More inside: Traversing Networks, Advanced Analytics Data Pipeline, Context Tables

SMART

OUTCOMES

Making Security Success the Norm

Investigating Compromised Credentials

Operationalizing this use case in two scenarios

Interview with Gorka Sadowski

On how focused data sources can streamline your operations

Kerberos Exploitation

Including the Golden Ticket and Pass the Ticket exploits

exabeam

Hello SOC! What you have in your hands right now is meant for you! It's meant for the analyst who's caught in an avalanche of tickets without a snowmobile. It's meant for the escalation desk who has become so cynical that they feel log sources are as trustworthy as Facebook profiles. And it's meant for the engineer whose most recent implementation already requires an upgrade, a patch, and a reinstall. So to the war-weary, skeptical, and determined: this zine is for you. Consider it a handy cartridge of information with a quick load of insight. A handbook of sorts. A graphic whitepaper. A SecOps travel guide for those who don't know SecOps.

Here at Exabeam we recently released our Threat Detection Investigation and Response (TDIR) Use Case Packages. These Use Case Packages are designed to enable businesses to achieve greater consistency, faster time to resolution, and better security outcomes. In this issue, Tim Lowe helps us turn that into reality as he focuses our attention on investigating a compromised insider with stolen credentials using Exabeam and good ol' fashioned know-how.

We hope you like this format because we'd like to do more. Let us know what you think. After all, Exabeam currently offers three use case packages: External Threats, Compromised Insiders, and Malicious Insiders, covering 20 threat-centric use cases. That means more to learn! From all of us here in Education and from Community, we hope this helps you Outsmart the Odds! And be sure to check out more great content on our Community pages and Content Library documentation on Github.

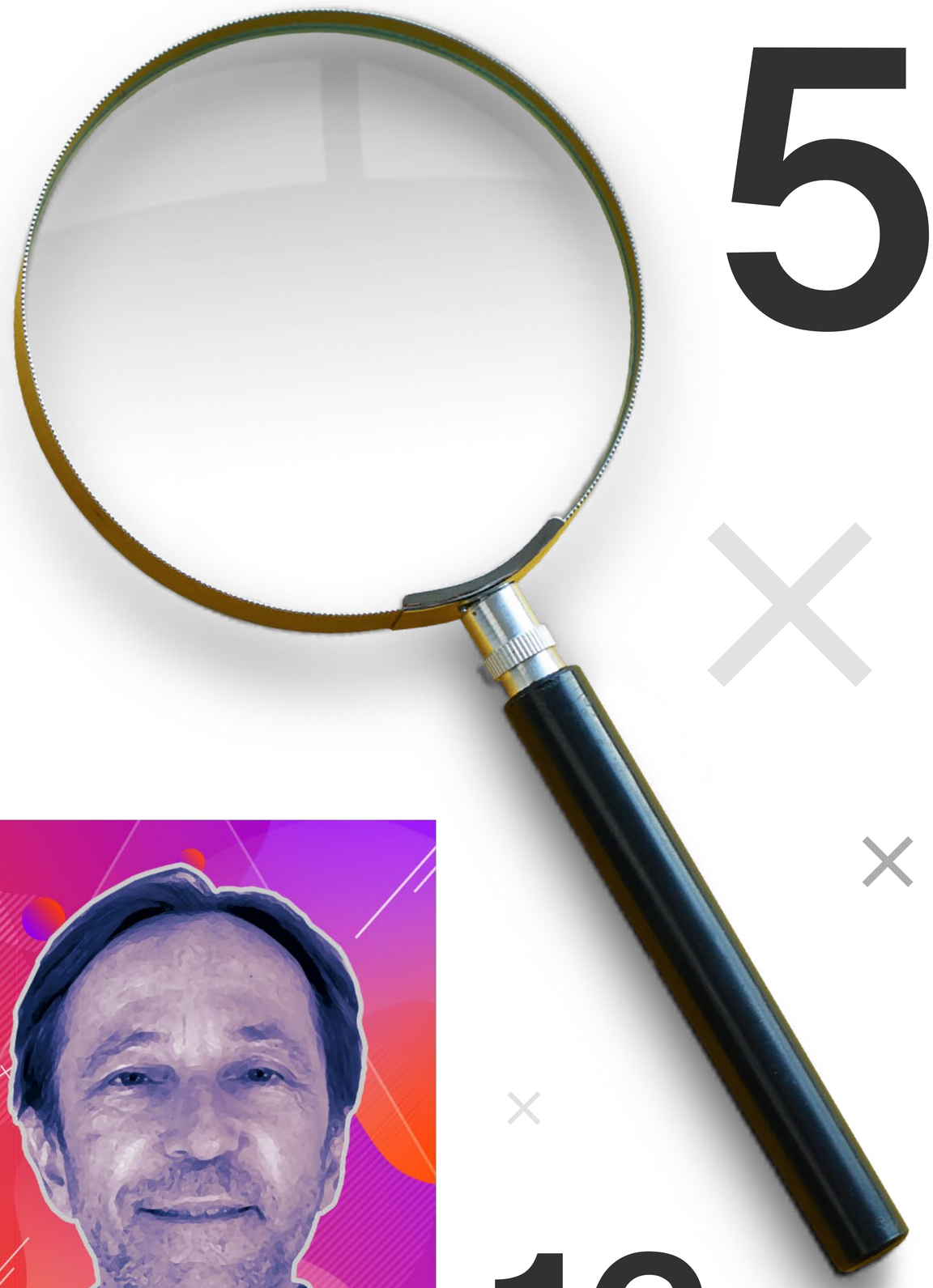
– ***Jason Yates,*** *Editor & Manager of Learning and Development*

Tim Lowe	Writer
Tim Schutz	Design & Layout
Jason Yates	Editor
Contributors	Tim Lowe
	Gorka Sadowski

Tim Lowe

Tim Lowe is a Senior Community Content Creator on the Exabeam Community team. Before coming to Exabeam, Tim was a Cybersecurity Engineer at a Fortune 500 company where he had hands-on experience conducting investigations in Exabeam for three years. Prior to that, he served as a Discovery Analyst for the National Security Agency for seven years, living in Europe for most of that time and living out history nerd dreams. Prior to that posting he attended the Defense Language Institute in Monterey, California to study Modern Standard Arabic. He then got to see the world, and underneath the sea, as a Multi-Discipline Language Analyst in the US Navy, deploying twice. He attended the University of Alabama, where he received a Master's in French Literature. He currently lives near Birmingham, Alabama where he has a wife and three daughters. For fun he mountain bikes and plays banjo and mandolin in a pop country band. For not as much fun, during COVID at least, he is the owner of a restaurant in Birmingham.

Inside:



Community

The following articles are excerpts from our **Use Case Knowledge Series**. Learn more about Compromised Credentials and other Use Cases by visiting the Exabeam Community website **here**.

COVER STORY

Two Scenarios Investigating Compromised Credentials

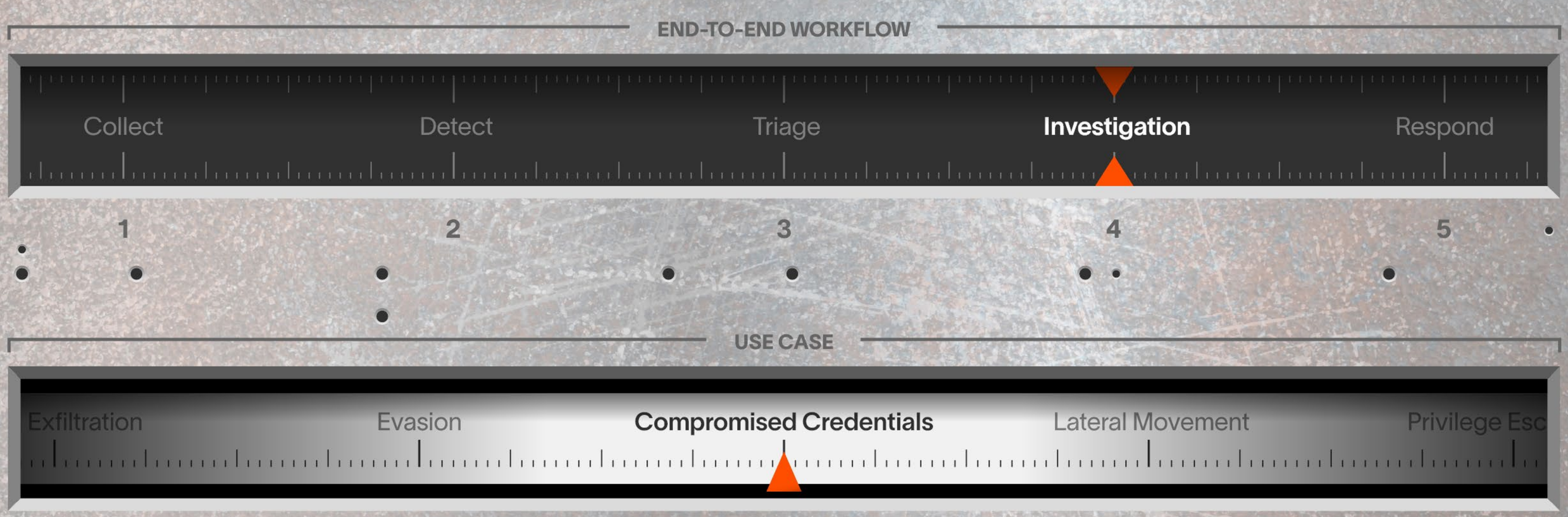
By **Tim Lowe**
Senior Community Content Developer

Operationalizing the Exabeam Compromised Credentials Use Case. Explore an investigation scenario involving compromised credentials.

Let's take a look at a couple of scenarios you might run into investigating suspected credential compromise and the questions we'll want to ask. These scenarios will serve as an example of how an investigation might proceed. It's important to create a workflow that works for your team and document those responses. Let's look at an example scenario and then walk through a potential play-by-play.

ARTICLE DETAILS

0001-12



Scenario One

Barbara Salazar is a Human Resources Coordinator based in Chicago. Recently the SOC reviewed a notable session in which Barbara was logging in from Ukraine. There were some other concerning alerts in the same session that look suspicious. What are our first steps?

Barbara Salazar

human resources coordinator | chicago

DEPARTMENT
hr

MANAGER
Tu Peterson

TOP PEER GROUP
104
+20 more groups

RISK SCORE
46

Watchlist

FIRST SEEN
1 Jun 2020

LAST SEEN
3 Jun 2020

LAST ACTIVITY
Account is active

EMPLOYEE TYPE
employee

LAST PASSWORD RESET
—

0 COMMENTS

In investigations, it's important to determine a couple of points first and foremost.

- Is this abnormal?
- Does this present a risk to my enterprise?
- How urgent is this risk according to our risk tolerance matrix?
- What does our organizational policy dictate that our response actions be?
- How do I investigate this incident?

Our first step is to determine if this is actually Barbara logging in from Ukraine. A quick check of Barbara's Data Insights in Exabeam Advanced Analytics will inform us of her usual locations. It looks like Barbara doesn't use a VPN very often and she does not have a habit of working while traveling. We gain massive intel value with these insights. From just a quick look at VPN Insights, we can deduce a good deal about this activity. Looking through other relevant Insights on Barbara we can arm ourselves with a broad awareness of her typical activity before we decide which step to take next.

Just a few things we could ascertain by taking a look at her VPN Insights are:

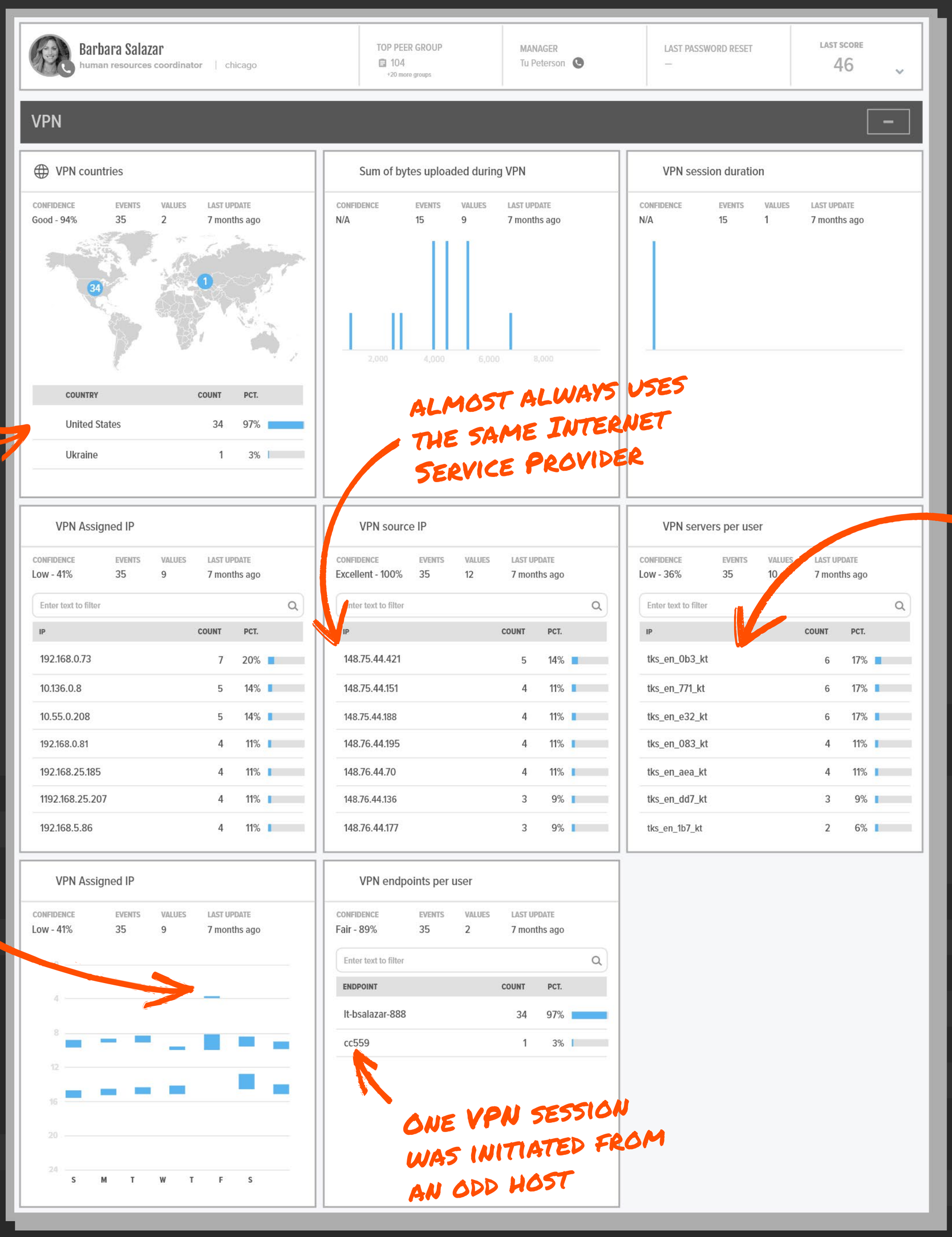
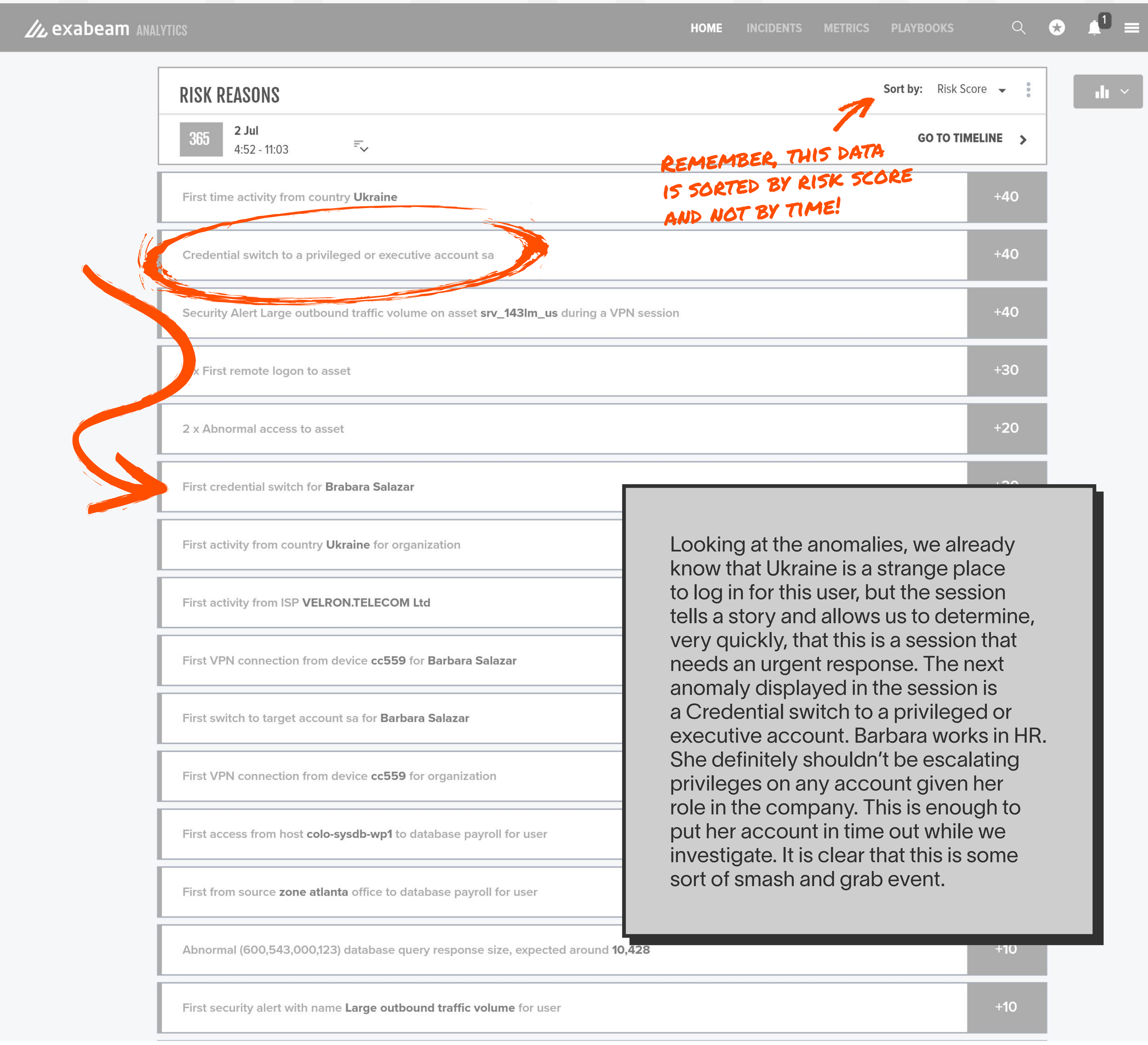


Figure 1: Data Insights, VPN view

What the Session Anomalies Tell Us

Let's take a look at Barbara's full session in the Risk Reasons view. Risk Reasons view is a summary of the anomalies in the session. The Timeline will have the complete picture and the ability to filter and drill down on events. For now, we'll see if we can paint a picture of this event from just the anomalies. We make a quick call to our Windows Security Team and give them advance notice that an incident that requires a response is likely coming their way and that they should be prepared to lock Barbara's access down. We may have further accounts to lock down, but it is clear that Barbara's is going to be the first.

Figure 2: Risk Reasons view



Looking at the anomalies, we already know that Ukraine is a strange place to log in for this user, but the session tells a story and allows us to determine, very quickly, that this is a session that needs an urgent response. The next anomaly displayed in the session is a Credential switch to a privileged or executive account. Barbara works in HR. She definitely shouldn't be escalating privileges on any account given her role in the company. This is enough to put her account in time out while we investigate. It is clear that this is some sort of smash and grab event.

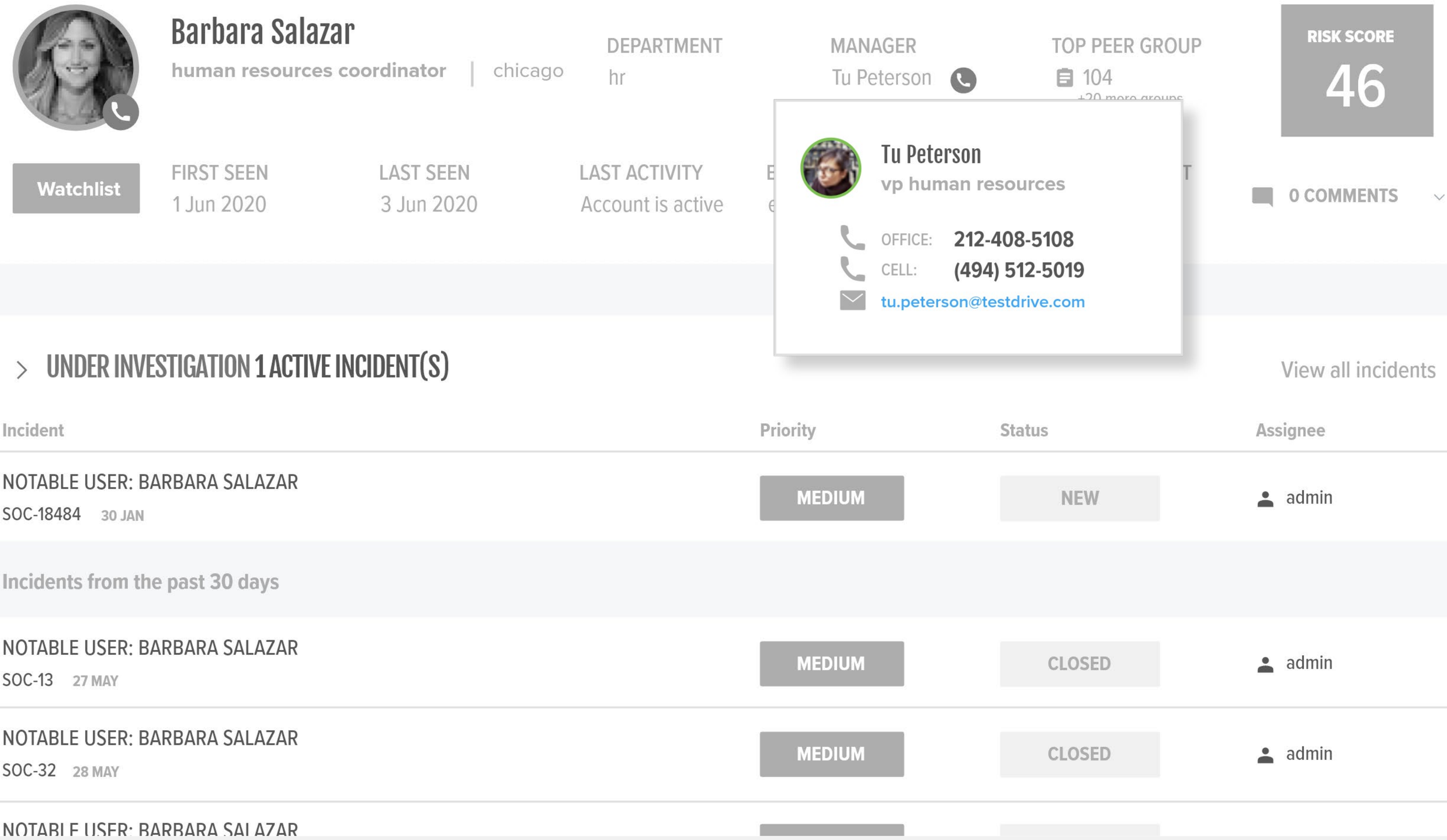


Figure 3: Data Insights

Barbara's auto-populated contextual info

We've established that this is definitely odd behavior from Barbara's account. We give her manager, Tu Peterson, a quick call to determine whether Barbara might be working on vacation or traveling to some other destination. We can find the contact information listed for Tu by clicking on the phone next to her name in Barbara's profile. Tu assures us on the phone that Barbara should be in Chicago and that this behavior was indeed very odd.

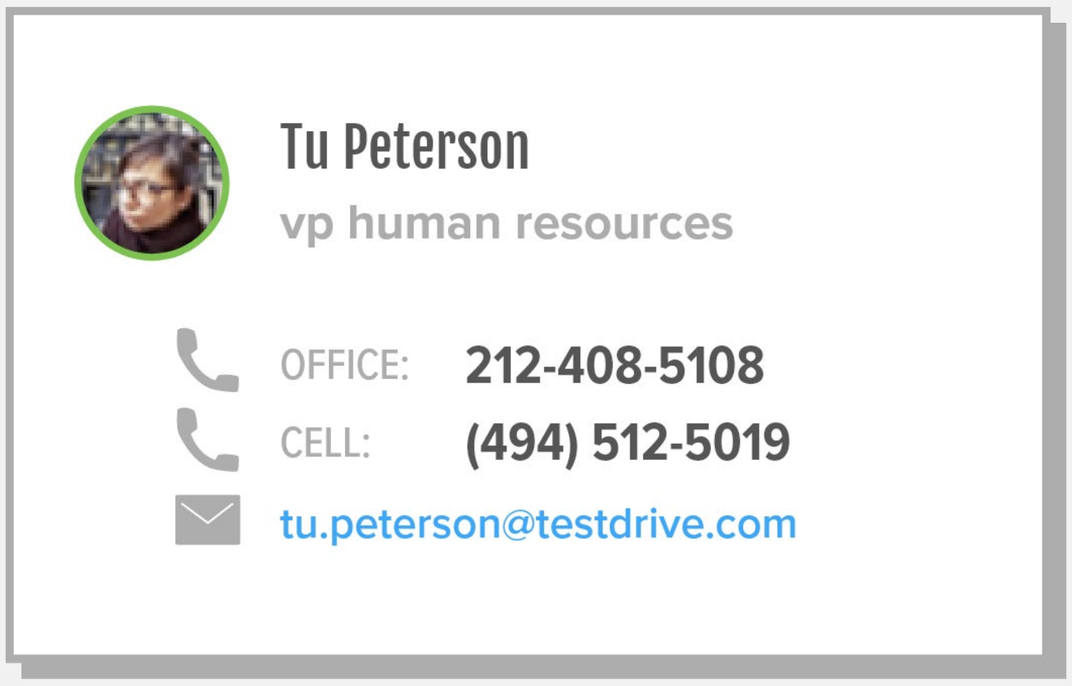
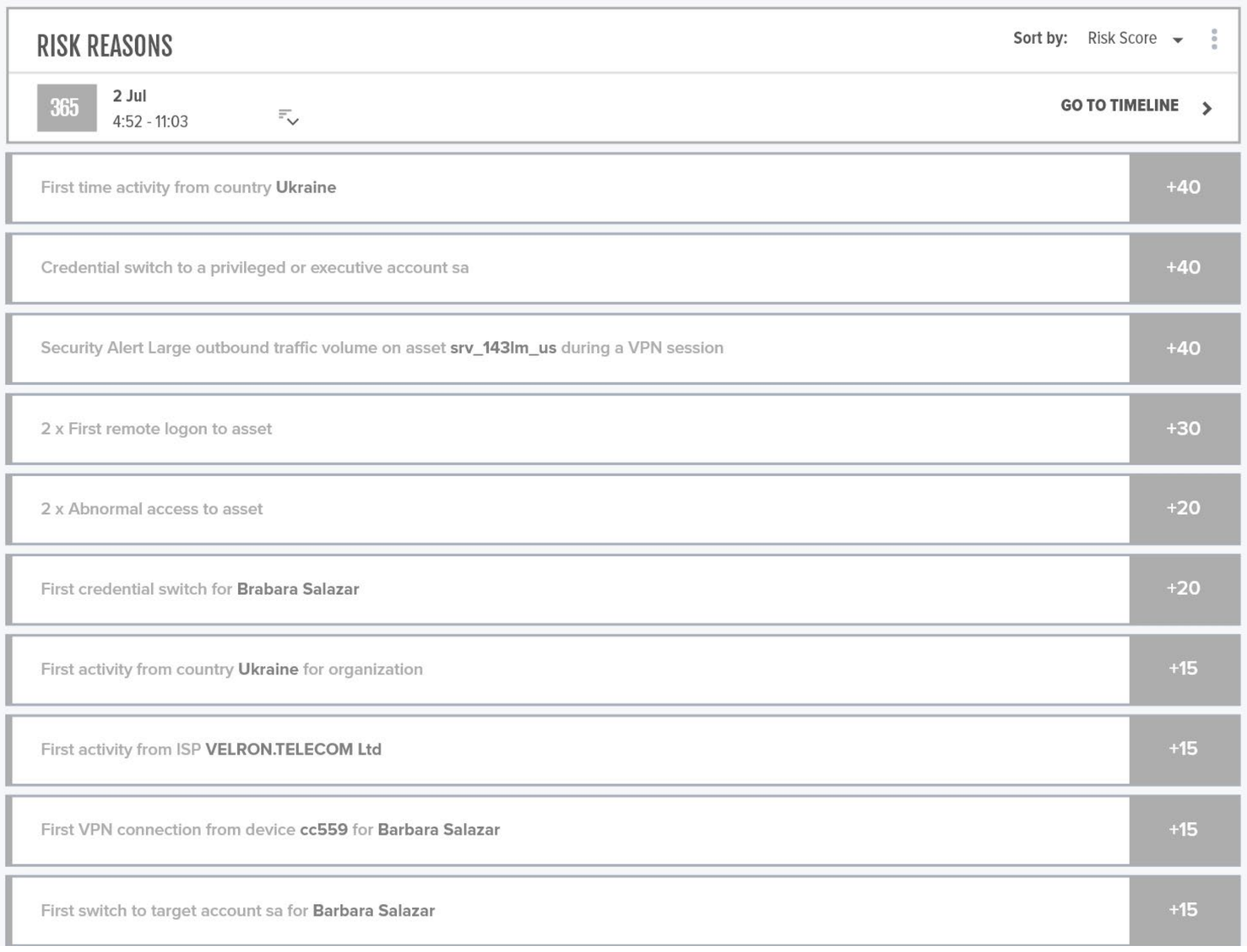


Figure 4: Data Insights detail, manager information

Timeline View vs. Risk Reasons View



Risk Reasons view

The Risk Reasons view is a summary of rule triggers that contributed to the aggregated score of the session. It is intended to give the analyst an instant idea of what activities led to the score of the session. As we've seen in both scenarios, more often than not it is sufficient to present an analyst with a clear picture of what is going on and what route to take with the analysis. In the example Risk Reasons view (Figure 5), an analyst can get an idea of the activity and decide on a path of action very quickly.

Figure 5: Risk Reasons view

Timeline view

The Timeline view presents the full picture of what occurred in a session. Many times the Timeline view can be overwhelming, as it contains every event associated with the user. This will contain high volume logs, such as Windows and Firewall logs. Scrolling through that volume of events can be slow and tedious, but sometimes is necessary. This view is very handy to pivot and filter on the types of events you want to see. The image (Figure 6) is an unfiltered view.

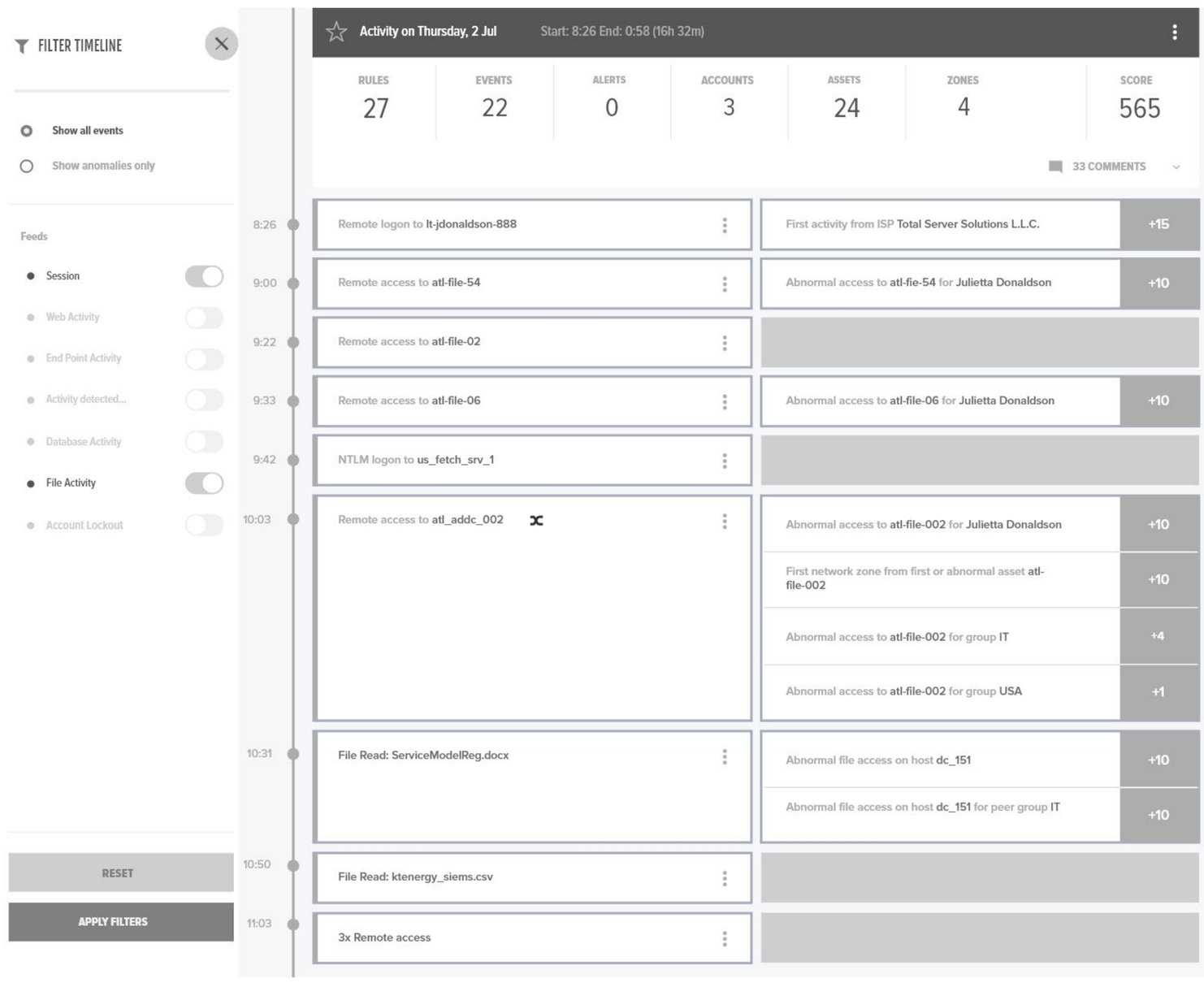
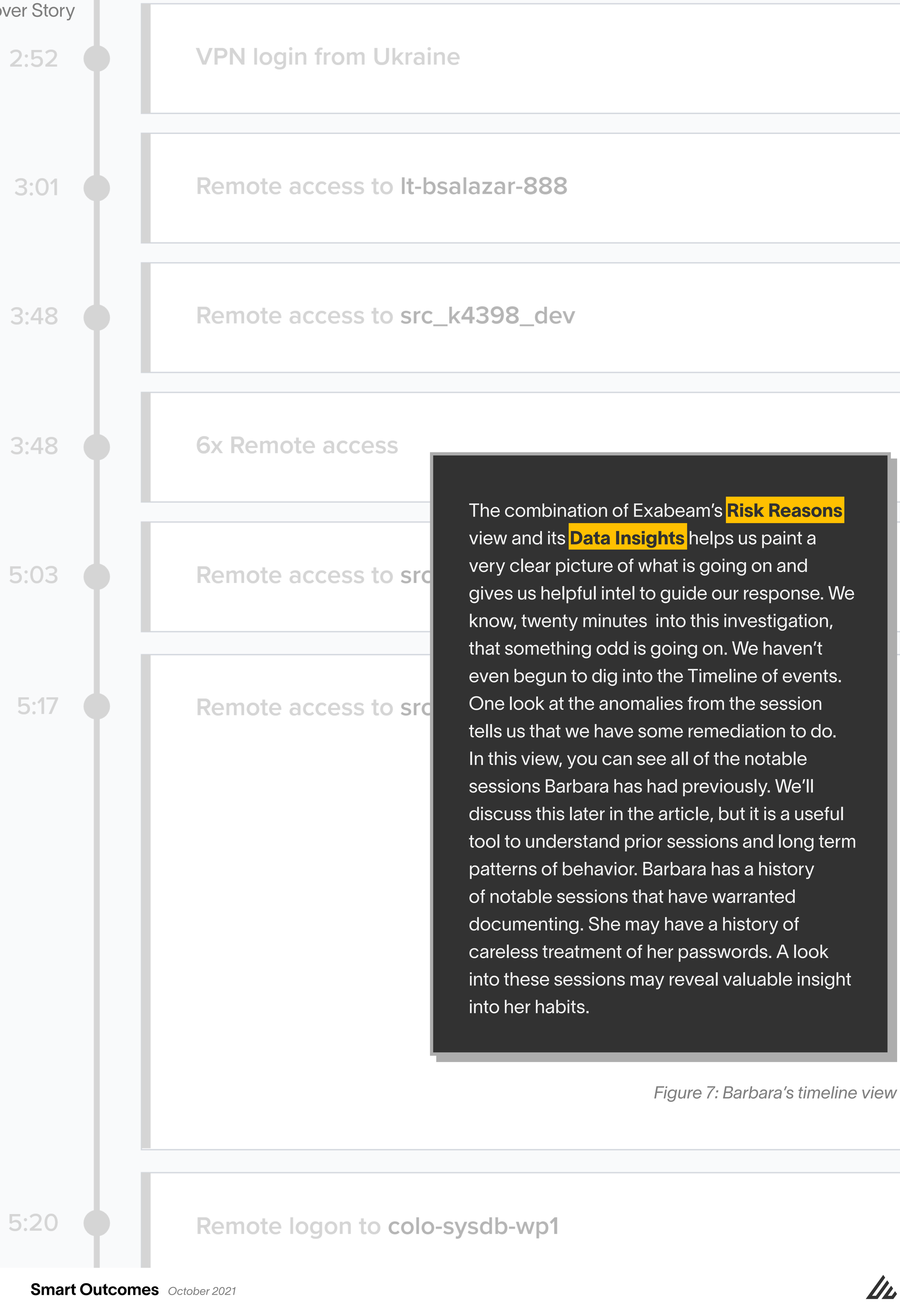


Figure 6: Timeline view



The combination of Exabeam's **Risk Reasons** view and its **Data Insights** helps us paint a very clear picture of what is going on and gives us helpful intel to guide our response. We know, twenty minutes into this investigation, that something odd is going on. We haven't even begun to dig into the Timeline of events. One look at the anomalies from the session tells us that we have some remediation to do. In this view, you can see all of the notable sessions Barbara has had previously. We'll discuss this later in the article, but it is a useful tool to understand prior sessions and long term patterns of behavior. Barbara has a history of notable sessions that have warranted documenting. She may have a history of careless treatment of her passwords. A look into these sessions may reveal valuable insight into her habits.

Figure 7: Barbara's timeline view

With just a quick glance, we can see we have a serious breach on our hands. We're going to have to initiate our Severity 1 protocols on this one. Next, we have the miscreant using these privileged credentials to access a server, srv_1431M_us, and to Secure Copy (SCP) a large amount of data out to a known malware URL. Next, they move laterally to colo-sysdb-wp1. We'll need to look this up, but from the naming protocol it appears that they've made it into a database of some sort. Looks like we have some big trouble. Fortunately, this is a hypothetical scenario because these bad guys have done a lot of damage in a short amount of time.

An investigation of this sort, without the aid of the vendor log aggregation in the Exabeam Risk Reasons summary, the highlighted anomalous behavior from the analytics engine, and the user role contextualization provided in the Exabeam Advanced Analytics UI, could potentially take many analysts several days. The other teams wouldn't have the analytical insights of first or abnormal access that Exabeam highlights and would have to do the analysis manually.

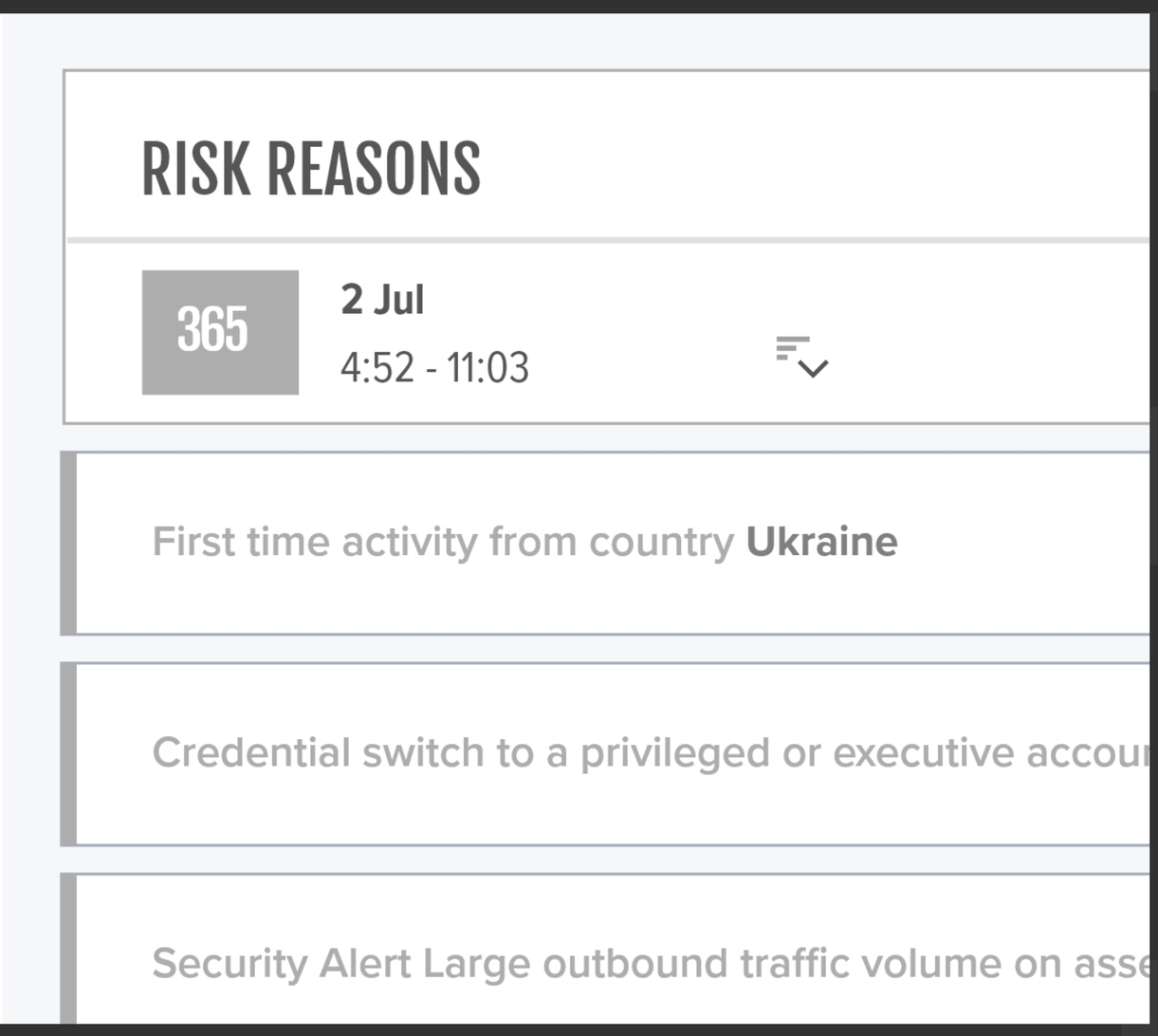
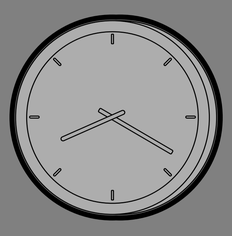


Figure 8: Barbara's Risk Reasons Summary

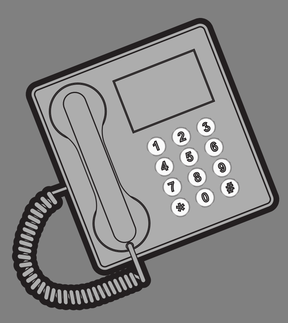
Action needed!

The miscreants are moving fast. Allowing them to escalate privilege and move laterally through your network could create further and more dangerous risks.



It will also significantly increase the effort you'll have to dedicate to analyzing and repairing the damage these bad actors have done to your security posture.

We already have a privileged account that might need remediation as well. We need to start with locking down these accounts and begin coordinating with the Intrusion Detection Team, who manages our End Point Detection and Response playbooks.



We make some phone calls and get these two users sandboxed.

Continue the investigation

Now that these accounts are locked down, we can proceed to investigate what, if any, other accounts or assets need to be disabled. The IDS team will also begin looking for abnormal or dangerous files and executions on Barbara and the user of the SA account. These bad guys are moving around quickly. Let's take a look at the full timeline to follow the story further.

Taking a look at the session above, we can create a timeline of the events that details the severity of the attack, the legitimacy of the attack, and track the flow of events to engage the proper Information Security partners in near real-time. It would be impossible to craft a timeline of events like this in typical SIEMs this quickly. From a glance at the Risk Reasons view, we can track the attack from one single source.

Without even delving into the metadata associated with the events, or even expanding the events, we can tell that:

2:32 a.m.
A Ukraine login occurred

3:01 a.m.
Remote access to lt-bsalazar-888

3:48 a.m.
Remote access to src_k4398_dev

3:48 a.m.
6x Remote access

5:03 a.m.
Remote access to src_n490_dev

5:17 a.m.
Remote access to src_o116_dev

5:20 a.m.
Remote logon to colo-sysdb-wp1

5:31 a.m.
Account switch to sa on colo-sysdb-wp1

7:03 a.m.
Remote logon to srv_sql05

7:07 a.m.
Login to database service payroll

7:55 a.m.
Database query on payroll

8:46 a.m.
Web access to fileshare.com

8:49 a.m.
Palo Alto Networks WildFire alert| Large outbound traffic volume on srv_143lm_us

9:03 a.m.
VPN logout

At this point we have barely delved into the metadata and log source info related to this breach. A wealth of information is available by expanding the activity.

Credential switch to a privileged or executive account sa

+40

DESCRIPTION

In addition to this being the first time this user has switched to these target credentials, the target credentials are privileged. This is a notable event because privileged credentials often have access to sensitive information

RULE TAGS

Exploitation for Privilege Esc...

EVENT TYPE

account-switch

ANCHOR SCORE		ANOMALY FACTOR		
40	X	1.0	=	+40

Event Details Rule Definition

Expanding the events and looking at the Event Details for the one event we can tell quite a bit:

- The user is on an abnormal account
- They are on an asset in an abnormal office
- They are logged into a host that someone in HR should not be logged into
- They are using Remote Desktop Protocol to access the host remotely

Figure 9: Credential switch information

Event Details for event ID 2315244@m

TIME	USER	ACCOUNT
7:31:00	bsalazar	sa
DOMAIN	**REPORTING HOST**	**ACCOUNT DOMAIN**
gcloud	colo-sysdb-wp1	—
DEST HOST	**DEST IP**	**DEST ZONE**
colo-sysdb-wp1	10.78.120.32	atlanta office
SOURCE HOST	**SOURCE IP**	**EVENT CODE**
cc559	10.77.129.122	4648
DIRECTORY		**PROCESS**
—		rdp.exe
SAFE/FOLDER/RESOURCE	**EVENT SUBTYPE**	**DEST SERVICE**
—	Windows	—

CLOSE

Figure 10: Event details

All of this critical intel is in just the second event in the session. This is the power of user and asset activity modeling and anomaly detection analytics. In just the second event in the timeline we already know we have to take urgent action.

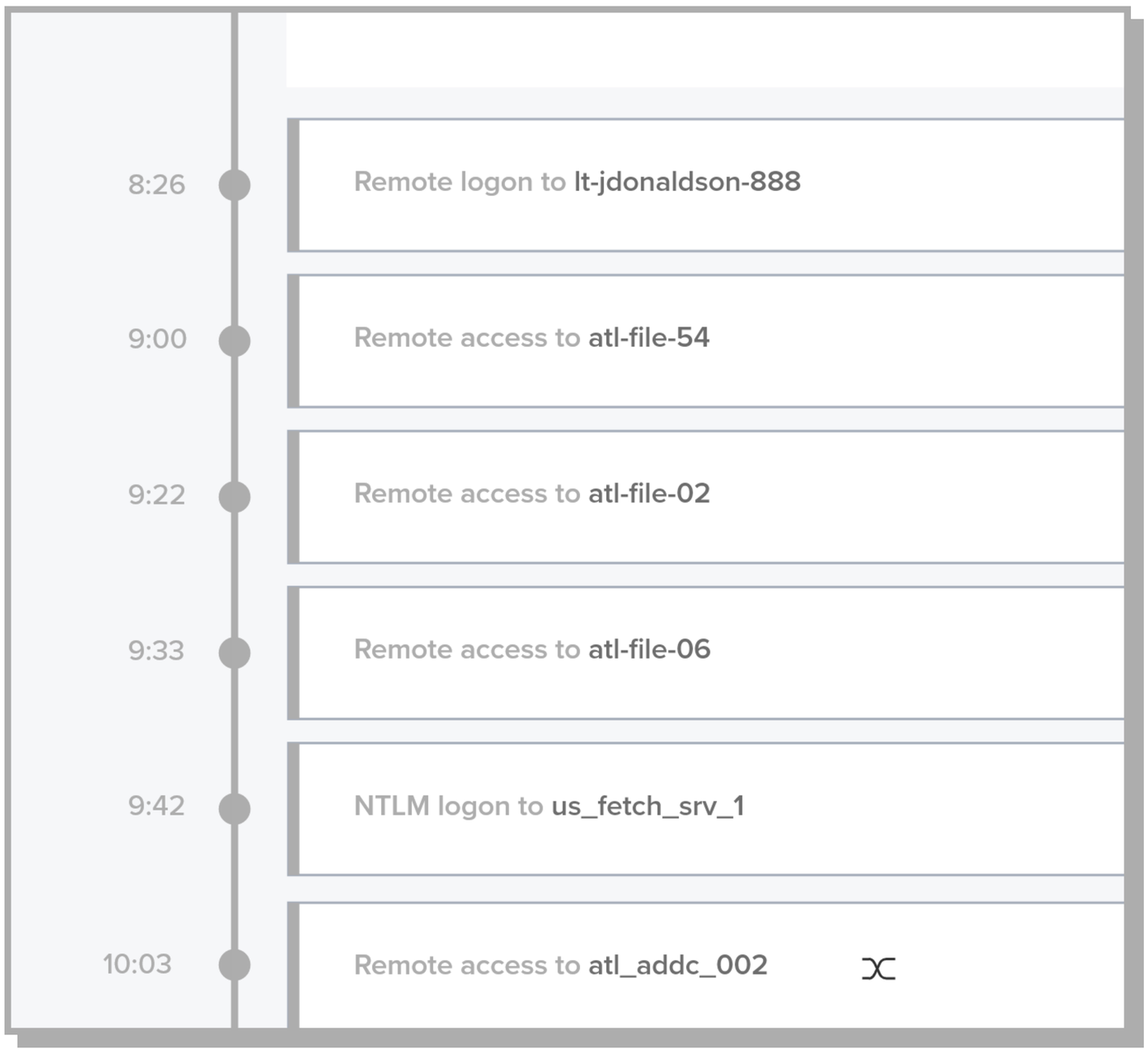


Figure 11: Timeline view

The Ukraine login happened at 4:32 a.m.. Privileges were escalated at 7:31 a.m. By the third anomaly alert, which occurred at 10:49 a.m., we have a notable session that would appear for SOC analysts to investigate. These three anomalies, scored appropriately, were enough to highlight this as a potential risk and alert an analyst to take action. In the best case, catching this so early saved hundreds of working hours for analysts responding to an event. In a worst case situation, these guys could have exfiltrated sensitive data that could cost the company millions of dollars, and what might be more valuable than that, their reputation in the market.

Barbara's session was a very noisy one. Not all miscreants bang around that loudly in your network. Many times, however, they do. Here's an anecdote from an analyst at a Fortune 500 company.

Continued on page 27

Notes from the Field

"Our organization hired a consultancy firm to come in and pen test our network. The scenario was a compromised insider scenario. One of our InfoSec execs willingly gave up his password to the red team. The red team laid low on the network until they were able to escalate their privilege and then ran roughshod through the network accessing hundreds of machines. Exabeam saw it almost immediately. Our threshold for notable sessions was 90 points. The score this user generated when the red teamers had control of their account was... wait for it, 27,000. It was the highest score I've seen, before or since. It was a big win for our team. The host IDS team didn't see it. The Windows Security team didn't see it until we told them about it. It was the first access rules that triggered hundreds of times. It was a big deal for our group and gave us a lot of confidence that we'd see it quickly if it happened by real bad guys."

Gorka Sadowski

An Exabeam Interview

More data means more outcomes. Can you explain how security is not a big data problem, rather a right data problem?

The question then becomes, well, what is the right data? And it's actually very easy to find out what data you need and what is the right data. You actually start with the end, you say, okay, so what is the outcome? What is the insight that I'm looking for? It would be an outcome for a particular use case or a particular scenario, it could be something along the lines of, I want to flag the insider threat issues that I could have. You start with the end, with the outcome and then based on the insight that you're looking for, then it's actually very easy to find out what are the data points and the data sources that you need in order to generate that insight. And by and large, it is better to focus on those few very valuable data sources, as opposed to say, "let me just bring all the data just in case". I heard "let's bring all the data 'just in case'" so many times. And what happens is that very quickly, you get too much data and the wrong data. So you first hit diminishing returns and then you hit a wall in terms of having too much data, and it's really polluting your SOC, it's polluting your tool, and it's really polluting the insight that you're looking for.

And by and large, it is better to focus on those few very valuable data sources, as opposed to say, "let me just bring all the data just in case". I heard "let's bring all the data 'just in case'" so many times. And what happens is that very quickly, you get too much data...

How can insight be generated with a "use case first" approach?

Think of the use case as a triangle. On top of the triangle you have the insight that you're looking for. And again, that insight could be, I want to make sure that my users are compliant with my security policy. I want to flag if I have an insider threat or if I have any malware or if I have any ransomware. So it's really about finding and generating an insight. And in order to generate that insight, you need two things. You need one or more data sources and then one or more analytics method. So you take those data sources, you apply some analytic methods to those data sources, and you generate the insight that you're looking for. So think of that almost as a triangle; insight, data sources and analytics.

Can you explain the idea of "high entropy" data and how all data is not created equally?

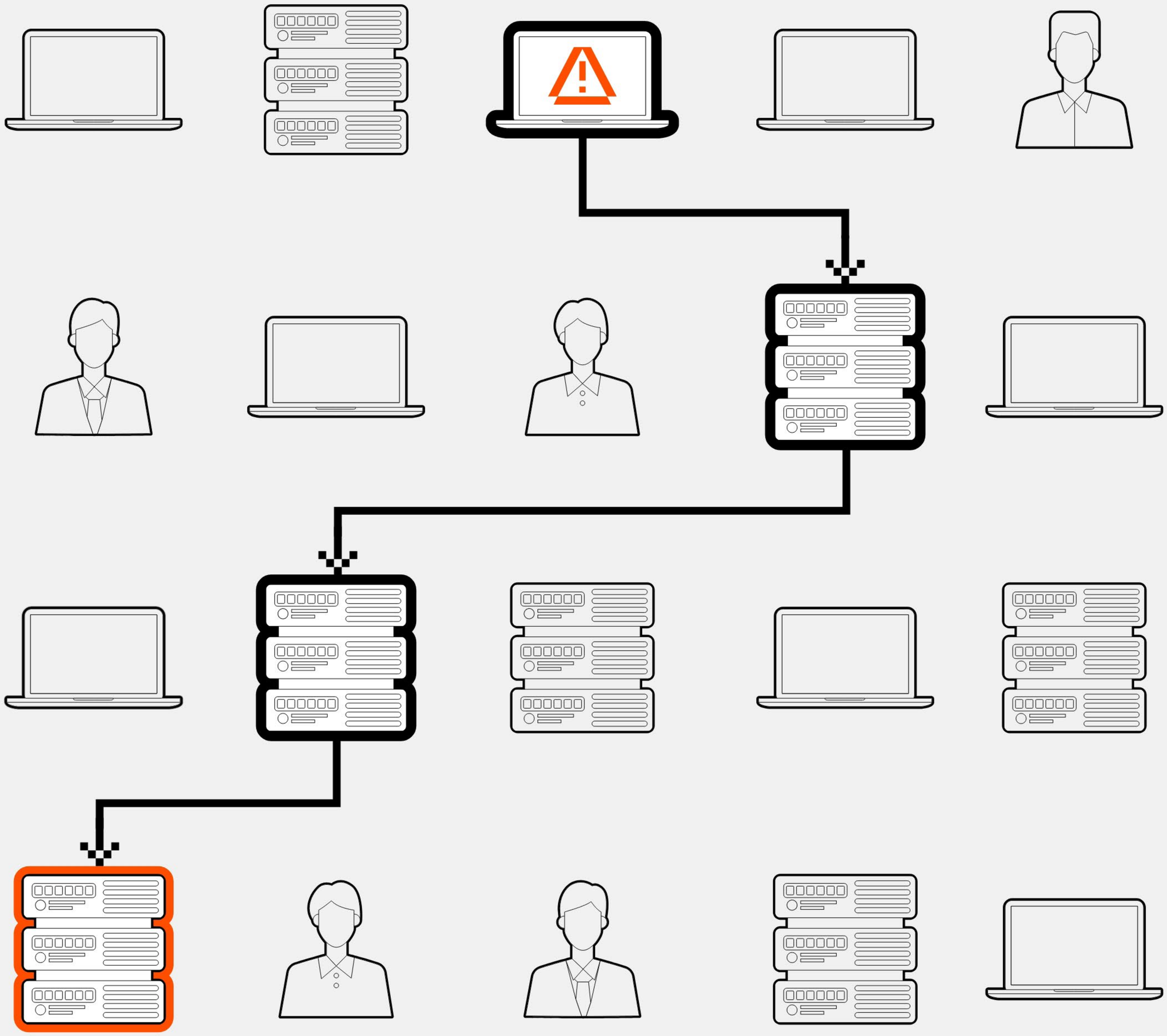
So entropy is really coming from the Shannon theorem of entropy. And, and it's about how much information do you have in a particular number of bits and bytes. It's a bit technical, but entropy really has to do with the value of a data source. And what you would notice as you go through the use case triangle is that they are data sources that are used for many, many use cases. It's actually a fairly well-known set of six to 12 data sources that are consistently used for 80% of the use cases that exists out there. So what are some of these data sources? They are your end point data sources or your EDR data sources if you have an EDR, or they can be your VPN, if you have remote people logging in via VPN, they could be your firewall alerts. And your active directory etc. It's about, you know, six, eight to 12 data sources that are used the most... That are used for many, many use cases. And the way you land on those is, again, you start with the insight you're looking for, and then you say, okay, for me to generate that insight, what are the data sources and the analytics? What are the data sources that are going to inform that? And then you can find out that you have those high entropy data sources that are being used over and over and over again. And on the flip side of that, there are some edge use cases that will require some very particular and very weird and very unique data sources that are used only for that insight. So again, take the use cases, look at what are the highest priority use cases for you. And then you will see that you will be landing on the half a dozen, to a dozen data sources that are high entropy.

What makes the workflow in Exabeam so powerful for an analyst?

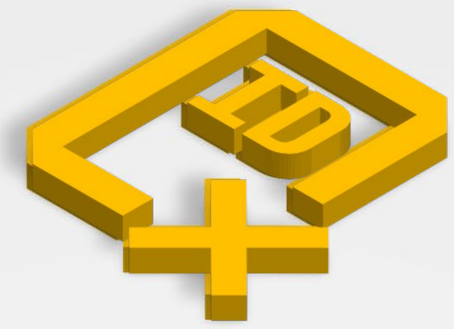
We provide you with use cases. We provide you with end-to-end workflows. And those workflows are not only content for the detection, but they are content for the detection, for the investigation, for the triage, and for the response. Think of it as an end-to-end workflow from threat detection, all the way to response. And at any moment you can enable some of these use cases, and as you do that, you will be told these are the data sources that you need. So it's really an out of the box experience that we're trying to provide to our client organizations in terms of quick time to value, quick time to operation ability. So yeah, that's what we do.

Traversing Networks

Lateral movement is a phrase used to describe a specific tactic when an attacker compromises or gains control of one asset and then moves from that asset to others.

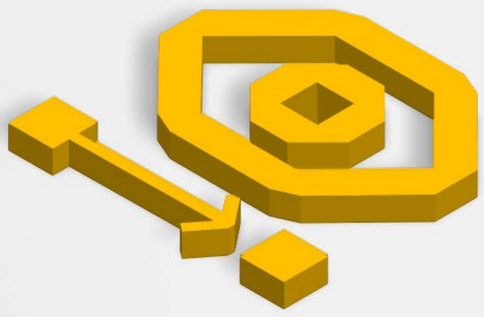


Compromised Credentials



...is often the starting point for...

...is used to achieve...



Lateral Movement

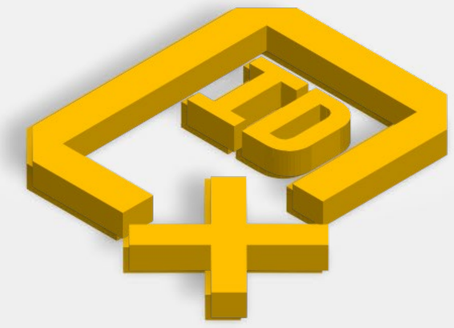
HOW THEY RELATE

Privilege Escalation

...happens very often because of further...

Horizontal privilege escalation is...

...is often achieved by further...



Compromised Credentials

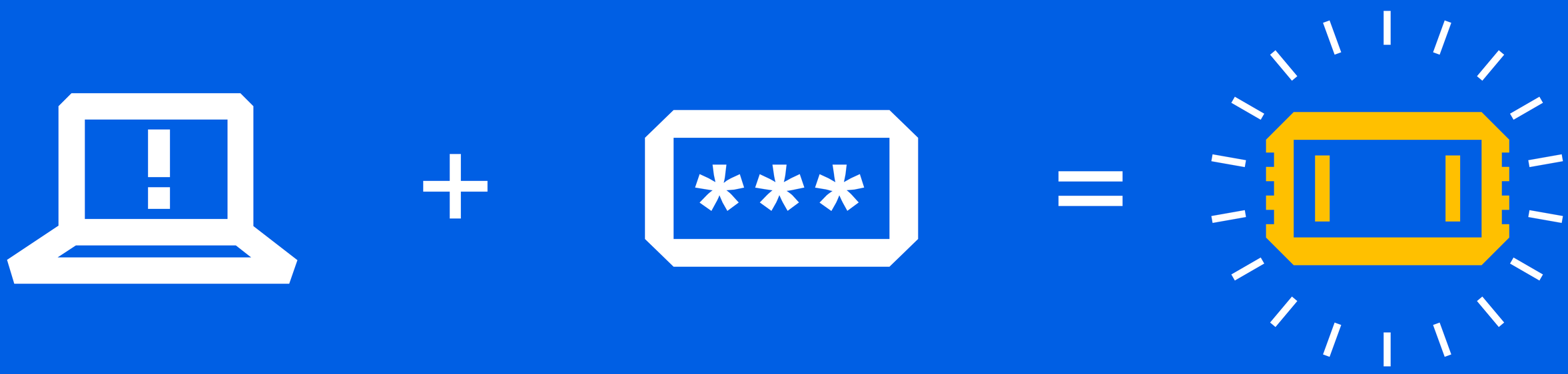
Kerberos Exploitation

Kerberos is the Microsoft authentication protocol most widely used on Windows systems. The manner in which Kerberos authenticates a user to a system is described in the image below.

By **Tim Lowe**
Senior Community Content Developer

Golden Ticket

One way attackers exploit Kerberos is to gain a golden ticket. Golden Ticket refers to an exploit where an attacker has access to a client's username and password. If this client is on a domain, the attacker can gain access to a ticket generating ticket. A ticket generating ticket, more commonly referred to as a TGT, is an authentication token granted by the ticket granting service. User account KRBTGT is the account that works in the background to encrypt authentication tokens on the domain. If this account is compromised and the attacker gains access to this account's hashed password, a "golden ticket" is acquired. This allows the miscreant to log into any account that they please.



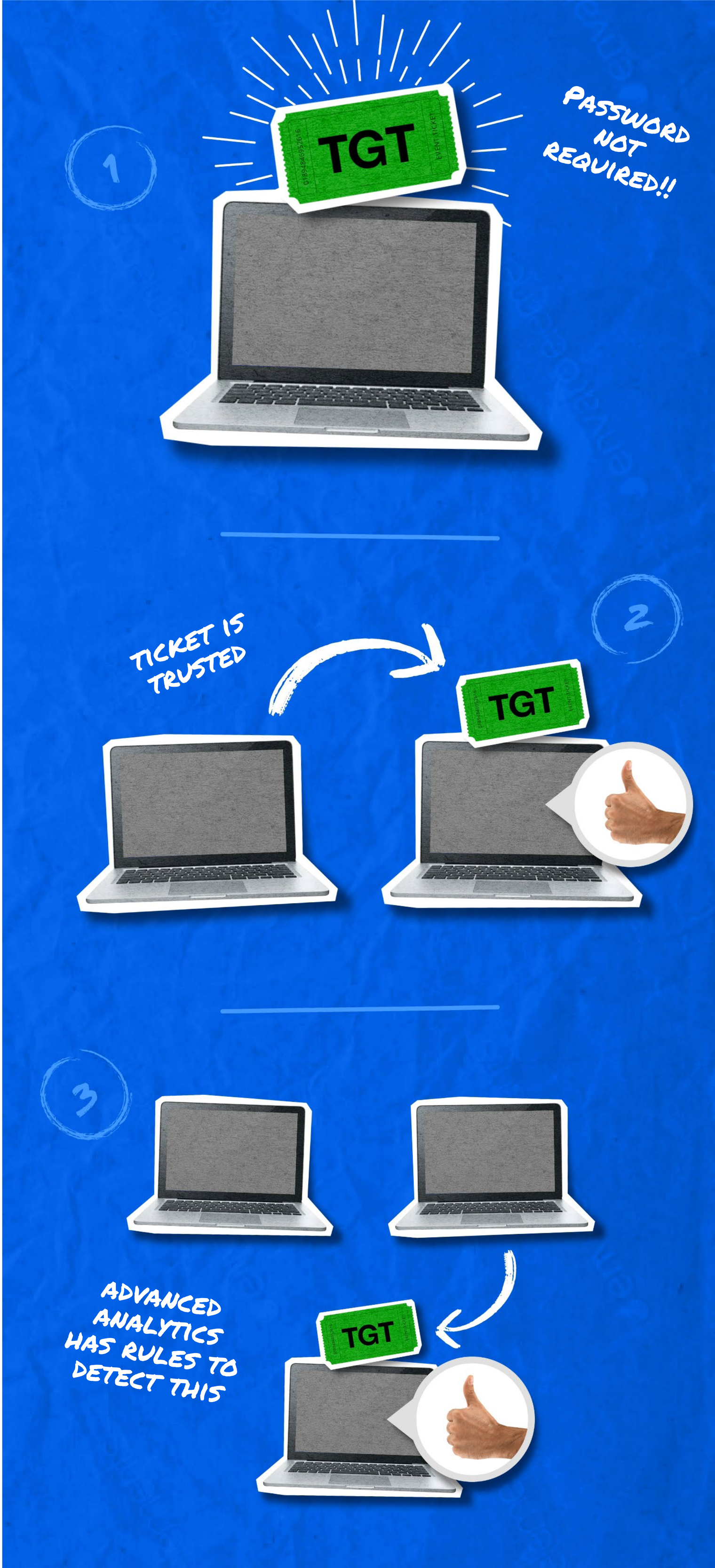
Compromised Account

Hashed Password

Golden Ticket

PASS THE TICKET

Pass the ticket is essentially the same as golden ticket. The difference is the level of privilege the account has will be lower than the KRBTGT account has. Pass the ticket attacks have the advantage of not requiring a user password to compromise systems. They locate a valid Kerberos ticket on a machine they have already compromised and use it on another system to gain access. The domain controller trusts this ticket, since it has already verified the identity of the user to whom it was granted. They then repeat this process on other Active Directory sessions until they achieve their goals. Advanced Analytics provides rules that identify when ticket passing is occurring.



Overview: the Advanced Analytics Data Pipeline

In order for Advanced Analytics to do work on log data (building timelines, assigning risk scores, etc.), it must parse the data into events according to categories called event types (Figure 1). These event types describe activity across the spectrum of a typical IT environment.

Some example event types include:

- Web activity
- VPN login
- Physical access
- Endpoint activity
- Print activity

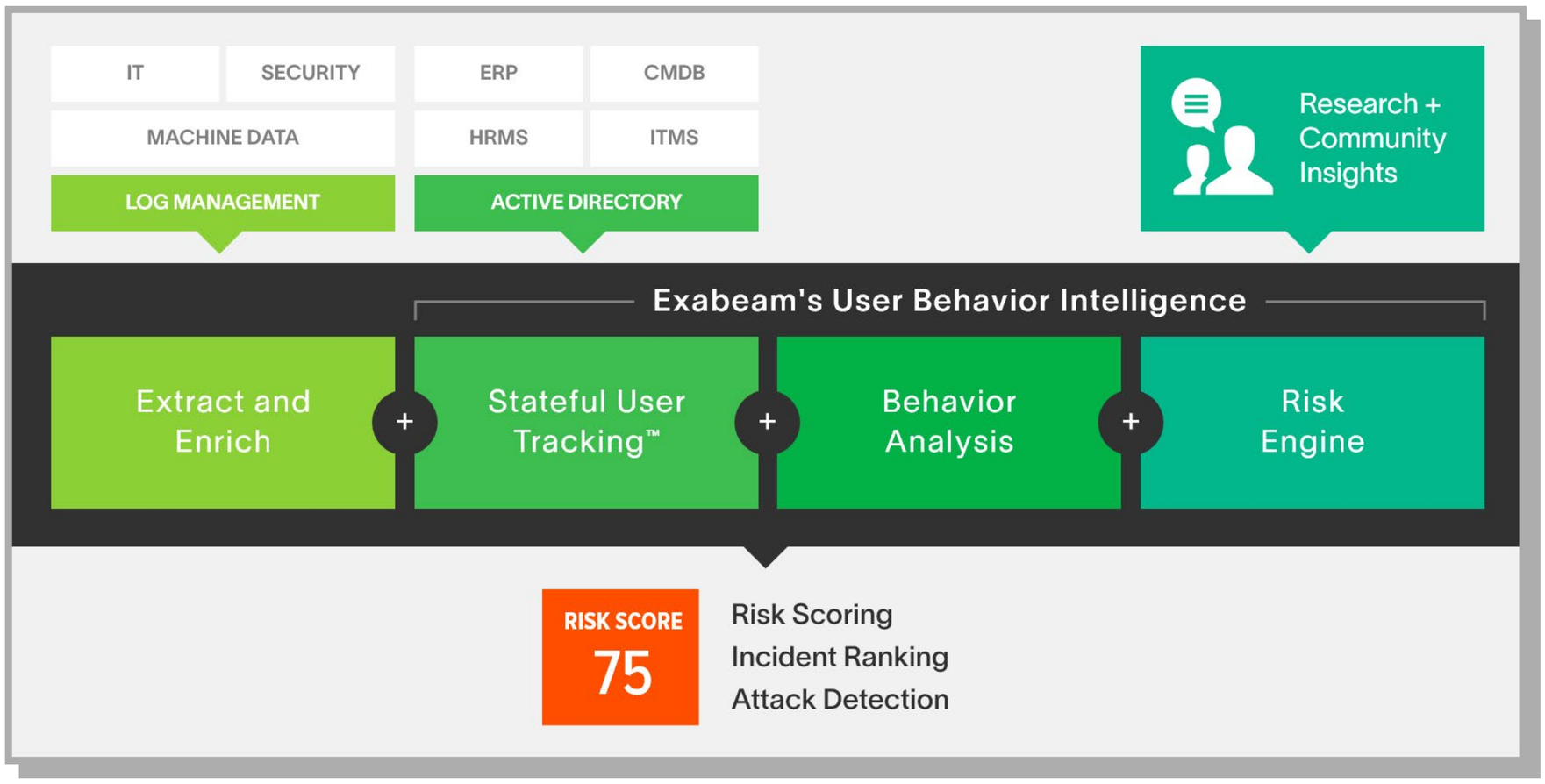


Figure 1: From the Advanced Analytics Admin Guide (for version i48), showing the data processing pipeline in relation to risk scoring.

Analytics then surfaces the given event along a user or asset timeline, organizing them according to configurable models and rules.

End to End Data Flow

Models

Models account for the core of Advanced Analytics' power for anomaly detection. Whereas a fact-based rule would trigger an event as a matter of simple "if-then" correlation—a user fails to login, and a rule fires accordingly—model-based rules surface events according to more complex parameters, such as:

Frequency

How often has the user failed to login?

Time

On which days, at what hour?

Data

Did an email attachment cross a certain acceptable threshold for file size?

Models divide into three categories and more information can be found about them in the How Content Works guide.

The three types of models:

CATEGORICAL

This type of model trains on string values, such as host or user names.

NUMERICAL_ CLUSTERED

This type of model trains on numerical values, such as the number of hosts a user logs into in a session.

NUMERICAL_TIME _OF_WEEK

This type of model trains on the time when events occur.

Some example models:

EPA-HP “Processes of the User” Models the processes of a user.

WEB-UBytesSum-Out “Sum of bytes written/uploaded to the web in a day by the user” Models the amount of data (in bytes) that were uploaded to the web in a day by the user

PR-UT-TOW “Print activity time for user” Models the times of day that this user performs print activity

Rules

Advanced Analytics uses configurable rules to:

Signal within the UI that an event has occurred

Associate that event with a value, called a rule score

You will find this referred to as a rule “firing” or “triggering”. Rules divide into two categories: fact-based and model-based, depending on the kind of behavior the given rule is designed to trigger on.

Fact-based

Fact-based rules can be thought of in a way analogous to traditional, static correlation rules, with the major difference being that a rule—fact-based or otherwise—is designed not simply to report an event, but to do so in a way that contextualizes that event within a session timeline and according to some measure of risk.

Model-based

Model-based rules make use of configurable models to track behavior that is too complex to trigger according to the simple “if-then” logic of a correlation rule. A fact-based rule might signal that a user has logged onto a given host, but a model-based rule will tell you when it was a first-time login for that user, or that they have done so at a statistically anomalous time of day.

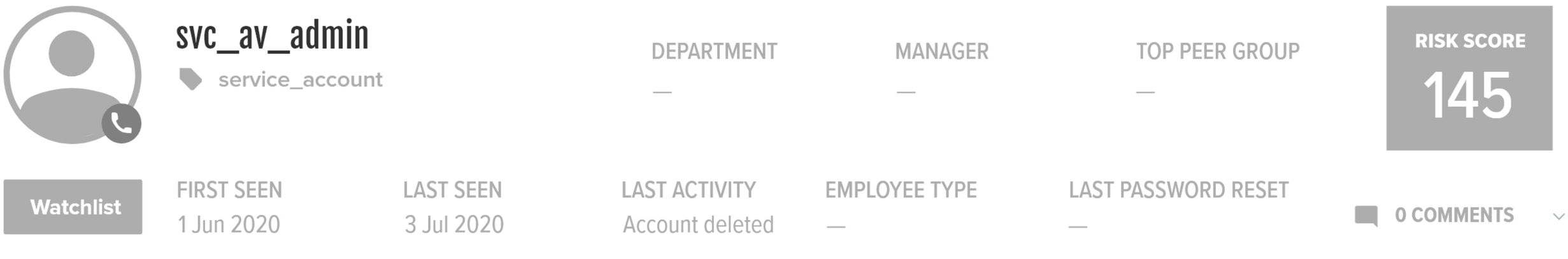
The rule score serves as the default value assigned to the event it governs. This value contributes to the risk score ultimately assigned to an event, but is not to be confused with the risk score itself. The other factors that contribute to the risk score will be covered later in this article.

More information can be found about rules in the How Content Works guide. We’ve included other resources pertaining to models and rules at the bottom of this article under Related Resources.

Continued from page 15

Scenario Two

One of your organization's service accounts, svc_av_admin, is exhibiting some notable behavior. The first anomaly in the session is a login from Russia. Being that you have no offices or remote workers in Russia, this could be a risky situation. It's not known what the designated purpose of this account is, but it is pretty clear that it needs to be investigated urgently.



This is a different type of compromised credential scenario. We'll need to drill down on this a bit since this is an unknown account, and service accounts require an extra layer of research since it is not always clear to whom they belong or what they are intended to accomplish. Human users and assets belonging to humans present a pretty clear path to the identification of the nature of the user's role and what we should expect them to be doing and logging into.

Service accounts, however:

- Often have names that don't specify clearly what their purpose is.
- They also have the potential to perform tasks that need to authenticate to a large number of devices to accomplish their task. You've probably seen this in your environment.
- Another differentiator with service accounts is that they are more likely to be left in the environment past the time they are needed than human-associated user accounts. When employees leave an organization, their user account gets deleted, but service accounts may need to persist. Often these are forgotten and remain active.
- Service account passwords don't change often, if ever, making them vulnerable to compromise.

Picking up an old service account, dusting it off, and using it to move laterally is a good way to hide under the cover of legitimacy to do bad deeds. These guys can be pesky to investigate, so let's dive into what we need to know about them.

Service accounts are created to serve a specific purpose

Let's say I have a security agent that I've deployed on every workstation in my organization. I need to update these periodically, usually about once a quarter. I don't want to necessarily have my admin creds on all those machines. I might create a service account called svc_isagent_kt. I name it in a way that it is easily identifiable to the people that need to know what it's for. It's a service account [svc], used in Information Security [is] for an agent [agent], in our company KT Energy [kt], scv_isagent_kt. Most organizations will choose a naming protocol like this one to identify their purpose and ownership.

Service accounts are intended to provide greater security when provisioned with least privilege

This way, if it becomes compromised somehow, it will not give a miscreant access to the permissions my admin account has. I'll assign this account minimum privileges for the task it is designated to do. In this case, it is only used to push updates to this agent, so I'll provision it appropriately for that purpose. That does not mean, however, that these accounts cannot be compromised. We'll look at a scenario here that describes such a compromise.

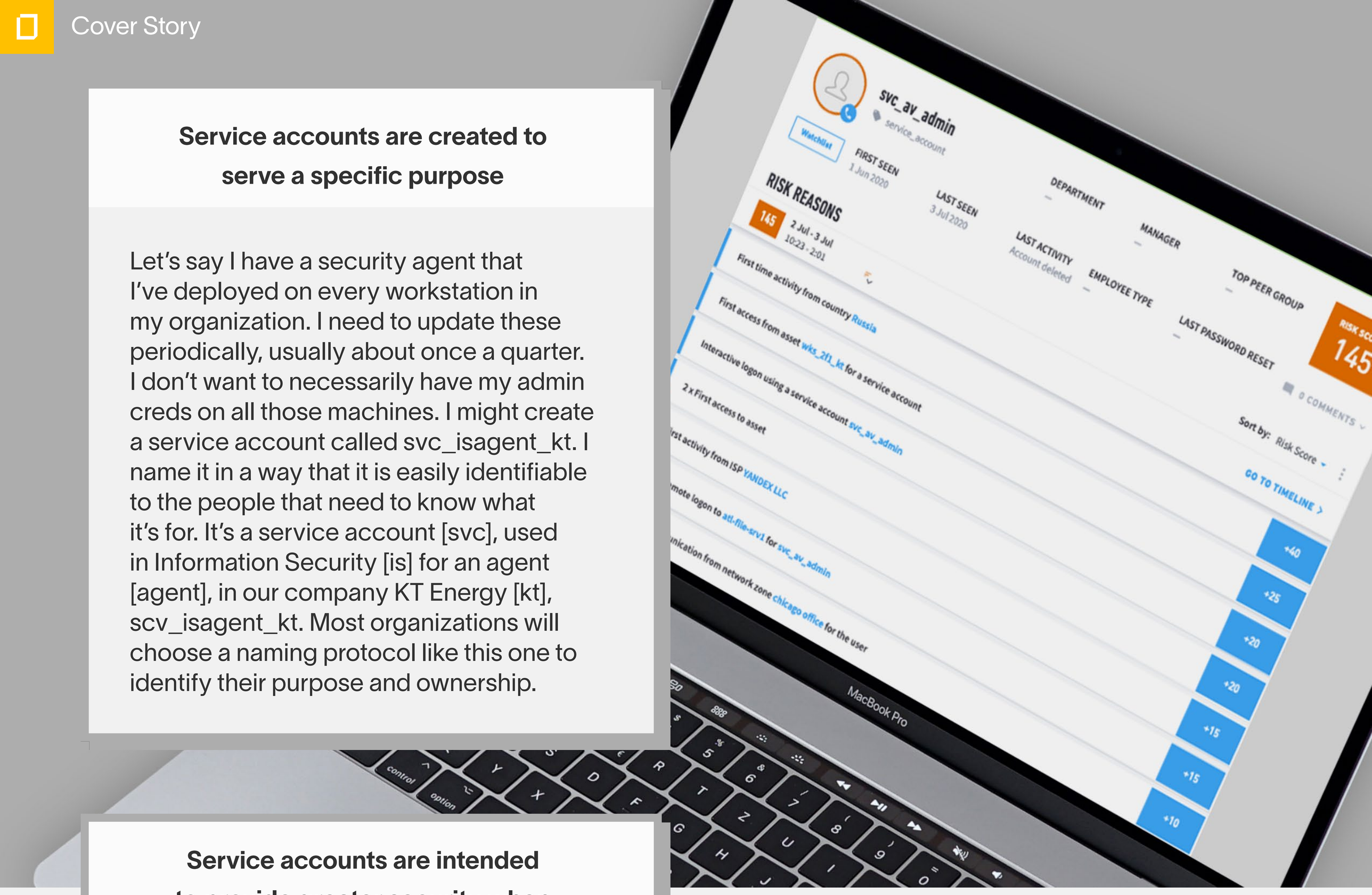


Figure 12: svc_av_admin Risk Reasons view

We can get a snapshot of the event from the Risk Reasons view. At first glance, we can see that this account is **using a VPN** to log into our network. Service accounts are not like human user accounts. This is odd for a service account, which is by its nature designed not to exist outside of your network. Next, there is an **odd login to one of our VPN servers** and then **an interactive login**. This account is then accessing new assets from a new ISP and then **accessing a file server from an odd location**. Whoever provisioned this account didn't give us too much to work with in the Active Directory. We're going to have to do some work on this one. To get as much information about this activity as possible, we'll move from the Risk Reasons view to the Timeline and construct the narrative of this event there to see if this is permitted or if this is some sort of credential compromise.

Getting started we need to know a few pieces of information about this account.

What does Active Directory tell us about this account?

Whose account is this?

What is it supposed to be used for?

What does it log into typically?

Does it have a history of generating incidents?

What is it logging into in this session and is that a risk?

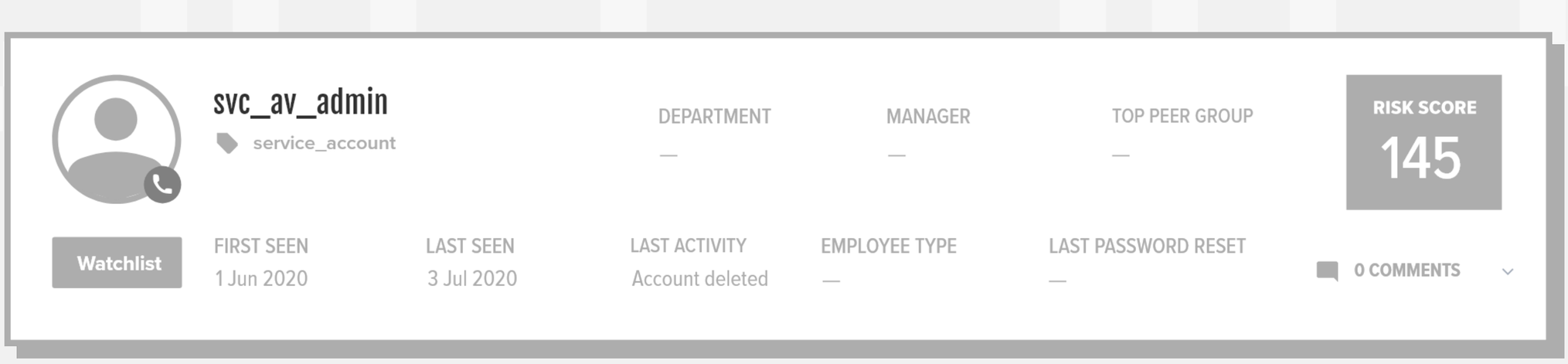


Figure 13: svc_av_admin Active Directory header

Let's take a look at what Active Directory tells us about this account. Looking at the header in the image above, we can see that AD doesn't tell us much. We don't have many of the research options for human users mentioned in the Triage section of this article.

In times where info is scarce in Active Directory, we have to identify the individuals who can help us provide context to this account.

A call to the Windows Security team informs us of a few things. The analyst working the desk gives us the following information they can see from audit logs. The account was **created June 1st, 2020**. The account was created **by Joseph McIntyre**, a Video Production Engineer. The account is **not provisioned to be able to log into assets interactively**. No service account in our organization is.

We give Joseph a call to see what the purpose of this account is. He informs us that **this account was made to give a media vendor access to their server** to deploy a newer version of their AV distribution software. He says that it was **only used in early June** and then he forgot to tell IT to deactivate the account.

This all makes sense, but the activity in the session does not, so let's see what the data tells us.

Let's head first to the account's data insights.

The assets touched by svc_av_admin tell a story. It is clear pretty quickly, just from a look at the first set of data insights, that this event was related to the Barbara Salazar event.

SAME DAY AS THE BARBARA SALAZAR EVENT!!

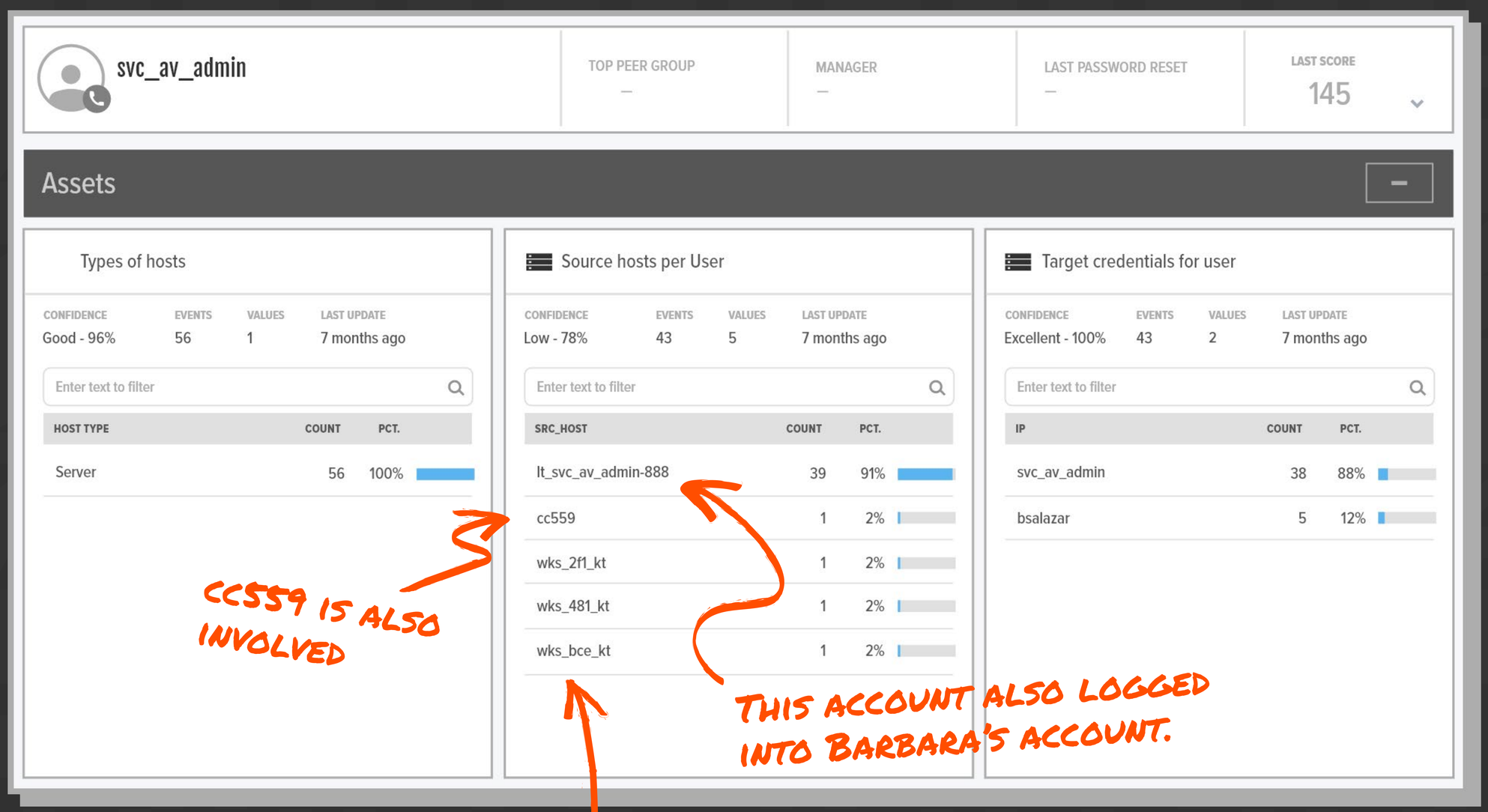


Figure 14: Data Insights, Assets view

Looking at the event in the Timeline view, we can choose to filter events in order to focus our investigation. In the Risk Reasons view, we see only the events that triggered anomaly rules. In the Timeline view, we can see all events that occurred in the session. The events in the Timeline view are grouped and are expandable. By expanding the events during our investigation, it is clear that this account has been compromised by the miscreant that compromised Barbara. Also, since we have identified that the service account should have been deactivated, we'll make a request to the Active Directory team to take this account down. If the account had still been needed we could have forced a password reset, checked to make sure that nothing else was compromised by this account, and allow the AV team to continue using it. Whether or not the account remains in use, it is very important to document findings.

CLICKING HERE SHOWS A GROUPED VIEW OF ANOMALIES

IT IS POSSIBLE TO FILTER ON CERTAIN TYPES OF ACTIVITY

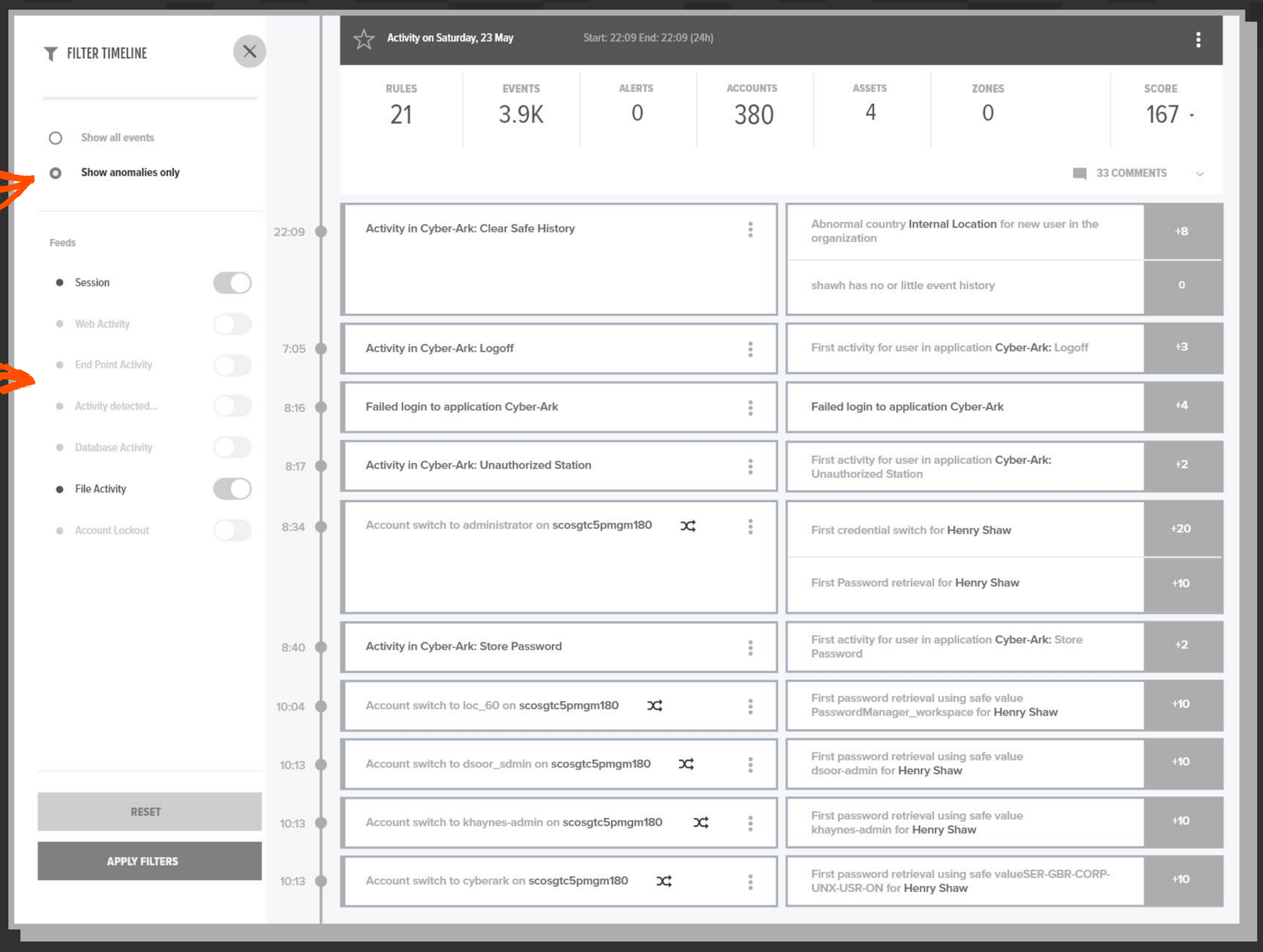
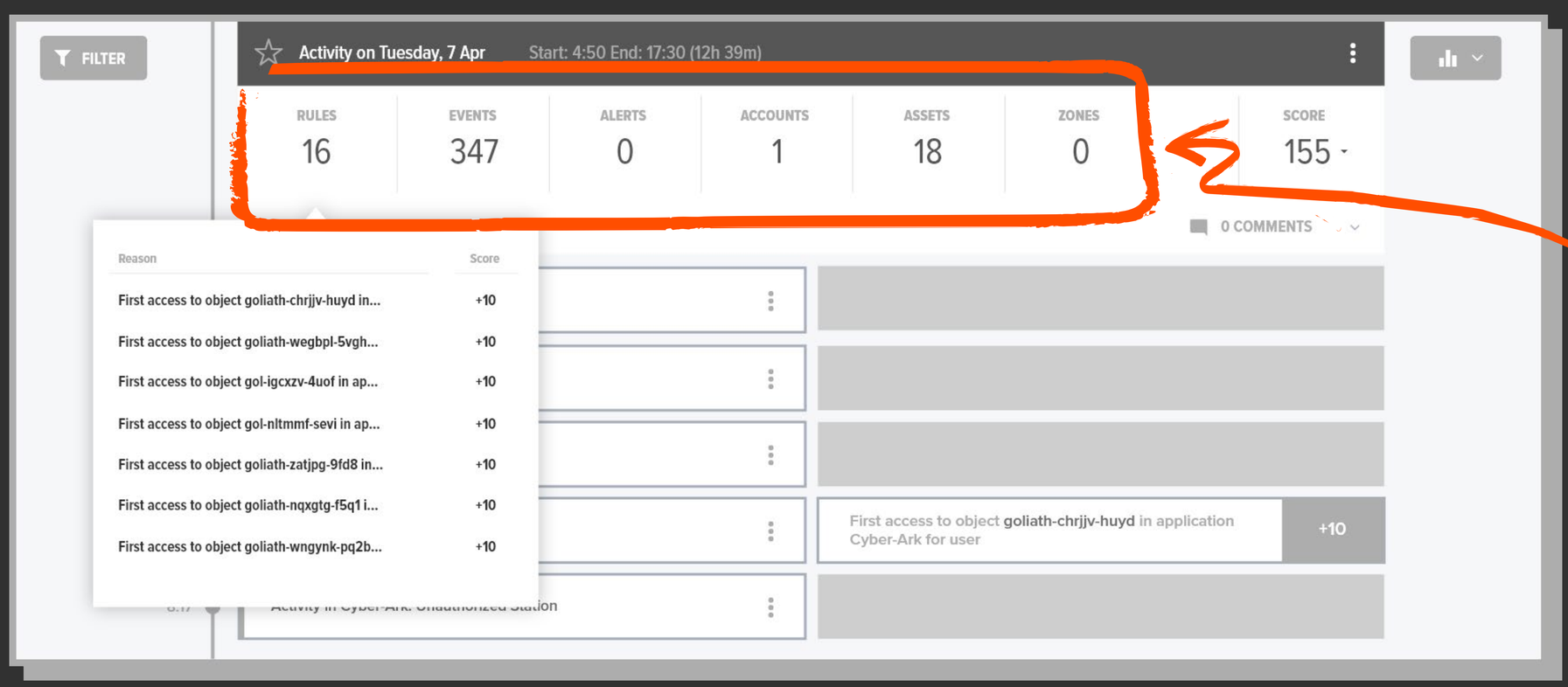
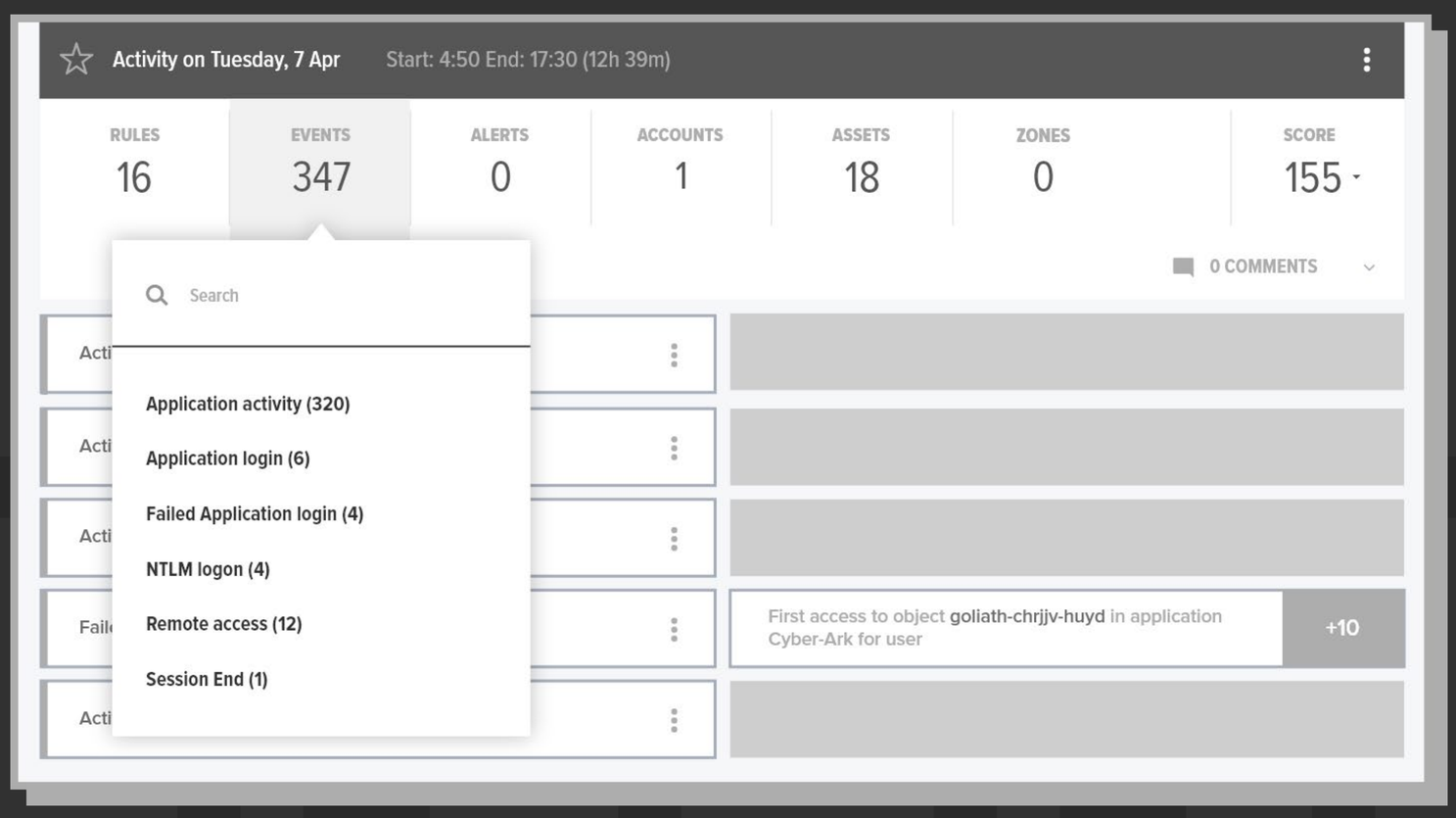


Figure 15: Timeline view with filters expanded



CLICK HERE TO FILTER FURTHER

Figure 16: Timeline view with Reasons filter expanded



FILTERING OUT NOISE STREAMLINES YOUR INVESTIGATION!!

Figure 17: Timeline view with Events filter expanded

Tracking Your Investigations

Those who cannot remember the past are condemned to repeat it, or so goes the adage. In a SOC, those who don't document their findings are condemned to repeat their work over and over. Auditors and associates charged with regulatory compliance likely will be unimpressed with either of these clever responses. Fortunately, Exabeam has a handy solution to this problem. When someone asks about the svc_av_admin account that got compromised six months from now, it won't fall on a SOC analyst's overburdened long term memory to pull out the details, they can just check **Case Manager** instead and get the facts.

Case Manager is not just a repository to store incident data, it also serves the following functions:

- A place to store playbooks, checklists, and feedback on incidents
- A management solution to coordinate escalations and inter-office investigations to ensure consistently uniform workflows
- An archive of associated user incidents to display user behavior trends
- A system of accountability to assign tasks to other users in your organization.

Open investigations are near the top of the user's profile page in Exabeam Advanced Analytics. We can tell that Barbara Salazar has a history of credential transgressions. From the number of investigations she has had it is clear that she has a pattern of laxity with regard to protecting her credentials. She has phishing investigations, the most recent compromised credential incident, and even a social engineering incident during which she passed her password to a lady with a funny accent that claimed to be from the service desk. It is clear that Barbara needs some remedial security awareness training.

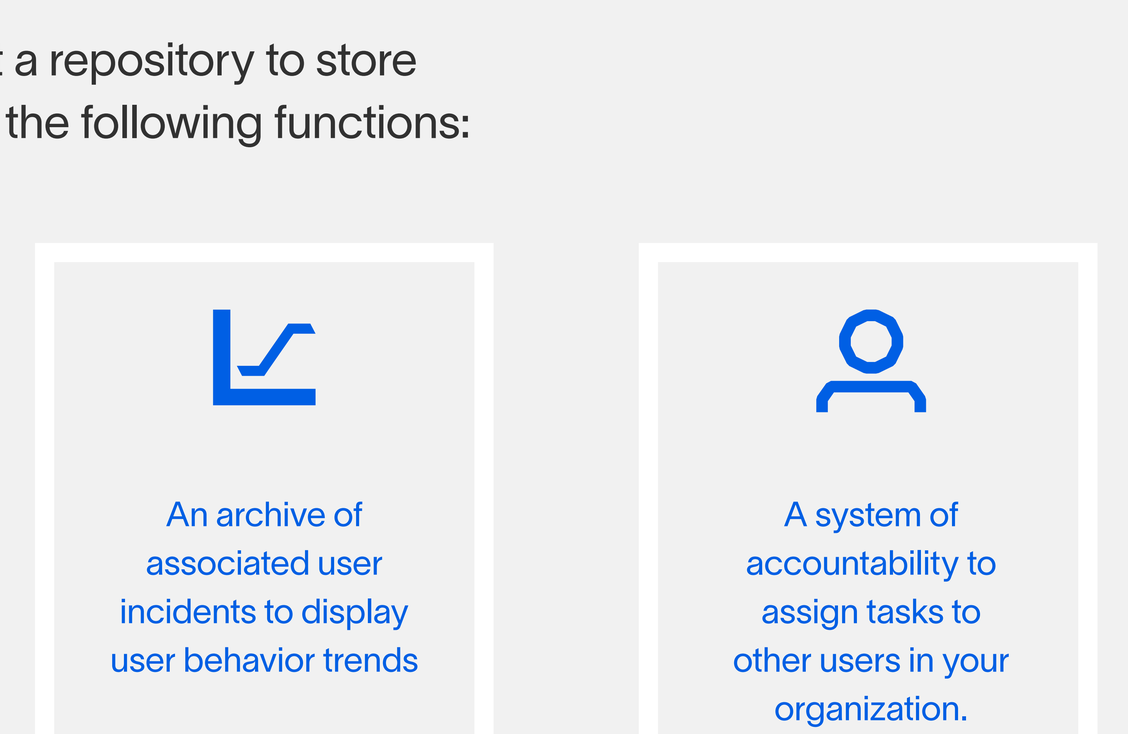
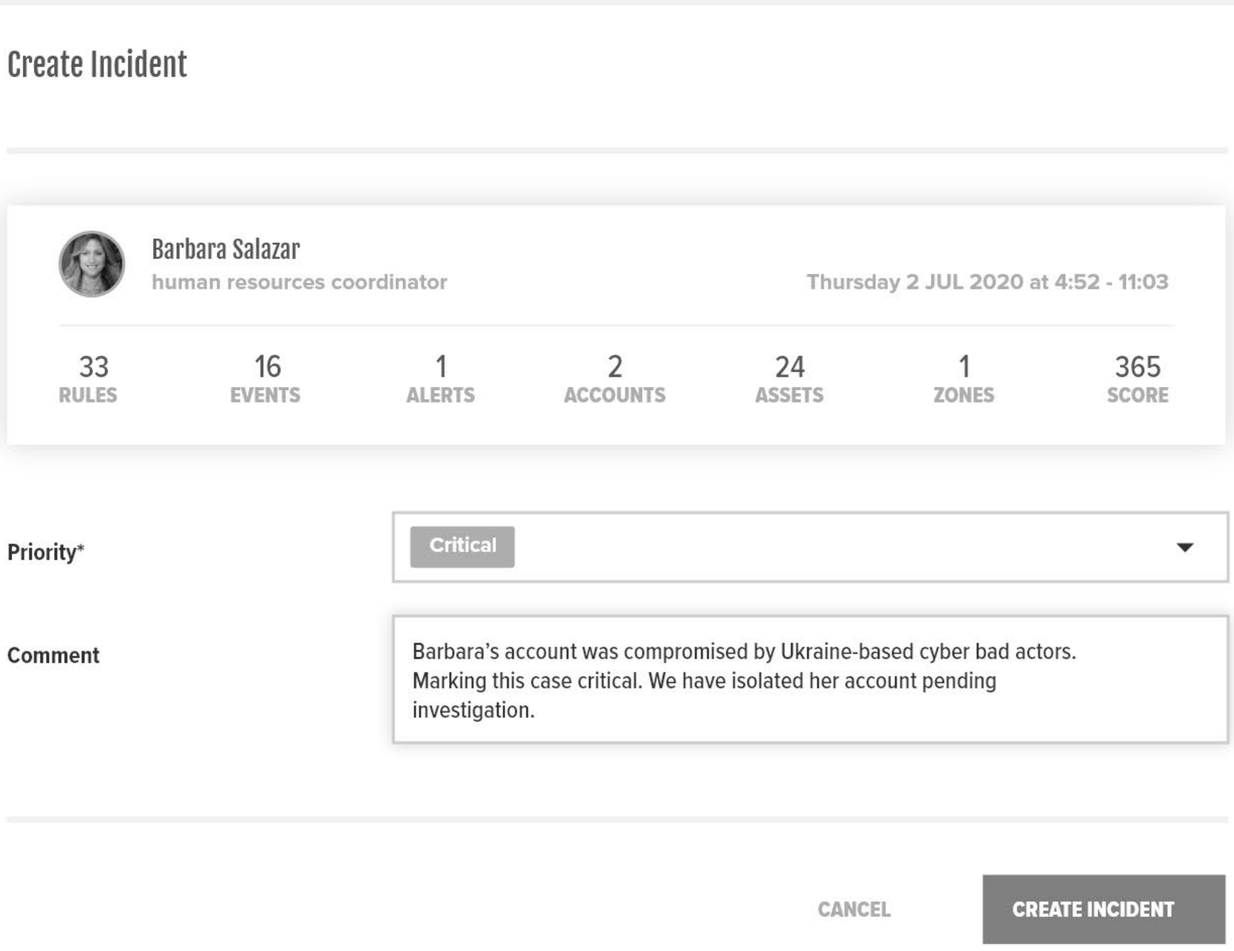


Figure 18: Barbara Salazar's open investigations



Risk Reasons view

Incidents are created when a session reaches a specified score. The default is 90 points, but this is configurable to meet your specific threshold. Incidents, or cases, can be created from the Risk Reasons view or the Timeline view under the ellipsis menu.

Figure 19: Incident creation screen

The fields in cases are likewise configurable to meet the needs of the investigation. Each step of the investigation can be tracked by any user with access to the system, and the ability to assign tasks makes sure that no one drops the ball on their specific task.

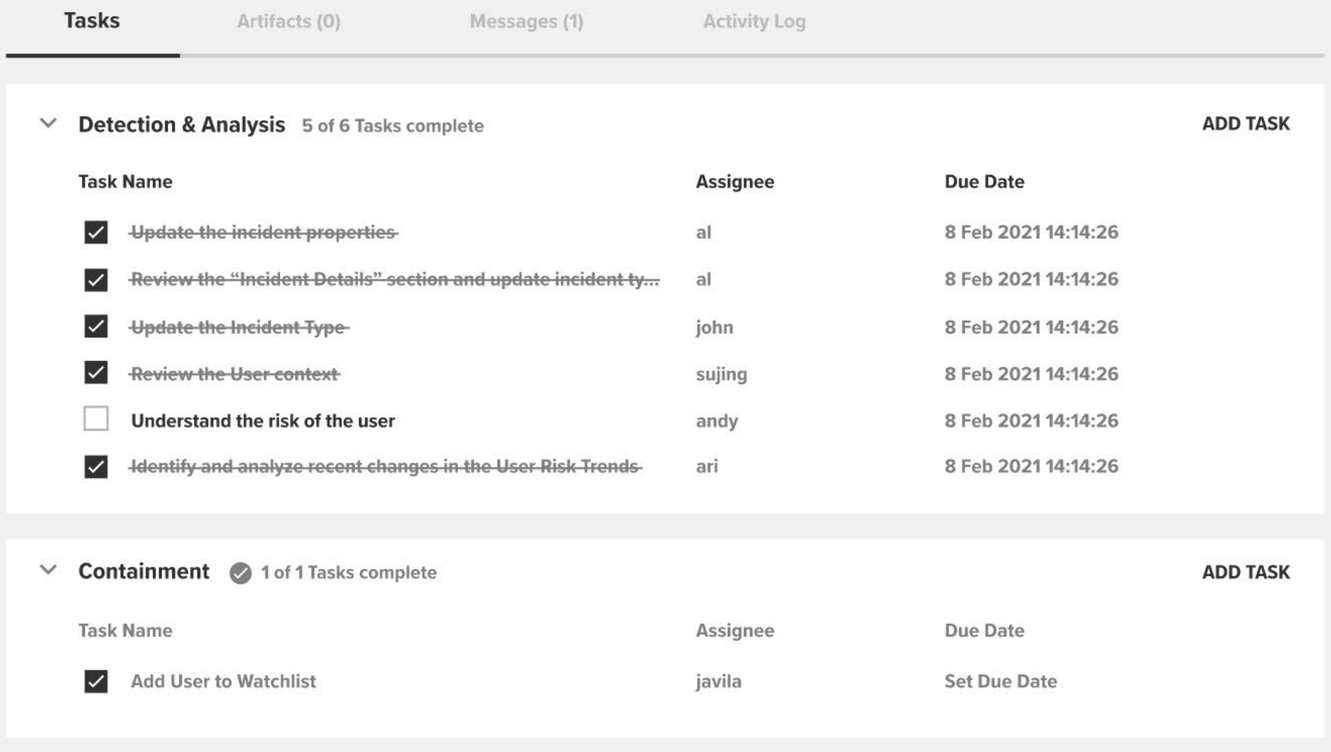


Figure 20: Adding tasks to an incident

Investigation Questions

This article speaks frequently to the importance of documenting processes. The reason for this is playbooks and workflow documentation keep everyone on the same page. No analyst can understand every event that takes place in their environment. When all stakeholders are aligned in their priorities and responses, bad behavior is less likely to be missed. Click **here** for a list of potential security questions to ask (these are useful in many investigations, not just compromised credentials). Use these to create your own custom workflow to standardize your response to different types of compromised credentials threats

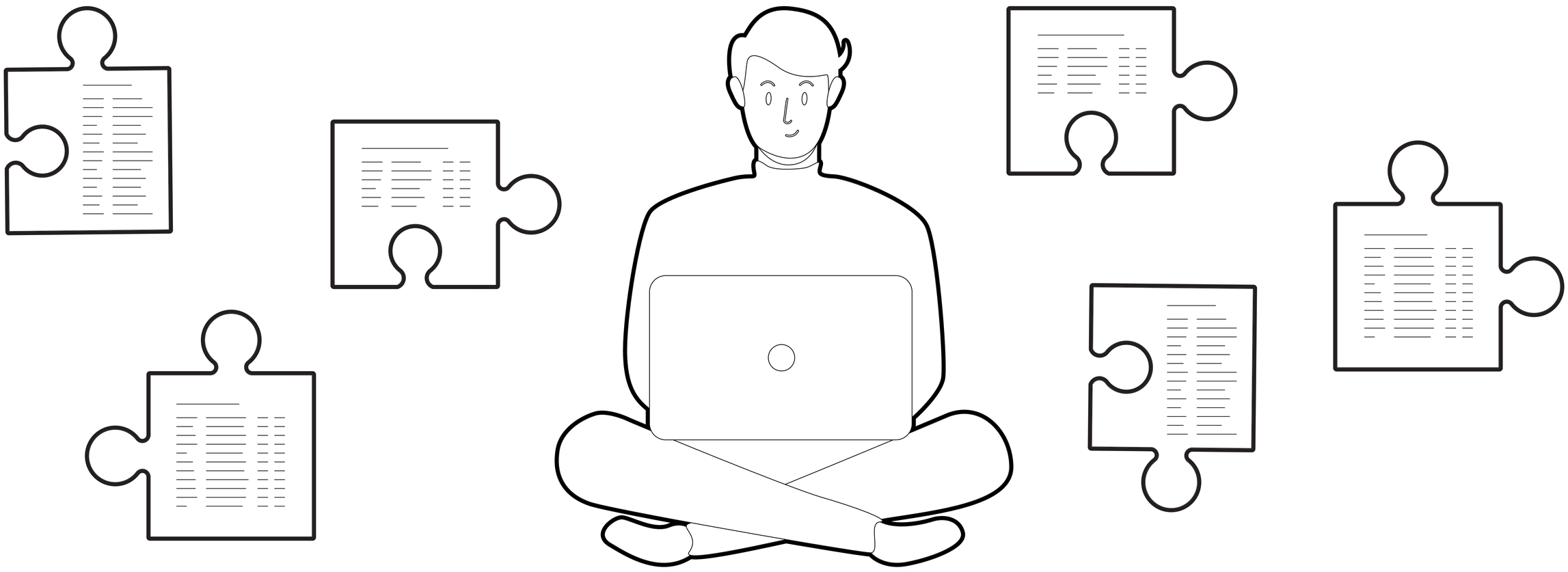
This is an excerpt from Exabeam Community. To continue reading this article, and to learn more about Compromised Credentials, view the full article **here**.

Power your security team with Exabeam education. Visit our **website** to learn more.

We offer virtual instructor led training as well as digital learning

Using Context Tables

for Leverage in Data Lake and Advanced Analytics



Exabeam Advanced Analytics out-of-the-box rules and models cover a lot of security territory, but while reviewing daily notable sessions and watchlists, there will be times when you want to detect or permit specific things. Context tables allow you to group sets of data in a single table for ease of manipulation. They are assignable variables — think lists or arrays in scripting — that hold a group of users, assets, or unique identifiers to include in rules or queries. Instead of writing out each identifier in a rule or query — say, with the user IDs of associates with a history of poor information security practices, or users from a watchlist of users with privileged accounts that would be very risky in a compromised credential situation — reference them by the context table in which they reside. Context tables are a very handy way to manage detection and permission in rules as well as Data Lake queries. Some out-of-the-box context tables are listed in the table below.

These tables map to a number of compromised credentials rules, but context tables can be used to manage detection and permission.

is_ip_threat	**reputation_domains**	**user_is_executive**	**user_is_privileged**	**workstations**

Example Scenario

Our organization, KT Energy, is considered critical infrastructure and is subject to federal, state, and local regulation and compliance requirements. A federal agency responsible for regulatory compliance in the energy sector regularly sends executives of the company notifications about advanced persistent threats and threat actors and their respective techniques. These executives are the only ones in the company that have access to critical infrastructure documents that are considered “crown jewels” and are highly protected.

Adding executives to the **user_is_executive** watchlist is an automated process that uses LDAP to generate a list of executives starting with the CEO. We can assign the number of rungs down the hierarchical ladder we want to provide enhanced monitoring for. An executive watchlist is provided out-of-the box because of their status. They are high value targets for attackers. Because of the nature of executives’ role within this business sector, we want to add value to scores when certain events occur that might indicate lateral movement to these accounts. In this case we will clone specific lateral movement rules and add an argument that if this rule triggers on a user that is included in the **user_is_executive** context table, we add a score of 200 to the session so that this is immediately responded to by the SOC. This allows the information security team to sleep better at night knowing that their coverage against an event of this type is air tight.

exabeam DATA LAKE

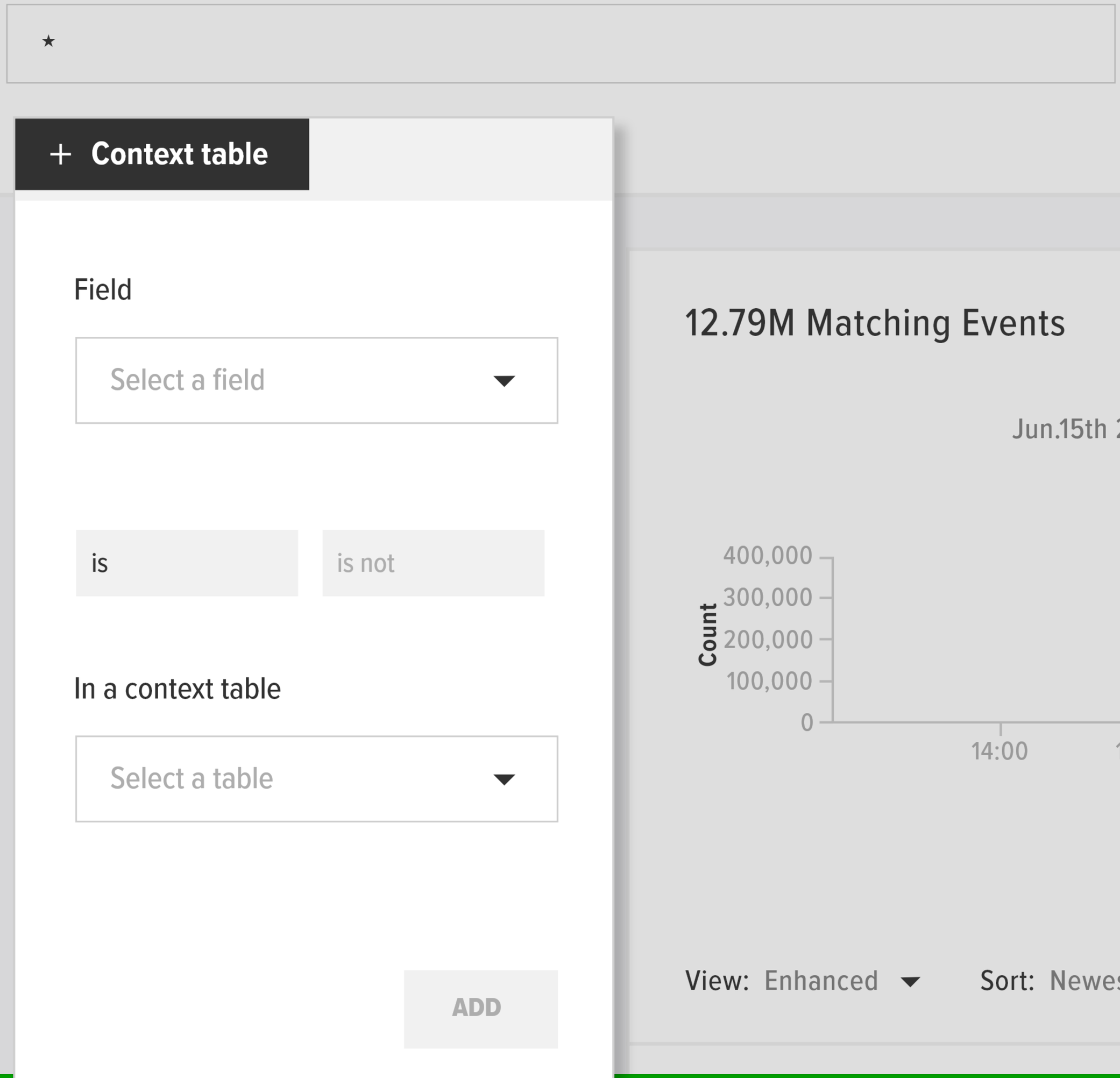


Figure 1: Creating a context table.

As with rules, context tables can also be assigned in **Data Lake** in order to efficiently query on groups of identifiers without having to list them individually in the query. In the scenario above, your team might want to know which contractors are showing up on the known list of IPs. As mentioned above, any set of data identifiers from any field in your logs can be added as a filter to your query in Data Lake.
Pretty cool eh?

Instructions on how to use context tables in your threat hunting is located in the Data Lake User Guide.