exabeam

WHITE PAPER

UNLOCKING EFFECTIVE THREAT DETECTION AND INVESTIGATION WITH ANALYTICS AND TTPs

How UEBA and MITRE ATT&CK Techniques Significantly Improves SOC Productivity

INTRODUCTION

AS FIRST RESPONDERS, SECURITY ANALYSTS ARE PAINFULLY AWARE THAT THE COMPLEXITY OF CYBERATTACKS IS ON A STEEP RISE.

Exploits are also getting more automated as attackers leverage tools to simultaneously assail related vulnerabilities in a vast range of targets. Security operations center (SOC) teams are struggling to keep up — furiously switching between various tools as they attempt to investigate, contain, and respond to security alerts — all while hoping nothing slips through the cracks.

Breaches continue so it's prudent to consider augmenting legacy approaches to threat detection. SOCs not only need the appropriate tools; they also need a standard way to communicate and collaborate about the attacks to which they are detecting, investigating and responding. This white paper describes how the MITRE ATT&CK framework enables this objective. It provides a common taxonomy for understanding the various tactics, techniques and procedures (TTPs) adversaries employ and how to use them for more effective threat detection efforts. The paper also describes enhanced results when adding behavioral analytics to threat detection with MITRE ATT&CK by using capabilities in Exabeam SIEM.

WHAT ARE TTPs, WHY SHOULD WE USE THEM?

Tactics, techniques and procedures (TTPs) provide a description of activities used by an adversary. They describe the "what and how" of an attack. Using TTPs enables security analysts to look for attack patterns instead of the artifacts left after as a result of an attack. Attack artifacts are often referred to as "indicators of compromise" (IOCs); they are merely pieces of evidence observed on a network or on operating systems that indicate some level of intrusion has occurred.

The figure below shows the varying levels of effort needed to detect different types of threat indicators. In the diagram, all levels below "Tools" represent IoCs. While they are easiest to spot, using IoCs for threat detection has several drawbacks. For example, IoCs are inherently reactive, so they are usually valid just for a short period of time as hackers change their attack infrastructure to avoid detection. IoCs also lack context about what a hacker was trying to achieve. Reasons like these make IoCs prone to high rates of false positives when used for threat detection.

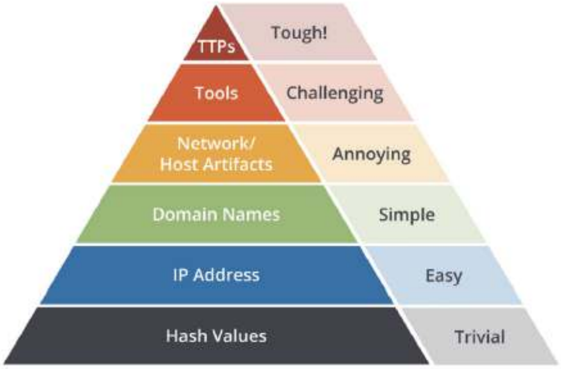


FIGURE 1 – PYRAMID OF PAIN, SHOWING THE LEVEL OF EFFORT REQUIRED TO DETECT DIFFERENT TYPES OF THREAT INDICATORS

Source: http://detect-respond.blogspot.com/2013/03/the-pyramid- of-pain.html

IoCs are also ineffective for threat hunting because there are so many of them. An attack's forensics typically show hundreds or thousands of IoCs, and sometimes many more. As you go up the pyramid, the threat indicators become more valuable, but also more difficult to detect. This paper will describe how to use TTPs instead of IoCs to greatly improve detection and threat hunting efficacy, and how to leverage behavioral analytics to further compound the effectiveness of this approach. It revolves around hunting threats and attack patterns with behavioral analysis guided by the MITRE ATT&CK framework.

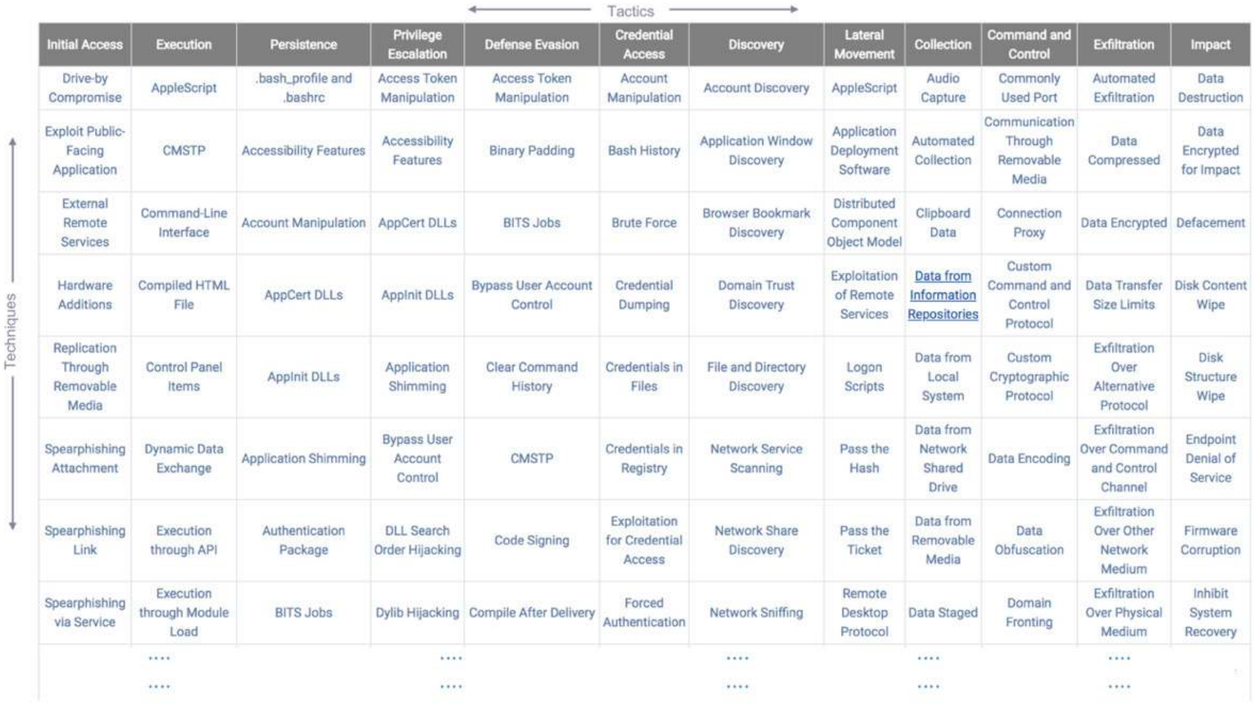
SOC teams require a common framework that aligns TTPs with their security tools and provides a standard language to use when hunting for threats and discussing attack patterns.

WHAT IS THE MITRE ATT&CK FRAMEWORK?

MITRE ATT&CK maps tactics, techniques, and procedures used by adversaries cataloged in millions of attacks on enterprise networks and systems to a common framework. It provides a common taxonomy and knowledge base that the security community can use in communication, as well as in their efforts for detection, investigation and response. This functional junction also helps security vendors to design threat hunting tools and detection methods capable of identifying specific tactics and techniques within the framework.

MITRE ATT&CK organizes TTPs into a simple matrix. Tactics are listed across the top, with individual techniques that achieve that tactic listed below in each corresponding column. Tactics are presented from left to right in the general order of an attack sequence.

FIGURE 2 – THE MITRE ATT&CK FRAMEWORK ORGANIZES HACKING TACTICS AND TECHNIQUES INTO A MATRIX. TACTICS SPAN THE TOP ROW, AND THE TECHNIQUES THAT CAN ACHIEVE THAT TACTIC ARE LISTED BELOW IN EACH COLUMN.


Tactics
Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
	....		....			....		....		....	
	....		....			....		....		....	

HOW TO USE THE MITRE ATT&CK FRAMEWORK?

Security analysts often wish to associate security events and abnormal activities with the relevant threat actors, intrusion sets and campaigns. This could be for threat hunting, incident investigation or general knowledge building. To that end, MITRE ATT&CK is the common knowledge base that maps different tactics and techniques used in attacks to the threat groups[1] and tools associated with them. Analysts can also find the tactics used by these groups should they want to search for potential activity by specific threat actors.

For example, by looking up APT3[2] in the ATT&CK database, one learns that the attack group is associated with the Chinese military and primarily targets U.S. government organizations and political organizations in Hong Kong. The database also notes this group has used LaZagne, PlugX, SHOTPUT, and RemoteCMD software in their past attacks.

In addition to being an effective learning tool and a common framework for analysts to communicate about attacks, MITRE ATT&CK is also useful for guiding the detection, investigation, and threat hunting efforts of analysts.

[1] https://attack.mitre.org/groups

[2] https://attack.mitre.org/groups/G0022/

DETECTING ABNORMAL TTPs WITH BEHAVIOR ANALYTICS

And now for the tricky part: while TTPs are a good thing for analysts because they illustrate how an attack happens, the digital evidence alone revealing TTPs cannot tell you if that activity is related to specific malicious action – or should be attributed to normal workflow performed by enterprise users.

For example, analysts are familiar with how attackers maliciously leverage processes for account creation, screensaver activity, remote desktop access, and many more. These are normal everyday activities in enterprise IT but they can also be used for hacking. **To distinguish the bad from the good, MITRE-related tools used by SOC analysts must be smart enough to detect and alert only when the behavior is malicious or has bad intent. The inability to make this distinction means analysts will end up with a lot of false positives!**

Behavioral analytics monitors all user and asset behavior with machine learning to understand what behavior is normal. This application of AI is what enables deviations from normal, and accurate detection of malicious TTPs. Exabeam's user and entity behavior analytics (UEBA) capability leverages TTPs defined in the MITRE ATT&CK framework to tag anomalous events to make it easier for security analysts to hunt for threats.

For example, consider an attacker logging onto a service designed to accept remote connections, such as telnet, SSH, or VNC. An adversary typically uses this technique to access the network and then move laterally within to attack high-value assets. This approach is a TTP, defined as Remote Services[3] in MITRE ATT&CK framework. With a legacy SOC tool TTP detection would be created using a static correlation rule. Once configured all occurrences of remote connections would be flagged by this rule because static correlation rules have no understanding of the normal operating circumstances that may involve remote connections. As a result this rule would create a large number of false positives, and consequently likely cause analysts to ignore alerts generated by the rule. However, combining MITRE ATT&CK detection with user and behavior analytics can help analysts home in on TTPs which occur in their environment that are genuinely abnormal, and thus more likely to represent real threats.

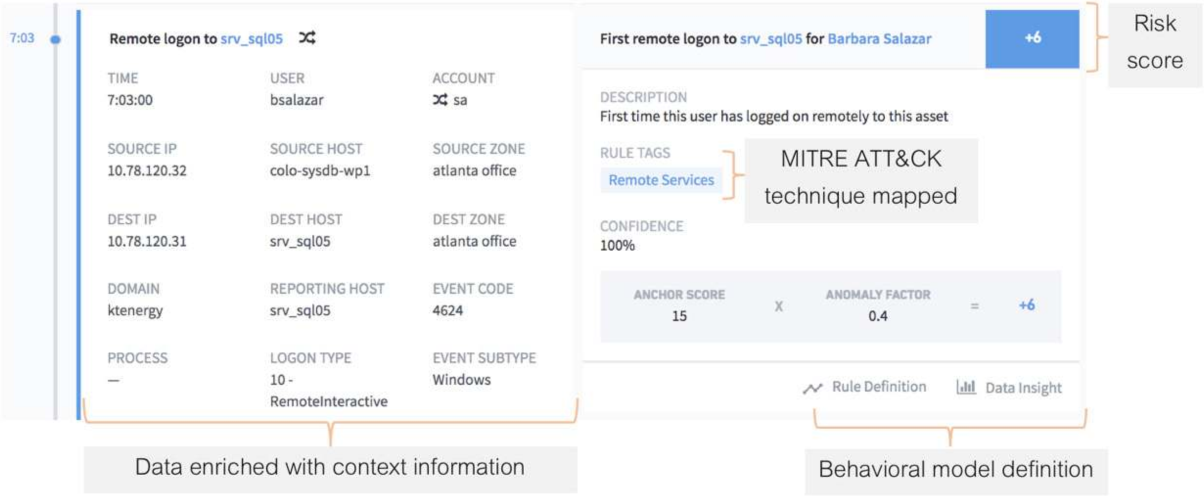
Exabeam has developed behavior analysis[4] to learn the behavior of users and assets. The ML-based models establish a baseline of an organization's normal behavior, enabling algorithms to easily detect deviation from the baseline. For example, assume the model detects that it's the first time a user has remotely logged onto a particular SQL server. Since this has never occurred before, it inherently carries more risk than an activity that happens regularly. Figure 3 shows a screenshot from Exabeam Advanced Analytics which shows an abnormal remote login. It displays the event risk score, MITRE technique used and the context dynamically built around the user and assets in question. The SOC analyst is provided with complete, contextually enriched information about this behavior with the risk reasons and evidence for this alert. No more guessing the meaning of obscure alerts and trace data!

Behavior analysis is used to track deviation from normal baseline behavior and to detect threats in real time.

[3] https://attack.mitre.org/techniques/T1053

[4] https://www.exabeam.com/siem/siem-threat-detection-rules-or-models/

FIGURE 3 – EXABEAM ADVANCED ANALYTICS FLAGGING A FIRST-TIME LOGON TO A SERVER BY THE USER AS ANOMALOUS. THIS IS SHOWN AS PART OF THE USER TIMELINE ALONG WITH THE MITRE TECHNIQUE TAGGED "REMOTE SERVICES", THE RISK SCORE, AND CONTEXTUAL INFORMATION SURROUNDING THE EVENT.



7:03

Remote logon to srv_sql05

TIME 7:03:00
USER bsalazar
ACCOUNT sa
SOURCE IP 10.78.120.32
SOURCE HOST colo-sysdb-wp1
SOURCE ZONE atlanta office
DEST IP 10.78.120.31
DEST HOST srv_sql05
DEST ZONE atlanta office
DOMAIN ktenergy
REPORTING HOST srv_sql05
EVENT CODE 4624
PROCESS —
LOGON TYPE 10 - RemoteInteractive
EVENT SUBTYPE Windows

First remote logon to srv_sql05 for Barbara Salazar +6

DESCRIPTION
First time this user has logged on remotely to this asset

RULE TAGS
Remote Services

CONFIDENCE
100%

ANCHOR SCORE 15 x ANOMALY FACTOR 0.4 = +6

Rule Definition
Data Insight
Risk score
MITRE ATT&CK technique mapped
Data enriched with context information
Behavioral model definition

Exabeam Advanced Analytics does not flood the SOC dashboard with individual alerts, since the occurrence of a TTP by itself does not provide enough proof that it's a threat. This is where the user timeline comes into play. The next section describes how the Exabeam timeline automatically aggregates all relevant events and alerts along with contextual information to give a complete picture of the attack.

> An alert of a TTP by itself does not provide proof of an attack. Analysts need to understand the context in which it occurred—ideally in an incident timeline—to get a complete picture of the threat.

INVESTIGATING AN ATTACK WITH EXABEAM AND THE MITRE FRAMEWORK

The incident timeline provided by Exabeam, called a Smart Timeline™, is the operational point of integration with the MITRE framework. Instead of becoming distracted by potentially irrelevant TTPs, the timeline provides useful one-click access to all of the context surrounding a potentially damaging incident. To understand how a timeline helps with threat investigation, let's consider its functional attributes.

The Smart Timeline automatically stitches together all behavior by users and assets and contextually presents the data within the timeline with highlighted risk reasons and risk scores. Exabeam enriches the data with context from various sources such as AD, LDAP, host-to-IP mapping and dynamic peer grouping.

Visual presentation of these data makes it easier to see the full attack pattern. Legacy tools tend to swamp SOC analysts with an alert for every technique used. This creates an impractical situation where analysts have to manually assemble these disparate alerts to hopefully make sense of a situation – whether or not malicious activity actually exists. For analysts in a large organization getting thousands of alerts daily, be assured that hope plays a major role in successful threat investigation! The Exabeam Smart Timeline gives investigators all the evidence they need with pinpoint accuracy. It reduces both false positives and mean time to detect/respond to real threats.

To enable collaboration, Exabeam has labeled TTPs that are identified in the MITRE ATT&CK framework. This helps to show where specific events map to the overall framework (i.e. tactics, and the kill chain). MITRE labels include a description of the attack and a link to the framework. Having direct hyperlinks to the MITRE ATT&CK knowledge base for any abnormal TTPs discovered helps analysts understand the implications of the techniques they detect and provides them with a resource for additional learning.

THREAT INVESTIGATION COMPARED

Legacy Indicators of Compromise vs. Exabeam Advanced Analytics & TTPs

	IoC-based Threat Investigation	Advanced Analytics & TTP-based Threat Investigation
Detect	Alert-based. Prone to false positive rates due to the high number of IoCs and their short-lived window of effectiveness.	Detects based on abnormal behaviors. Zeroes in on abnormal occurrences of TTPs.
Search	Query language-based. Analysts usually search for known IoCs. Results are raw logs.	Intuitive, point-and-click UI interface. Analysts can search for TTPs or IoCs. Results are machine build timelines.
Pivot	Analysts must deeply understand the attack they are looking for to create a new query capable of retrieving the proper result.	No need to understand the underlying attack change search parameters. Can search by MITRE ATT&CK tags to quickly zero in on abnormal occurrences of specific techniques or tactics.
Prioritize	Analysts must manually determine which alerts are worthy of further investigation. High numbers of alerts and low contextual information often result in wasting investigation cycles on false positives.	Automatically identifies abnormal TTPs and sorts them by risk score to prioritize the highest risk items for analyst review.
Investigate	Analysts must manually determine which alerts are worthy of further investigation. High numbers of alerts and low contextual information often result in wasting investigation cycles on false positives.	Automatically identifies abnormal TTPs and sorts them by risk score to prioritize the highest risk items for analyst review.

Practical Example: Detecting an Exfiltration Attack

Consider the scenario of an exfiltration attack pattern. An attacker gets initial access to an internal enterprise asset, does a privileged account switch to a service account, moves laterally to find the host where sensitive data is held, logs into the host with the service account and uploads the data outside of the enterprise. Let us peel back this attack chain and look at the auto-assembled timeline to give investigators a complete story. In sequence:

1. An attacker uses external remote services like VPN to connect to internal enterprise assets from external locations. This technique can be mapped to External Remote Services (T1133)[5] per the MITRE framework. Exabeam is able to detect this event as anomalous based on the model which tracks all the external locations a user typically logs in from. Variations are deemed abnormal.
2. An attacker does an account switch to a service account in order to obtain privileged access and gain a foothold to key assets in the organization. This is termed as Account Manipulation (T1098)[6] that usually consists of modifying permissions, credentials, permission groups or account settings.
3. Next, an attacker logs into a database server using the service account. This technique is mapped to Remote Services (T1021)[7] per the MITRE framework. The adversary is also shown using Valid Accounts (T1078)[8] technique, which is typically done together by the adversary to laterally move across different assets after gaining credentials. There are many models for detecting these techniques.
4. As a last step, the adversary runs queries to collect data from the database server and uploads them to an external location. There are various methods of exfiltration as defined by MITRE, and in this example it's mapped to the Exfiltration over Alternative Protocol (T1048)[9] technique, where data exfiltration is performed using protocols such as FTP, SMTP, HTTP/S and other networking protocols.

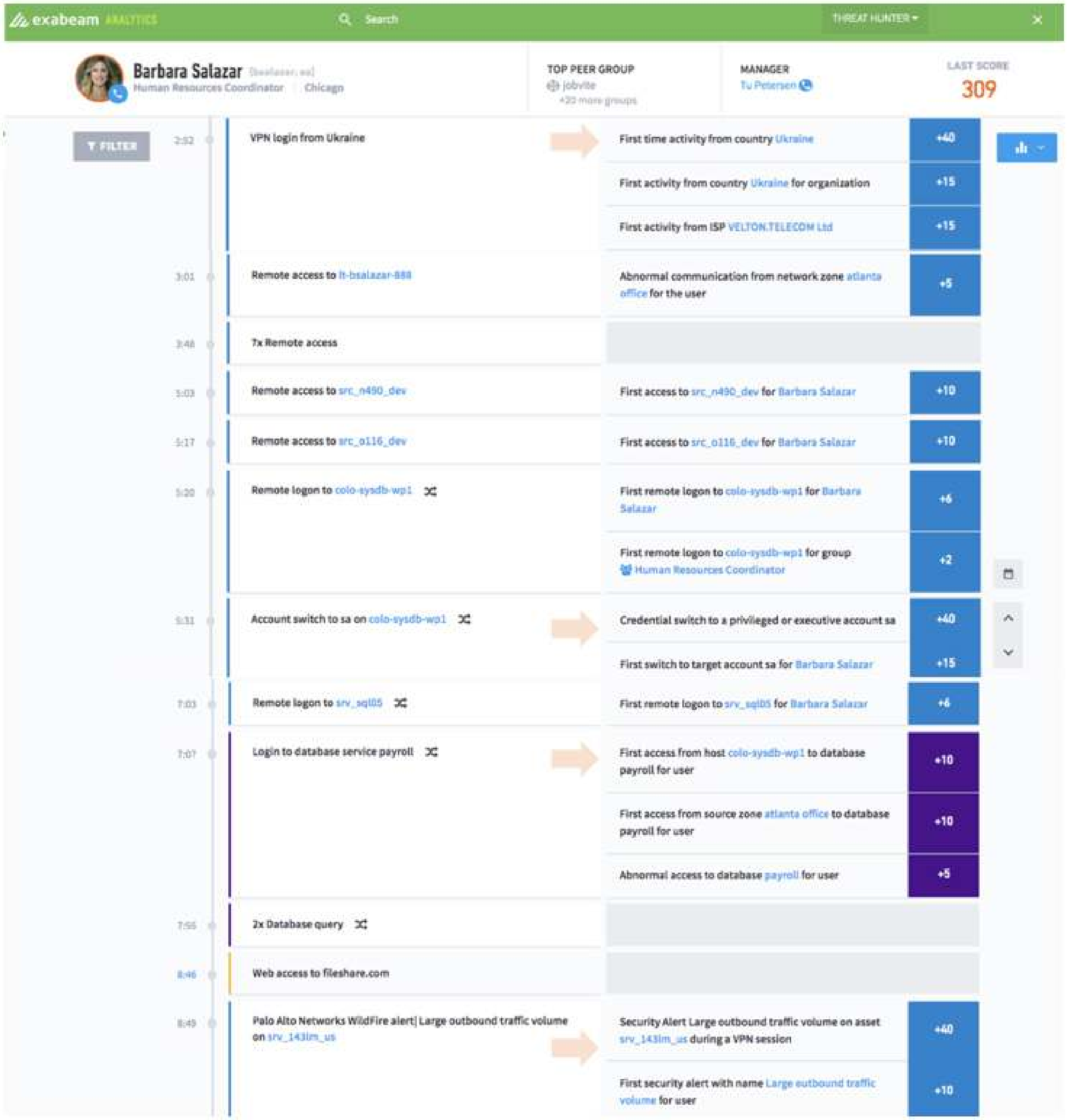
In the above sequence, many of these TTPs would have at some point set off alerts in most SOCs. With legacy tools, many of the alerts would have to be investigated with a manual assembly of the evidence in order to get a complete picture of the attack chain. By the time analysts make sense of the alerts and assemble the evidence, the attacker will have gained deeper access into the organization's network and systems. It's probably too late to undo the damage.

There is an easier, reliable way to surmount these issues. SOC analysts need a controlled, enriched and complete timeline of events to accurately pinpoint all the anomalous events before they result in a breach. Exabeam provides this capability with Smart Timelines[10] by including all the events – normal and abnormal – and automatically stitching them together along with associated risk reasons and risk scores. Figure 4 shows the Smart Timeline for the above attack scenario. The arrows indicate the techniques as discussed in the scenario above.

Smart Timelines make investigations and incident response more effective, which makes security analysts smarter. If the risk score of a user or device crosses a preset threshold, it's flagged as notable and is prominently listed on the SOC dashboard to help prioritize investigations.

[5] https://attack.mitre.org/techniques/T1133
[6] https://attack.mitre.org/techniques/T1098/
[7] https://attack.mitre.org/techniques/T1021/
[8] https://attack.mitre.org/techniques/T1078/
[9] https://attack.mitre.org/techniques/T1048/
[10] See Exabeam Smart Timelines white paper – https://www.exabeam.com/library/exabeam-smart-timelines/

FIGURE 4 - AN EXABEAM SMART TIMELINE SHOWING ACCOUNT SWITCH ACTIVITY, LATERAL MOVEMENT AND DATA EXFILTRATION, ALL TIED TOGETHER AUTOMATICALLY TO MAKE INVESTIGATIONS EASIER. THE ARROWS SHOWN INDICATE THE TECHNIQUES THAT ARE DISCUSSED IN THE ABOVE SCENARIO.



Barbara Salazar (bsalazar, aa)
Human Resources Coordinator | Chicago

TOP PEER GROUP
jobvite
+20 more groups

MANAGER
Tu Petersen

LAST SCORE
309

2:52	VPN login from Ukraine	First time activity from country Ukraine	+40
		First activity from country Ukraine for organization	+15
		First activity from ISP VELTON.TELECOM Ltd	+15
3:01	Remote access to lt-bsalazar-888	Abnormal communication from network zone atlanta office for the user	+5
3:46	7x Remote access		
5:03	Remote access to src_n490_dev	First access to src_n490_dev for Barbara Salazar	+10
5:17	Remote access to src_o116_dev	First access to src_o116_dev for Barbara Salazar	+10
5:20	Remote logon to colo-sysdb-wp1	First remote logon to colo-sysdb-wp1 for Barbara Salazar	+6
		First remote logon to colo-sysdb-wp1 for group Human Resources Coordinator	+2
5:31	Account switch to sa on colo-sysdb-wp1	Credential switch to a privileged or executive account sa	+40
		First switch to target account sa for Barbara Salazar	+15
7:03	Remote logon to srv_sql05	First remote logon to srv_sql05 for Barbara Salazar	+6
7:07	Login to database service payroll	First access from host colo-sysdb-wp1 to database payroll for user	+10
		First access from source zone atlanta office to database payroll for user	+10
		Abnormal access to database payroll for user	+5
7:56	2x Database query		
8:46	Web access to fileshare.com		
8:49	Palo Alto Networks WildFire alert| Large outbound traffic volume on srv_143lm_us	Security Alert Large outbound traffic volume on asset srv_143lm_us during a VPN session	+40
		First security alert with name Large outbound traffic volume for user	+10

THREAT HUNTING WITH BEHAVIORAL ANALYTICS AND TTPs

Exabeam's user and entity behavior analytics (UEBA) solution brings threat hunting and the MITRE ATT&CK framework to fast, accurate and powerful results. Exabeam Threat Hunter provides an intuitive point-and-click UI capable of performing detailed searches without a need to write complex queries to hunt for threats. Behavior analytics allows analysts to zero in on abnormal TTPs, as opposed to all of the TTPs occurring in an environment. Threat Hunter search results not only contain the alerts the investigator is looking for, but the complete Smart Timeline with all risk reasons, risk scores, all events tied together and rule tags mapped to MITRE techniques. This is a vastly more efficient way to threat hunt when compared to the traditional IoC-based approach taken by legacy tools and traditional SIEMs (see figure 5 below). The integration dramatically reduces mean-time-to-response (MTTR) as analysts are presented with key evidence – machine-built timelines for every user and device in your enterprise.

With Advanced Analytics as the foundation layer for threat detection, Smart Timelines for rapid investigation, and Threat Hunter to easily hunt for abnormal TTPs. Exabeam greatly reduces mean-time-to-response (MTTR).

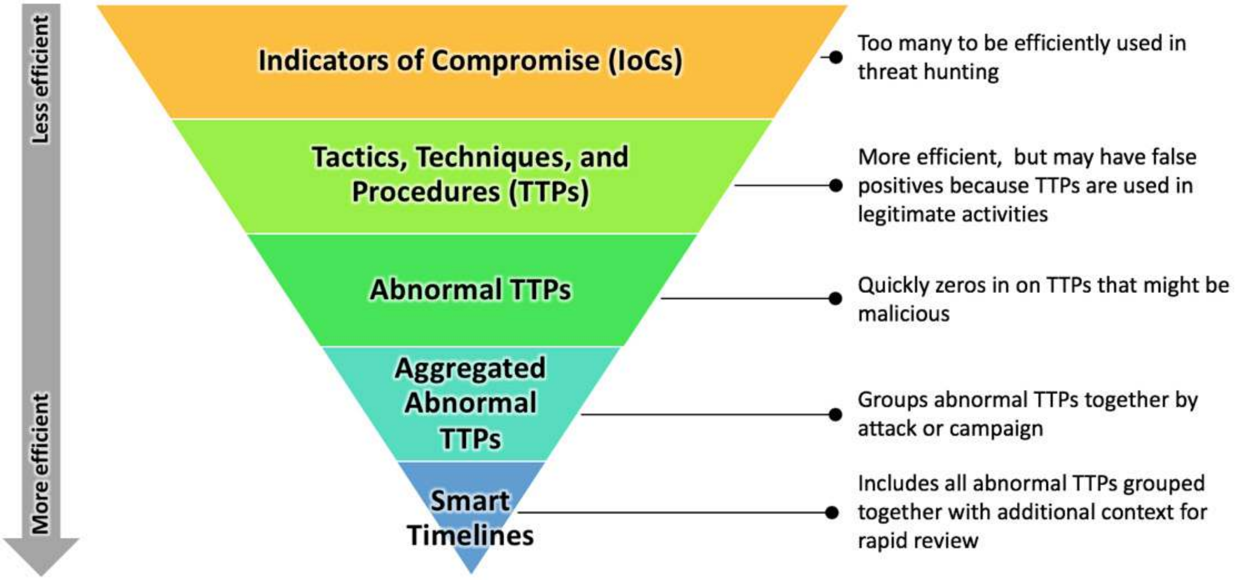

Less efficient
More efficient
Indicators of Compromise (IoCs)
Too many to be efficiently used in threat hunting
Tactics, Techniques, and Procedures (TTPs)
More efficient, but may have false positives because TTPs are used in legitimate activities
Abnormal TTPs
Quickly zeros in on TTPs that might be malicious
Aggregated Abnormal TTPs
Groups abnormal TTPs together by attack or campaign
Smart Timelines
Includes all abnormal TTPs grouped together with additional context for rapid review

FIGURE 5 - SHOWS THE EFFICIENCY OF VARIOUS THREAT HUNTING APPROACHES, RANKED FROM LEAST TO MOST EFFICIENT.

CONCLUSION

Time is of the essence for detecting and resolving security threats. The rising sophistication of attack sequences is ill-met by legacy tools used by SOCs. The old way of manually addressing a deluge of alerts and manually attempting to stitch together an event timeline is slow and impractical – if it works at all. Legacy tools and IoC-based approaches make it difficult for an analyst to quickly and fully understand the scope of an incident when there are multiple users, processes, devices, and network connections involved. Resolving the attack sequences requires SOC analysts to see the complete picture. By using a modern approach in Exabeam of ML-based behavioral analytics to identify activity as anomalous and risky, and automatically mapping those to the techniques identified in the MITRE ATT&CK framework, responders can now quickly detect, trace and respond to the steps an attacker has taken before they cause significant damage to an organization.

FURTHER READING

- Mitigating Security Threats with MITRE ATT&CK
- MITRE Publishes Domain Generation Algorithm T1483 in the ATT&CK Framework
- Using the MITRE ATT&CK Knowledge Base to Improve Threat Hunting and Incident Response
- Why Understanding the Entire Attack Chain Before Responding is Critical

ABOUT US

Exabeam is the Smarter SIEM™ company. We help security operations and insider threat teams work smarter, allowing them to detect, investigate and respond to cyberattacks in 51 percent less time. Security organizations no longer have to live with excessive logging fees, missed distributed attacks and unknown threats, or manual investigations and remediation. With the modular Exabeam Security Management Platform, analysts can collect unlimited log data, use behavioral analytics to detect attacks, and automate incident response, both on-premises or in the cloud. Exabeam Smart Timelines, sequences of user and device behavior created using machine learning, further reduce the time and specialization required to detect attacker tactics, techniques and procedures. For more information, visit www.exabeam.com.

TO LEARN MORE ABOUT HOW EXABEAM CAN HELP YOU, VISIT EXABEAM.COM TODAY.