever-growing amount of data that challenges today's organizations, Exabeam offers its Data Lake. Exabeam designed Data Lake to scale. Built on ElasticSearch, an open source stack of software tools, Data Lake scales by simply adding nodes. And instead of charging by GB of data (storage capacity), Exabeam charges by user to address cost issues. Thus, the customer is free to leverage any amount of data for ongoing security monitoring, enabling analysts to stay ahead of potential threats.

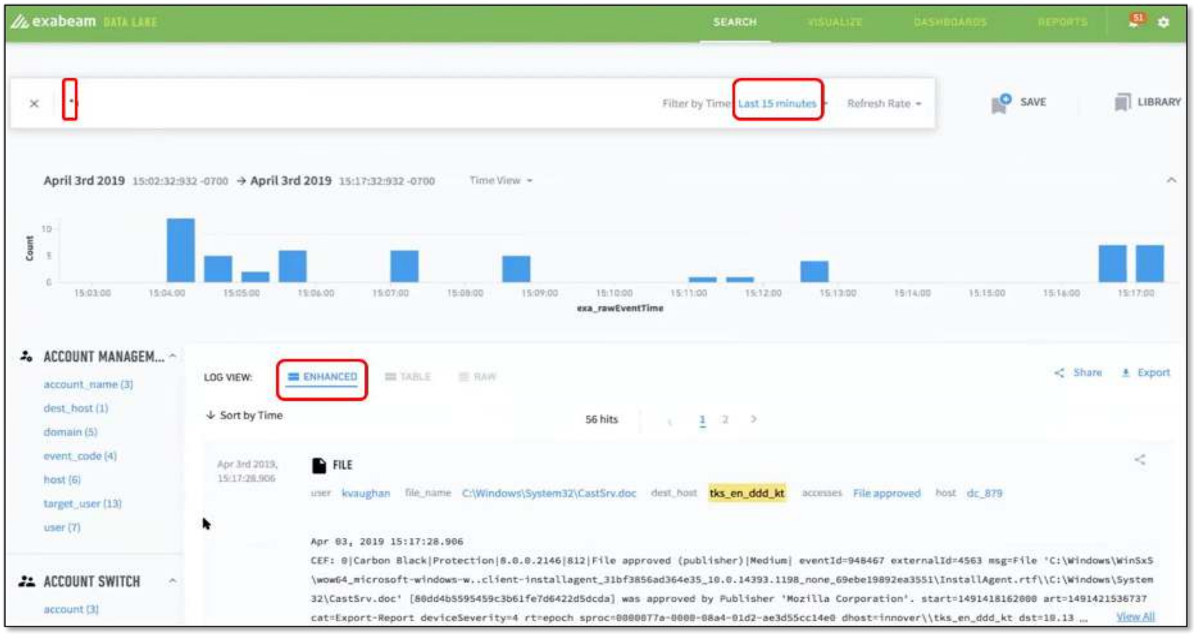
The Advanced Analytics and Entity Analytics modules, along with Incident Responder and Case Manager, provide additional security breach detection and response capabilities. The UEBA component ingests data collected by the Data Lake and constructs Smart Timelines based on what it deems normal and abnormal user activity. Smart Timelines are designed to automatically combine sequence, behavior, identity, and scope into a preprocessed object that can be instantly retrieved whenever needed—when threat hunting, for example. The underlying rules and models are continuously trained as the platform ingests more data. Exabeam offers these analytics to decrease the manual work done by security analysts to construct such timelines today, thus decreasing the time to respond to potential security breaches.

Case Manager and Incident Responder allow an organization to orchestrate and automate the appropriate responses to security-related events. Usually, security analysts must prioritize responses because they are unable to address all events in a timely manner. With Case Manager and Incident Responder, analysts can create automated workflows to address recurring incidents. As a result, analysts can decrease response times as well as manual errors.

Data Lake

ESG first reviewed the capabilities of the Data Lake. We navigated to the screen as shown in Figure 3. An analyst begins a session by viewing the summary screen that displays the number of logs collected in discrete time intervals.

Figure 3. The Exabeam Data Lake



Apr 3rd 2019, 15:17:28.906

FILE

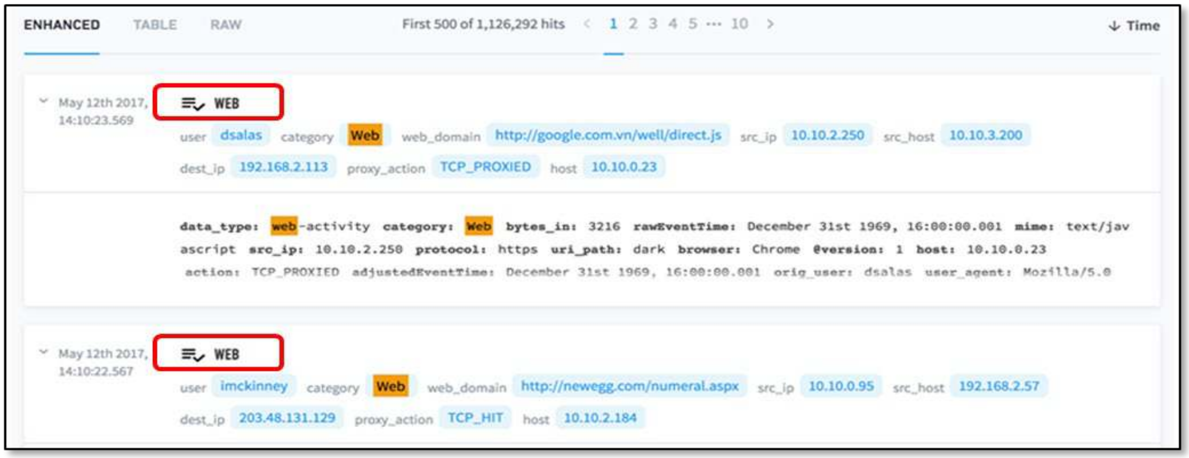
user kvaughan file_name C:\Windows\System32\CastSrv.doc dest_host tks_en_ddd_kt accesses File approved host dc_879

```
Apr 03, 2019 15:17:28.906
CEF: 0|Carbon Black|Protection|8.0.0.2146|812|File approved (publisher)|Medium| eventId=948467 externalId=4563 msg=File 'C:\Windows\WinSxS
\wow64_microsoft-windows-w..client-installagent_31bf3856ad364e35_10.0.14393.1198_none_69ebe19892ea3551\InstallAgent.rtf\\C:\Windows\System
32\CastSrv.doc' [80dd4b5595459c3b61fe7d6422d5dcda] was approved by Publisher 'Mozilla Corporation'. start=1491418162000 art=1491421536737
cat=Export-Report deviceSeverity=4 rt=epoch sproc=0000077a-0000-08a4-01d2-ae3d55cc14e0 dhost=innover\\tks_en_ddd_kt dst=10.13 ...
```

In the search bar at the top of the screen, we typed an asterisk to see all logs that had been collected in the last 15 minutes. The number of logs is noted and reported every 30 seconds. The analyst could choose to see log counts over a longer period of time by clicking on the down arrow of the menu to the right of the search bar.

On the left-hand side of the screen, the Data Lake lists logs based on category, along with the tags associated with them and associated counts. To use a log view that highlights security-relevant data from individual log details, we clicked on the *Enhanced* tab. Each log shows the specific value noted for each tag. ESG Lab then clicked on the *Web* filter to limit search results to web proxy logs. The search results are shown in Figure 4. We saw those logs that contained the term “Web” within their detailed records.

Figure 4. Enhanced View of Logs Generated by Search on “Web”



May 12th 2017, 14:10:23.569 WEB

user dsalas category Web web_domain http://google.com.vn/well/direct.js src_ip 10.10.2.250 src_host 10.10.3.200 dest_ip 192.168.2.113 proxy_action TCP_PROXIED host 10.10.0.23

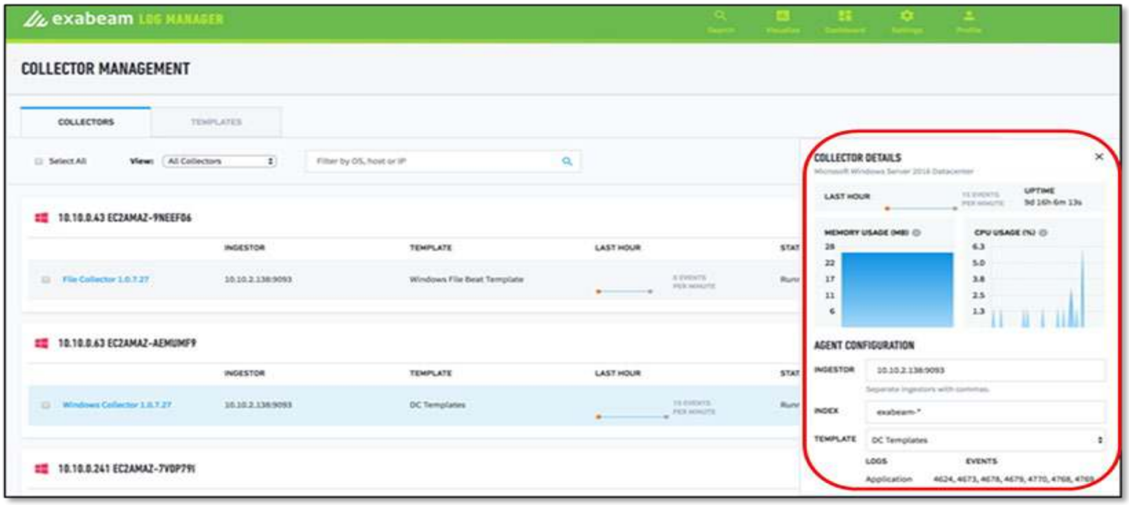
```
data_type: web-activity category: Web bytes_in: 3216 rawEventTime: December 31st 1969, 16:00:00.001 mime: text/jav
ascript src_ip: 10.10.2.250 protocol: https uri_path: dark browser: Chrome @version: 1 host: 10.10.0.23
 action: TCP_PROXIED adjustedEventTime: December 31st 1969, 16:00:00.001 orig_user: dsalas user_agent: Mozilla/5.0
```

May 12th 2017, 14:10:22.567 WEB

user imckinney category Web web_domain http://newegg.com/numeral.aspx src_ip 10.10.0.95 src_host 192.168.2.57 dest_ip 203.48.131.129 proxy_action TCP_HIT host 10.10.2.184

ESG then proceeded to examine the Collector Management screen in the Data Lake, as shown in Figure 5. We clicked on one collector and viewed details associated with it. Analysts can create custom data collectors or edit them in bulk using Beats or Exabeam-defined templates. ESG clicked on one collector related to logs from *Microsoft Windows Server 2016 Datacenter* to view its attributes. Collector attributes included CPU and memory usage and configuration details, such as tracked events and number of events collected in a given time period. Viewing these attributes can help analysts monitor how active certain collectors are and determine the health of the endpoint and the logs being collected.

Figure 5. Collector Management Screen



10.10.0.43 EC2AMAZ-9NEEF06

	INGESTOR	TEMPLATE	LAST HOUR	STAT
File Collector 1.0.7.27	10.10.2.138:9093	Windows File Beat Template	8 EVENTS PER MINUTE	Runr

10.10.0.63 EC2AMAZ-AEMUMF9

	INGESTOR	TEMPLATE	LAST HOUR	STAT
Windows Collector 1.0.7.27	10.10.2.138:9093	DC Templates	15 EVENTS PER MINUTE	Runr

10.10.0.241 EC2AMAZ-7VDP79I

COLLECTOR DETAILS
Microsoft Windows Server 2016 Datacenter

LAST HOUR 15 EVENTS PER MINUTE
UPTIME 9d 16h 6m 13s

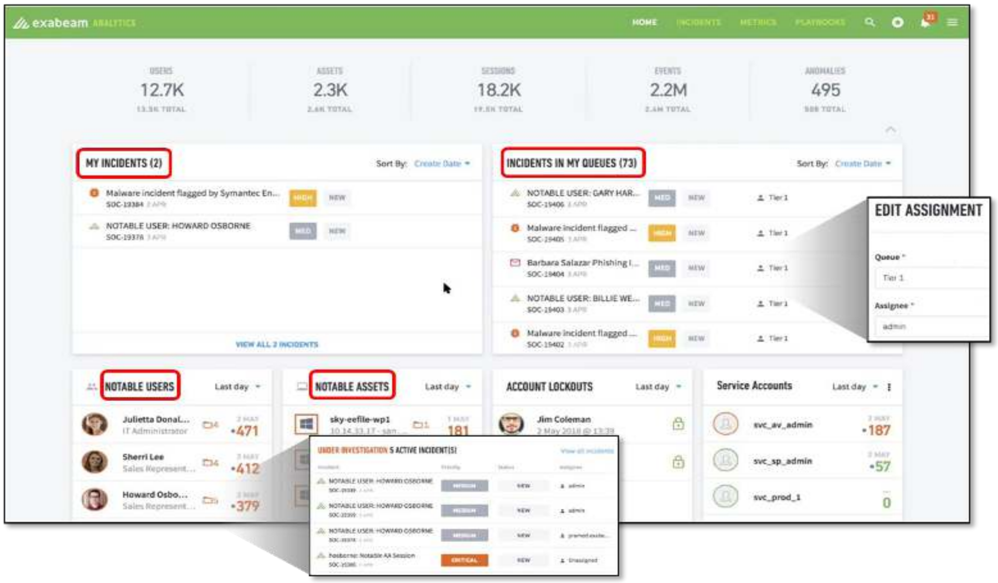
AGENT CONFIGURATION
INGESTOR 10.10.2.138:9093
Separate ingestors with commas.
INDEX exabeam-*
TEMPLATE DC Templates

LOGS	EVENTS
Application	4624, 4673, 4678, 4679, 4770, 4768, 4769

Advanced Analytics and Entity Analytics

ESG next reviewed the capabilities of Exabeam’s analytics modules. We navigated to the screen shown in Figure 6. Exabeam’s dashboard displays summary statistics across the top, including users, assets, sessions, events, and cumulative count for anomalies. We noted that the analyst can create user watchlists to monitor (e.g., account lockouts). Other watchlists can focus on listing users associated with events, such as those infected with malware. The analyst can leverage user-specific watchlists to isolate sources of potential security threats. The tool will assign a risk score to each user and entity that denotes how risky an individual’s activity is to the organization. Assigning risk scores allows the analyst to identify and monitor potential security breaches more quickly.

Figure 6. The Exabeam Analytics Dashboard



MY INCIDENTS (2) Sort By: Create Date

- Malware incident flagged by Symantec En... SOC-19384 HIGH NEW
- NOTABLE USER: HOWARD OSBORNE SOC-19378 MED NEW

VIEW ALL 2 INCIDENTS

INCIDENTS IN MY QUEUES (73) Sort By: Create Date

- NOTABLE USER: GARY HAR... SOC-19406 MED NEW Tier 1
- Malware incident flagged ... SOC-19405 HIGH NEW Tier 1
- Barbara Salazar Phishing I... SOC-19404 MED NEW Tier 1
- NOTABLE USER: BILLIE WE... SOC-19403 MED NEW Tier 1
- Malware incident flagged ... SOC-19402 HIGH NEW Tier 1

EDIT ASSIGNMENT
Queue *: Tier 1
Assignee *: admin

NOTABLE USERS: Julietta Donal... IT Administrator 471; Sherri Lee Sales Represent... 412; Howard Osbo... Sales Represent... 379

NOTABLE ASSETS: sky-eefile-wp1 10.14.33.17 - san... 181

UNDER INVESTIGATION 5 ACTIVE INCIDENT(S)

- NOTABLE USER: HOWARD OSBORNE MEDIUM NEW admin
- NOTABLE USER: HOWARD OSBORNE MEDIUM NEW admin
- NOTABLE USER: HOWARD OSBORNE MEDIUM NEW
- hosborne: Notable AA Session CRITICAL NEW Unassigned

ACCOUNT LOCKOUTS: Jim Coleman 2 May 2018 @ 13:39

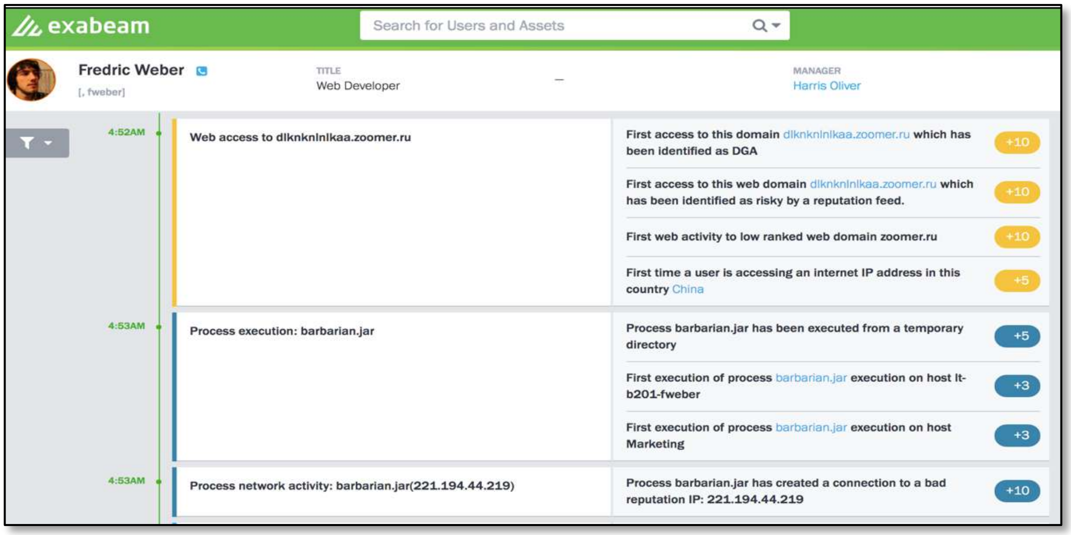
Service Accounts: svc_av_admin 187; svc_sp_admin 57; svc_prod_1 0

ESG also saw that Exabeam updated this dashboard with two cards named “My Incidents” and “Incidents In My Queues.” These cards display data from Case Manager to list out those cases that are of highest priority to address from both an individual analyst and analyst team perspective. An individual can also edit a case assigned to an individual by clicking on the person icon next to the incidents in the “Incidents In My Queue” card.

The dashboard also highlights the results of its Advanced and Entity Analytics in the “Notable Users” and Notable Assets” cards. Exabeam escalates these results based on a user or entity’s risk score crossing a predefined risk threshold, indicating it may be involved in a security incident. Clicking on the file icon next to each source on these cards, ESG saw all incidents related to the source, enabling an analyst to further assess the source’s security risk.

Using its Smart Timeline technology, Advanced Analytics will stitch together all alerts and events involved in a security incident into a machine-built incident timeline. For an analyst, this saves the time involved in gathering evidence and assembling it into a timeline and allows her to focus more on higher value tasks like interpreting the results and responding to the incident.

Figure 7. Smart Timeline of an Incident including Proxy and Process Logs for a Single User



Fredric Weber [, fweber]
TITLE Web Developer
MANAGER Harris Oliver

4:52AM Web access to dlknknlnlkaa.zoomer.ru

- First access to this domain dlknknlnlkaa.zoomer.ru which has been identified as DGA +10
- First access to this web domain dlknknlnlkaa.zoomer.ru which has been identified as risky by a reputation feed. +10
- First web activity to low ranked web domain zoomer.ru +10
- First time a user is accessing an internet IP address in this country China +5

4:53AM Process execution: barbarian.jar

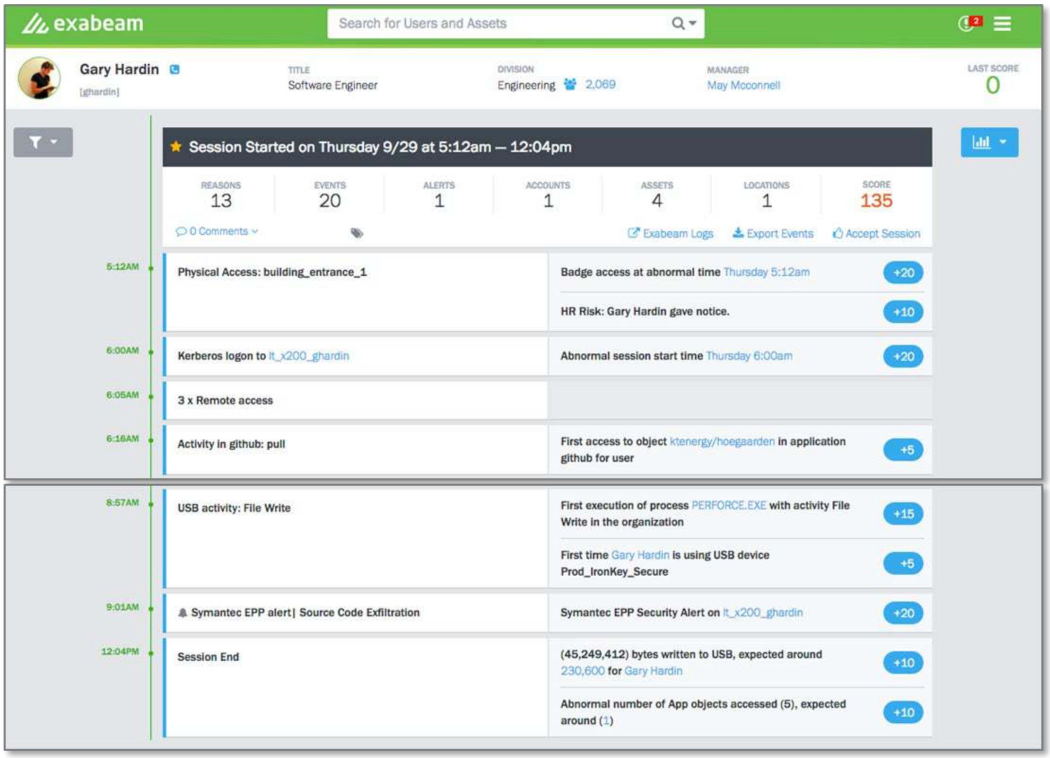
- Process barbarian.jar has been executed from a temporary directory +5
- First execution of process barbarian.jar execution on host lt-b201-fweber +3
- First execution of process barbarian.jar execution on host Marketing +3

4:53AM Process network activity: barbarian.jar(221.194.44.219)

- Process barbarian.jar has created a connection to a bad reputation IP: 221.194.44.219 +10

In addition to the example above, Advanced Analytics includes built-in content for detecting insider threat activity, i.e., an employee purposely attempting to exfiltrate sensitive information. Figure 8 shows a timeline for our user, *Frederic Weber*. Again, the timeline leverages the Smart Timeline technology to combine results from the Advanced and Entity Analytics, lateral movement tracking (tracing potential attacks as they occur over time), and risks associated with these events for an individual user. ESG noted that this timeline construct can increase analyst productivity when investigating a specific user, rather than using multiple sources (e.g., spreadsheets of incidents, log files, and IP addresses) to find these incidents and correlating them to assess an individual's security risk to the organization.

Figure 8. Insider Threat Session Timeline



Gary Hardin
[ghardin]

TITLE: Software Engineer
DIVISION: Engineering 2,069
MANAGER: May Mcconnell
LAST SCORE: 0

★ Session Started on Thursday 9/29 at 5:12am — 12:04pm

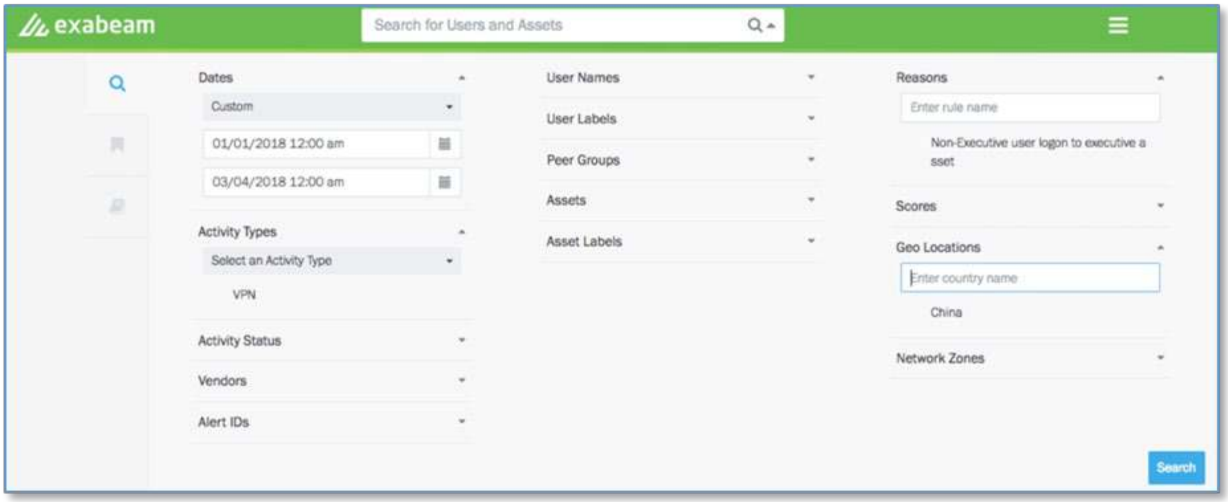
REASONS	EVENTS	ALERTS	ACCOUNTS	ASSETS	LOCATIONS	SCORE
13	20	1	1	4	1	135

5:12AM	Physical Access: building_entrance_1	Badge access at abnormal time Thursday 5:12am	+20
		HR Risk: Gary Hardin gave notice.	+10
6:00AM	Kerberos logon to lt_x200_ghardin	Abnormal session start time Thursday 6:00am	+20
6:05AM	3 x Remote access		
6:16AM	Activity in github: pull	First access to object ktenergy/hoegaarden in application github for user	+5
8:57AM	USB activity: File Write	First execution of process PERFORCE.EXE with activity File Write in the organization	+15
		First time Gary Hardin is using USB device Prod_IronKey_Secure	+5
9:01AM	Symantec EPP alert| Source Code Exfiltration	Symantec EPP Security Alert on lt_x200_ghardin	+20
12:04PM	Session End	(45,249,412) bytes written to USB, expected around 230,600 for Gary Hardin	+10
		Abnormal number of App objects accessed (5), expected around (1)	+10

Threat Hunter

Threat Hunter allows analysts to create sophisticated search queries without learning proprietary search query languages. It generates Smart Timelines as search results instead of discrete log events. This greatly improves analyst threat hunting speed and makes threat hunting accessible for junior analysts (see Figure 9).

Figure 9. Threat Hunter



Dates: Custom, 01/01/2018 12:00 am – 03/04/2018 12:00 am

Activity Types: Select an Activity Type – VPN

Activity Status

Vendors

Alert IDs

User Names

User Labels

Peer Groups

Assets

Asset Labels

Reasons: Enter rule name – Non-Executive user logon to executive asset

Scores

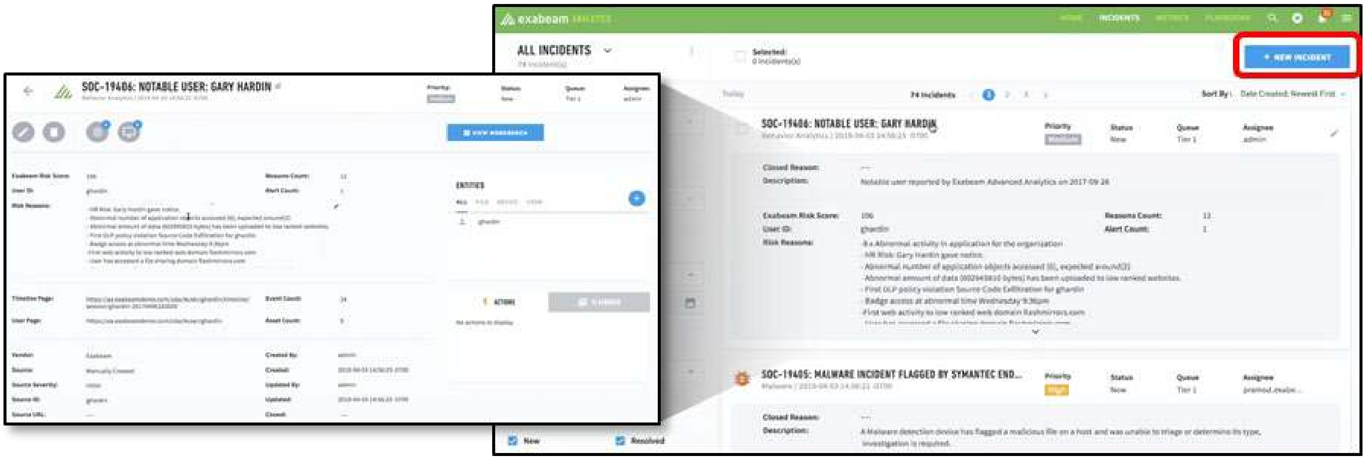
Geo Locations: Enter country name – China

Network Zones

Case Manager and Incident Responder

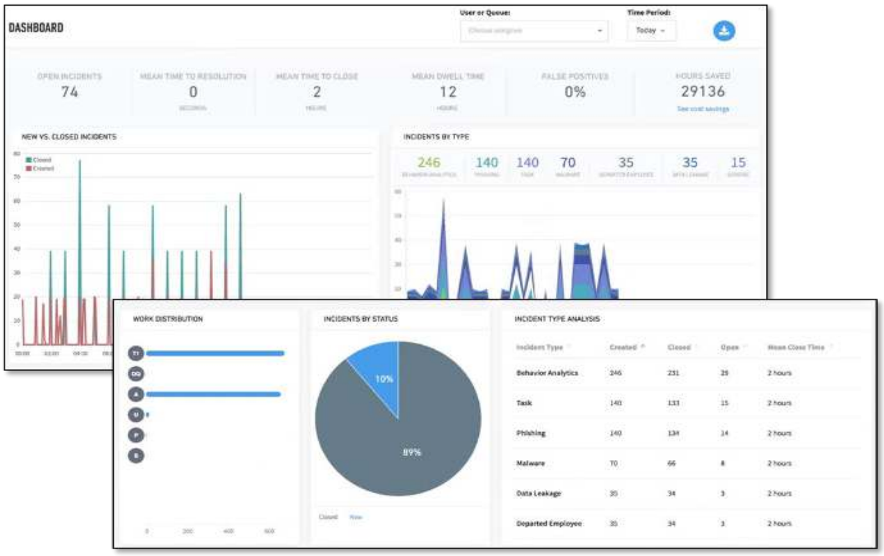
Finally, ESG reviewed the capabilities of Case Manager and Incident Responder. Exabeam designed Case Manager and Incident Responder specifically to track incidents (called cases) under review and automate corrective activities should specific incidents occur, respectively. We navigated to the screen shown in Figure 10 to view a list of outstanding cases. Incidents can be pushed or pulled into Exabeam's Case Manager from many sources such as an existing SIEM, Exabeam's analytics solutions, a ticketing system, or other security products. As seen in Figure 10, the Case Manager generated a list of incidents. An analyst can also create a new incident by clicking on the ***New Incident*** button in the top right-hand corner. The tool can automatically open incidents for any notable user discovered by Advanced Analytics and Entity Analytics. Generating incidents helps the analyst to spend more time on fixing issues as opposed to creating incidents to address. An analyst can obtain specific details about an incident by double clicking on the incident title, such as the incident associated with the user *Gary Hardin*. Details include incident source, affected IP addresses, and actions taken by the tool to resolve the incident. Additionally, the analyst can view the rules used by Exabeam for the resolution.

Figure 10. Case Manager—List of Open Incidents and Individual Incident Detail



Exabeam also helps the analyst to track metrics associated with incident resolution (as shown in Figure 11). ESG navigated to the metrics home screen to view the various metrics tracking incident resolution. We noted that these metrics can help individual analysts and analyst teams to examine their performance according to parameters such as new versus closed incidents, incident type, and resolution status.

Figure 11. Metrics Related to Incident Resolution

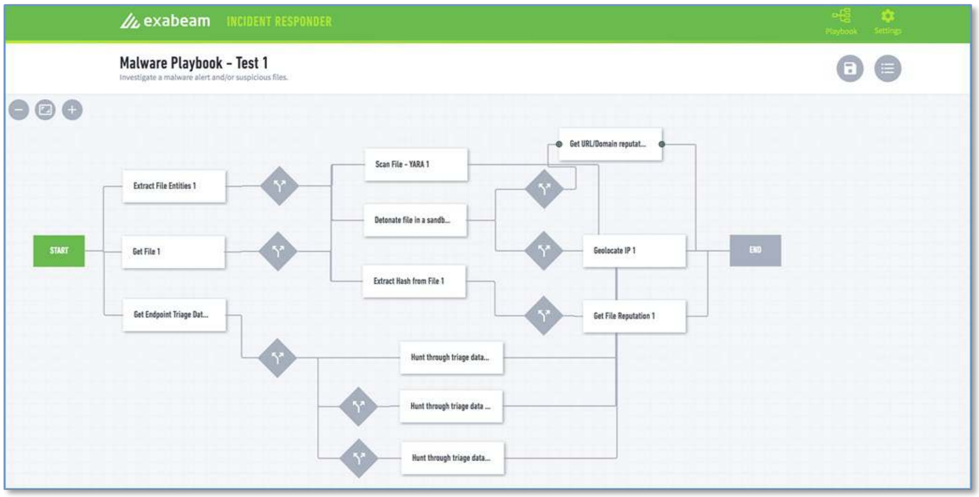


INCIDENT TYPE ANALYSIS

Incident Type	Created	Closed	Open	Mean Close Time
Behavior Analytics	246	231	25	2 hours
Task	140	133	15	2 hours
Phishing	140	134	14	2 hours
Malware	70	66	8	2 hours
Data Leakage	35	34	3	2 hours
Departed Employee	35	34	3	2 hours

Via Incident Responder, Exabeam also helps the analyst to partly or fully automate responses to incidents encountered, depending on the nature and severity of the incident. The analyst can also leverage playbooks, which are defined and automated procedures for dealing with incidents. For incidents common to many organizations, Exabeam provides prebuilt playbooks. For incidents specific to an organization, an analyst can build a playbook using Exabeam's visual playbook editor, as shown in Figure 12.

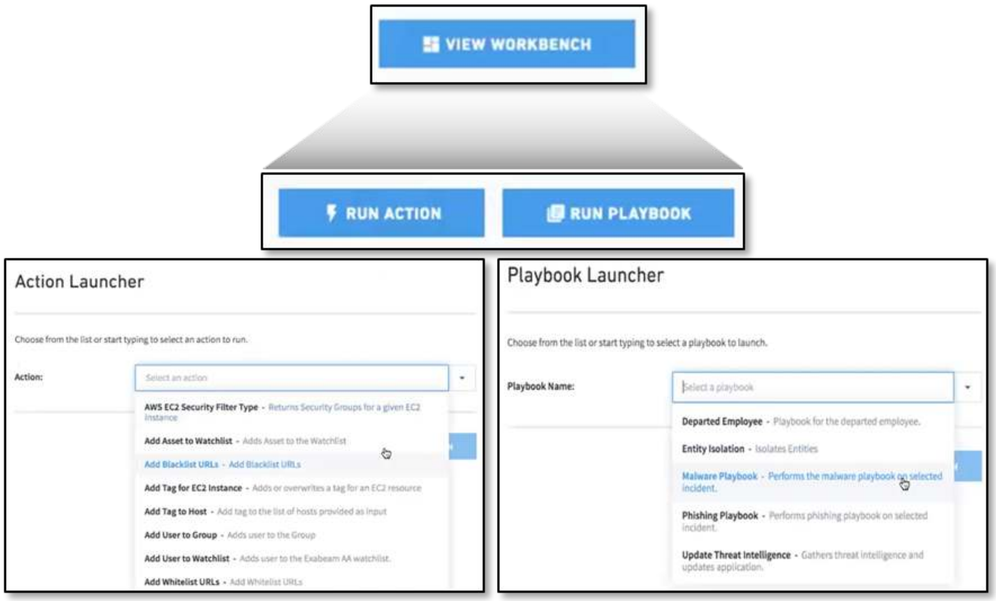
Figure 12. Incident Responder—Visual Playbook Editor


exabeam
INCIDENT RESPONDER
Playbook
Settings
Malware Playbook - Test 1
Investigate a malware alert and/or suspicious files.
START
Extract File Entities 1
Get File 1
Get Endpoint Triage Dat...
Scan File - YARA 1
Detonate file in a sandb...
Extract Hash from File 1
Get URL/Domain reputat...
Geolocate IP 1
Get File Reputation 1
Hunt through triage data...
Hunt through triage data ...
Hunt through triage data...
END

The playbook editor enables the analyst to create partially or fully automated resolution procedures for incidents not addressed by those playbooks that Exabeam already supplies. Instead of resolving incidents manually, an analyst can now easily create and automate new procedures via playbooks, rather than learning a new programming or scripting language. The playbooks can now run in the background without the analyst searching actively for specific incidents. The playbook editor can help the analyst construct ways to address specific incidents more easily, thus helping again to increase productivity while reducing the organization's security risk profile.

ESG also observed the ease with which specific actions or playbooks can be run for specific incidents. From a specific incident listed in the Case Manager, we clicked on the *View Workbench* button. We saw that an analyst can run either a specific action or playbook previously defined by a user or supplied by Exabeam (see Figure 13).

Figure 13. Incident Responder—Workbench



Action Launcher

Choose from the list or start typing to select an action to run.

Action: Select an action

- AWS EC2 Security Filter Type - Returns Security Groups for a given EC2 Instance
- Add Asset to Watchlist - Adds Asset to the Watchlist
- Add Blacklist URLs - Add Blacklist URLs
- Add Tag for EC2 Instance - Adds or overwrites a tag for an EC2 resource
- Add Tag to Host - Add tag to the list of hosts provided as input
- Add User to Group - Adds user to the Group
- Add User to Watchlist - Adds user to the Exabeam AA watchlist.
- Add Whitelist URLs - Add Whitelist URLs

Playbook Launcher

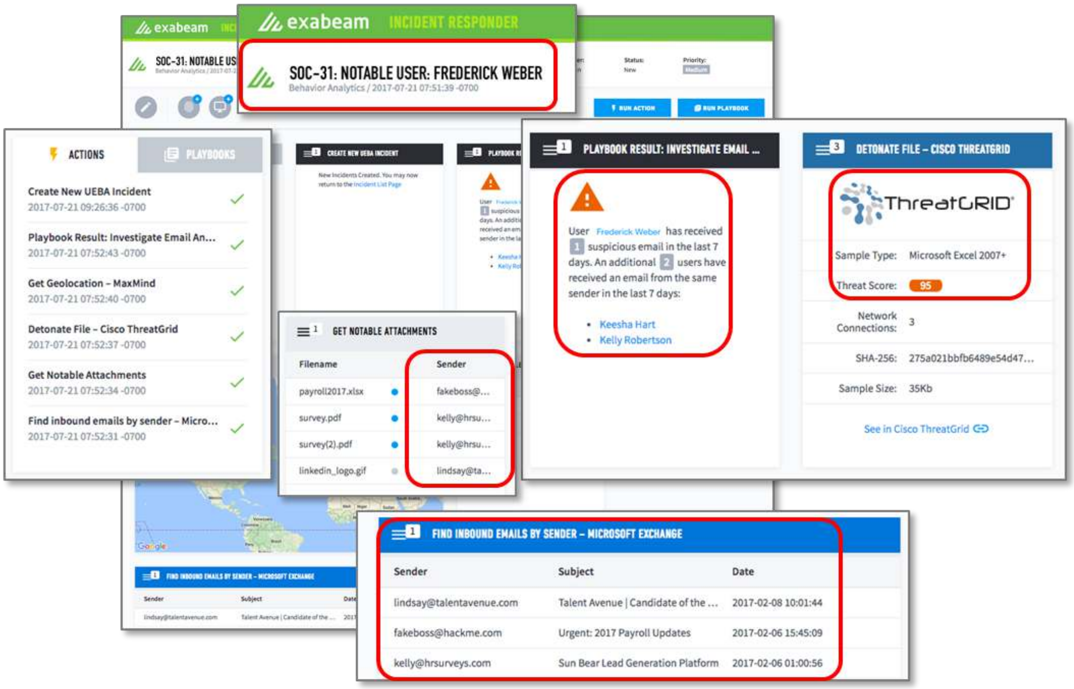
Choose from the list or start typing to select a playbook to launch.

Playbook Name: Select a playbook

- Departed Employee - Playbook for the departed employee.
- Entity Isolation - Isolates Entities
- Malware Playbook - Performs the malware playbook on selected incident.
- Phishing Playbook - Performs phishing playbook on selected incident.
- Update Threat Intelligence - Gathers threat intelligence and updates application.

Figure 14 shows an example of an actual incident playbook, for *Frederic Weber*, who has been flagged as a notable user. The playbook determined that *Frederick* was infected via a suspicious email, identified the sender and other recipients, identified other emails from that sender, and reported the risk of the attachment based on analysis by the Cisco ThreatGrid sandbox.

Figure 14. Exabeam Incident Playbook



SOC-31: NOTABLE USER: FREDERICK WEBER
Behavior Analytics / 2017-07-21 07:51:39 -0700

Create New UEBA Incident 2017-07-21 09:26:36 -0700	✓
Playbook Result: Investigate Email An... 2017-07-21 07:52:43 -0700	✓
Get Geolocation – MaxMind 2017-07-21 07:52:40 -0700	✓
Detonate File – Cisco ThreatGrid 2017-07-21 07:52:37 -0700	✓
Get Notable Attachments 2017-07-21 07:52:34 -0700	✓
Find inbound emails by sender – Micro... 2017-07-21 07:52:31 -0700	✓

CREATE NEW UEBA INCIDENT

New Incidents Created. You may now return to the Incident List Page

GET NOTABLE ATTACHMENTS

Filename		Sender
payroll2017.xlsx	●	fakeboss@...
survey.pdf	●	kelly@hrsu...
survey(2).pdf	●	kelly@hrsu...
linkedin_logo.gif	●	lindsay@ta...

PLAYBOOK RESULT: INVESTIGATE EMAIL ...

User Frederick Weber has received 1 suspicious email in the last 7 days. An additional 2 users have received an email from the same sender in the last 7 days:

- Keesha Hart
- Kelly Robertson

DETONATE FILE – CISCO THREATGRID

Sample Type:	Microsoft Excel 2007+
Threat Score:	95
Network Connections:	3
SHA-256:	275a021bbfb6489e54d47...
Sample Size:	35Kb

See in Cisco ThreatGrid

FIND INBOUND EMAILS BY SENDER – MICROSOFT EXCHANGE

Sender	Subject	Date
lindsay@talentavenue.com	Talent Avenue | Candidate of the ...	2017-02-08 10:01:44
fakeboss@hackme.com	Urgent: 2017 Payroll Updates	2017-02-06 15:45:09
kelly@hrsurveys.com	Sun Bear Lead Generation Platform	2017-02-06 01:00:56

Why This Matters

Legacy SIEM products are increasingly unable to keep up with the rising number of data breaches and cyberattacks. Beyond aggregating data and analytics into one repository, today's SIEM products are evolving to enable analysts in consuming and processing security data in real time. As organizations continue to grapple with a gap in cybersecurity skills, SOC and IR analysts struggle to identify and resolve breaches quickly, placing the organization's information assets at significant risk

Exabeam offers seven modules—Data Lake, Cloud Connectors, Advanced Analytics, Entity Analytics, Threat Hunter, Case Manager, and Incident Responder—that allow analysts to focus on issue identification and resolution. Leveraging its Smart Timeline technology, the products stitch together disparate data from endpoint, network, and security devices, and combine it with user and application activity into timelines that track individual user activity, whether the user is logging into an organization from an internal network or the cloud. Exabeam's products also enable an analyst to identify and resolve issues more quickly by leveraging analytics to search continuously for recurring patterns of security breaches and automating responses to those breaches via prebuilt or customized playbooks.

ESG reviewed the user interfaces and capabilities of the Exabeam Security Management Platform. We verified that the Data Lake notes cumulative log activity over time and provides details for individual logs under various categories. We then verified that the Advanced and Entity Analytics modules can create timelines of user activity or activity from other sources to detect potential breaches, removing the need for an analyst to construct such timelines manually. With Threat Hunter, ESG found that organizations can quickly identify risks associated with specific activities within these timelines. Finally, ESG verified that the Case Manager not only allows an analyst to note reported incidents but also generates incidents uncovered via the analytics engine. The Incident Responder helps organizations to automate responses to similar incidents as they occur in the future, decreasing an organization's overall security risk profile. All three tools work together to increase operational efficiency and the effectiveness of analysts.

The Bigger Truth

While organizations are encountering an increasing threat of cyberattacks, they are facing the challenge of closing the cybersecurity skills gap. Any continuing investment in cybersecurity should include tools that will increase the SOC and IR analysts' efficiency in identifying and resolving issues, or the business will risk losses in both revenue and brand equity.

The Exabeam platform uses data science for behavioral modeling, machine learning, and advanced analytics designed for comprehensive insider and entity threat detection, leveraging a modern, scalable big data infrastructure. Exabeam Advanced Analytics and Entity Analytics provide insider threat detection, tracking anomalous behavior and lateral movements within an organization while securing cloud services, machines, devices, and IoT assets. Automated incident response and case management are employed to enable teams to respond to security incidents rapidly and with less effort.

ESG verified that the Data Lake collects and aggregates data efficiently from disparate devices and user and application activity, both from the internal network and the cloud. The analyst can leverage the Data Lake to investigate activity in a consolidated manner and identify potential problem areas, rather than spending time aggregating data from various logs into a digestible format.

The Advanced Analytics and Entity Analytics tools construct Smart Timelines using Data Lake data and enabled ESG to view activity from both a user and timeline point of view. By detailing user activity in this manner, an analyst can identify risky behavior, affected assets, and potential root causes more quickly, shortening response and resolution time.

Finally, ESG looked at Case Manager and Incident Responder and confirmed that they facilitate automated responses to resolve security issues. This ultimately allows an analyst to focus more on resolution as opposed to issue identification.

ESG validated that Exabeam's Security Management Platform helps organizations overcome the cybersecurity skills gap with end-to-end detection, analytics, and response capabilities. For organizations that want to move beyond the capabilities of legacy security information and event management (SIEM) platforms to gain more complete visibility into threats in their environment and orchestrate intelligent, automated response, it would be smart to take a close look at Exabeam's Security Management Platform.

The goal of ESG Validation reports is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Validation reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.