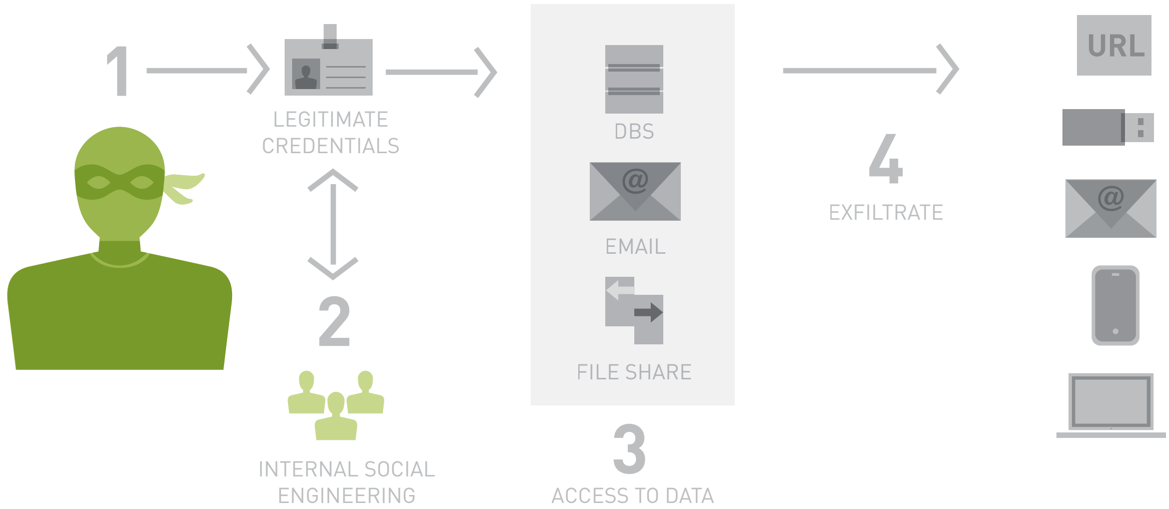
FORTSCALE
INTELLIGENT CYBER INSIGHT

USE CASE

SUCCESSFULLY UTILIZING USER BEHAVIOR ANALYTICS TO MITIGATE THE INSIDER THREAT

INSIDER THREAT SCENARIO



USER BEHAVIOR ANALYTICS TO MITIGATE THE INSIDER THREAT

The FBI and the U.S. Department of Homeland Security (DHS) recently warned of an increase in insider threats from disgruntled current and former employees. This type of threat is a classic example of every CISO's worst nightmare – a completely legitimate and authorized insider who leverages his user privileges to steal sensitive data.

What Edward Snowden did is the most famous example demonstrating the importance of protecting the enterprise from insider threats. Edward Snowden, a systems admin contractor working for the NSA in Hawaii, was able to access, download and leak thousands of secret agency documents.

According to reports, not only did Snowden use his own privileges to access internal systems and databases, he also was able to persuade a number of his colleagues at the NSA to give him their credentials. This social engineering ploy widened his access to critical systems and allowed him to reduce the risk of getting caught. Snowden is a textbook case illustrating why enterprises need to analyze user behavior and the use of access privileges.

WHAT IS AN INSIDER THREAT?

A MALICIOUS INSIDER THREAT TO AN ORGANIZATION IS A CURRENT OR FORMER EMPLOYEE, CONTRACTOR, OR OTHER BUSINESS PARTNER WHO HAS OR HAD AUTHORIZED ACCESS TO AN ORGANIZATION'S NETWORK, SYSTEM, OR DATA AND INTENTIONALLY EXCEEDED OR MISUSED THAT ACCESS IN A MANNER THAT NEGATIVELY AFFECTED THE CONFIDENTIALITY, INTEGRITY, OR AVAILABILITY OF THE ORGANIZATION'S INFORMATION OR INFORMATION SYSTEMS.

(CERT, 2013)

Yet he is only an example. The infamous Target breach, as well, started with the hijacking of user credentials from an HVAC systems contractor by external attackers. Tracking user behavior can be critical for mitigating insider threats and outsider threats - in both type of scenarios the user identity is the primary vehicle of the attack.

THE THREAT DETECTION CHALLENGE

Data breach statistics clearly indicate how compromised user credentials are at core of this growing problem. These studies underscore the need for a new security paradigm for discovery, detection and mitigation of the user threat, based on the ability to identify compromised or rogue users. According to Verizon's 2013 data breach investigation report, 76% of network intrusions exploit weak or stolen user credentials.

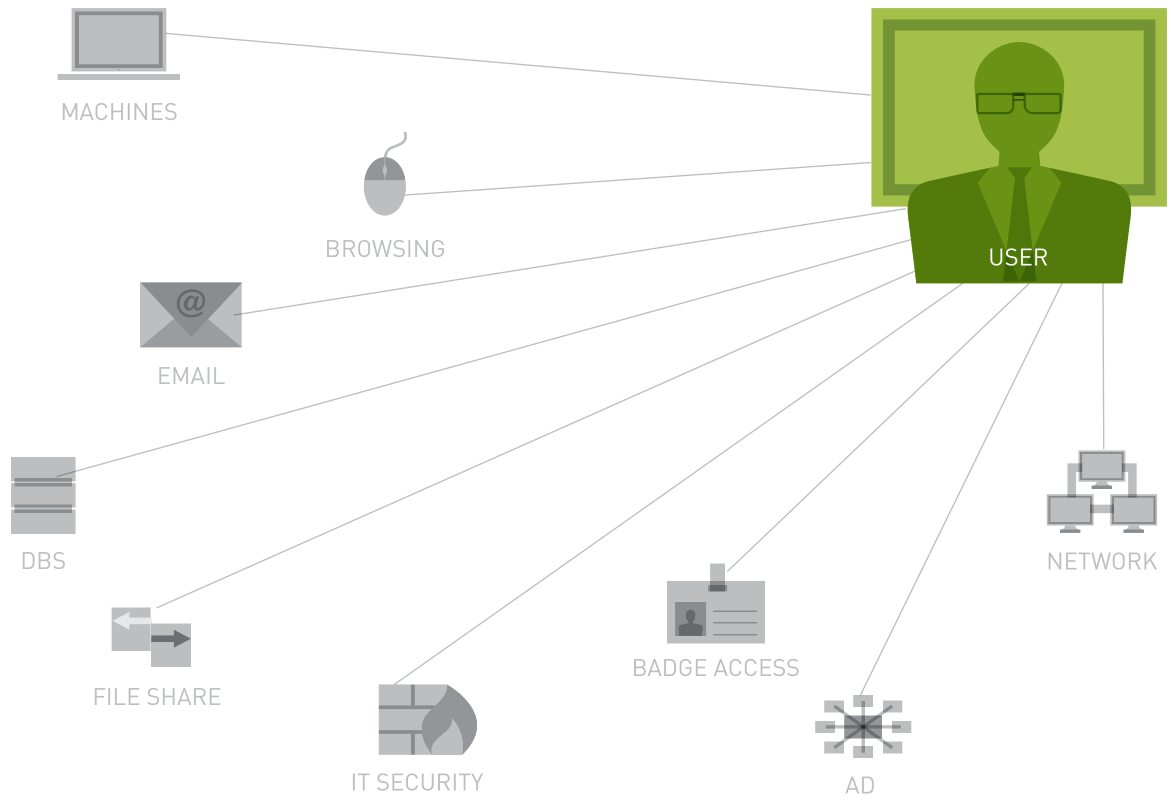
Whether the attacker is a malicious insider or an adversary that has hijacked a legitimate user's identity, the challenge is the same – discovering suspicious activities performed by a user already within your network and with legitimate credentials. The best way to address these dangerous scenarios is through User Behavior Analytics solutions. Organizations require advanced tools to transform their massive amounts of event and log data into effective and actionable user threat detection intelligence. User behavior analytics can be used to analyze current and historical data collected from hundreds of sources and data silos in order to create a profile of a user's characteristics, activity and behavior, and to use this profile as a basis for discovering abnormal behavior that could indicate a possible security breach.

For example, a project manager that has been employed for six months has started downloading various files to his computer in an abnormal pattern. This authorized user downloads multiple files with different sizes and spreads the downloads over a large time frame. He then uploads the small files to his private email account, while downloading the larger files from home via his VPN connection to the office. His actions are slightly different from his peers and from most of the company. Looking at the user's profile would reveal unusual behavior that is distinctive to a user that is harvesting large portions of data. The proxy logs analysis would show the suspicious files that the user has been extracting, and the user's directory permissions analysis would reveal the suspicious permissions used for his actions. Moreover, the VPN analysis would show long connections to the office at unusual hours. Comparing this user with his peers would expose the malicious actions, and aggregating the analytics would generate a high risk score for this user that would lead to further investigation.

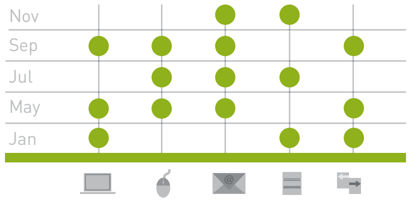
> INSIDERS WERE THE TOP SOURCE OF BREACHES IN THE LAST YEAR, WITH 36% OF BREACHES ATTRIBUTED TO THE INADVERTENT MISUSE OF DATA BY EMPLOYEES.
> Source: Forrester Research (Oct 2013)

GENERATE USER PROFILE

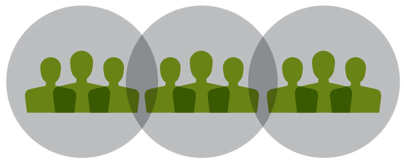
User Related Logs



User History



Peer Analysis



76% OF NETWORK INTRUSIONS EXPLOIT WEAK OR STOLEN USER CREDENTIALS

(Source: Verizon 2013 Data Breach Investigation Report)

The need for advanced user behavior analytics represents a major security challenge for today's enterprises. Their current security systems are not equipped to handle sophisticated insider attacks, while existing Big Data log repository platforms do not yet have the user behavior analytics tools required to generate effective and reliable user threat detection insights.

EVOLVING THREAT DETECTION TO INCLUDE USER BEHAVIOR ANALYTICS

Enterprises and large organizations employ a variety of perimeter and network security tools designed to protect their environments from external threats. Many use log repository platforms and SIEM systems to collect and analyze security events. However, these systems were not distinctly designed to detect new types of user based threats, such as APTs and malicious insider attacks.

Traditional Security Systems

Traditional rule-based systems, such as IDS/IPS, malware detection and network access control, are not equipped to discover today's advanced user based threats, since they typically detect signature-based malware or attack scenarios. These mature products are good at stopping direct attacks using vulnerabilities and exploits, but they are not built to address the sophisticated measures used by today's attackers to circumvent traditional security tools and systems. Another drawback of rule-based systems is the use of pre-defined thresholds. Consider, for example, a rule that triggers an alert each time a file over 2MB is downloaded. That means that any sensitive data contained in a file smaller than 2MB could be exfiltrated by an attacker without raising an alarm. On the other hand, such a threshold-based rule would inevitably result in a large number of "false alarms" and non-productive work for already overburdened security analysts.

> INSIDER THREATS ARE THE MOST COSTLY AND DAMAGING SECURITY THREAT TO THE ENTERPRISE, WITH AVERAGE COST OF $412K PER INCIDENT AND AVERAGE VICTIM LOSS: ~$15M PER YEAR.
>
> Source: FBI / CSI Reports 2013

COMMON BIG DATA SYSTEMS USED FOR ENTERPRISE SECURITY ARE:

SIEM Systems

These centralized systems usually support real time correlation of events. However, because SIEM systems are rule based, they cannot discover unknown scenarios. A further limitation is that they only operate in real-time, and cannot run sophisticated user behavior analytics on historical data. For example, an employee has entered the wrong password. While there is no reason to highlight this event in real-time, it could become significant if this behavior is part of a pattern. If this particular user never made a mistake entering his password when attempting to access his computer from the VPN, this could be a red flag. These patterns cannot be planned for or programmed in advance - only historical data and cross-silo analysis can reveal them.

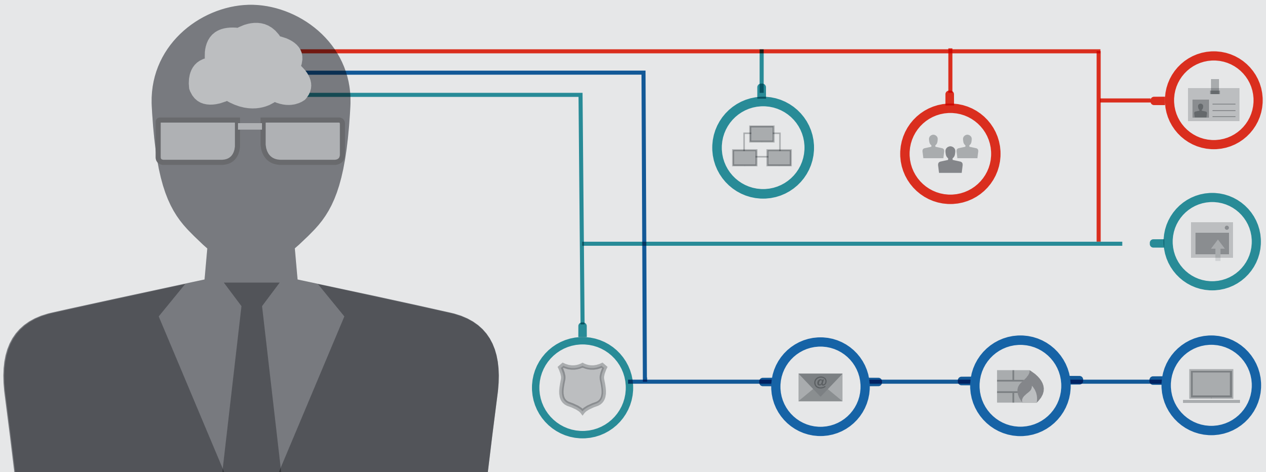
Big Data Analytics Platforms

Hadoop environments enable the enterprise's security team to run cutting-edge analytics on large datasets – but the challenge is that the average security analyst has limited visibility into user based threats and user behavior analytics expertise. Knowing what to ask and writing the specific query and algorithm (i.e., how to ask) typically requires expert knowledge in data mining and/or machine learning algorithms and/or cyber warfare, which is hard to find in enterprise IT environments. In addition, even if the enterprise security team has these abilities, thinking of and developing the relevant queries is a very time consuming task. Another point to keep in mind is that simplification of complex user behavior using off-the-shelf algorithms is one of the main reasons for false positives and inaccuracies in security analytics.

FORTSCALE - TURNING LOG DATA INTO USER INTELLIGENCE FOR THE SECURITY ANALYST

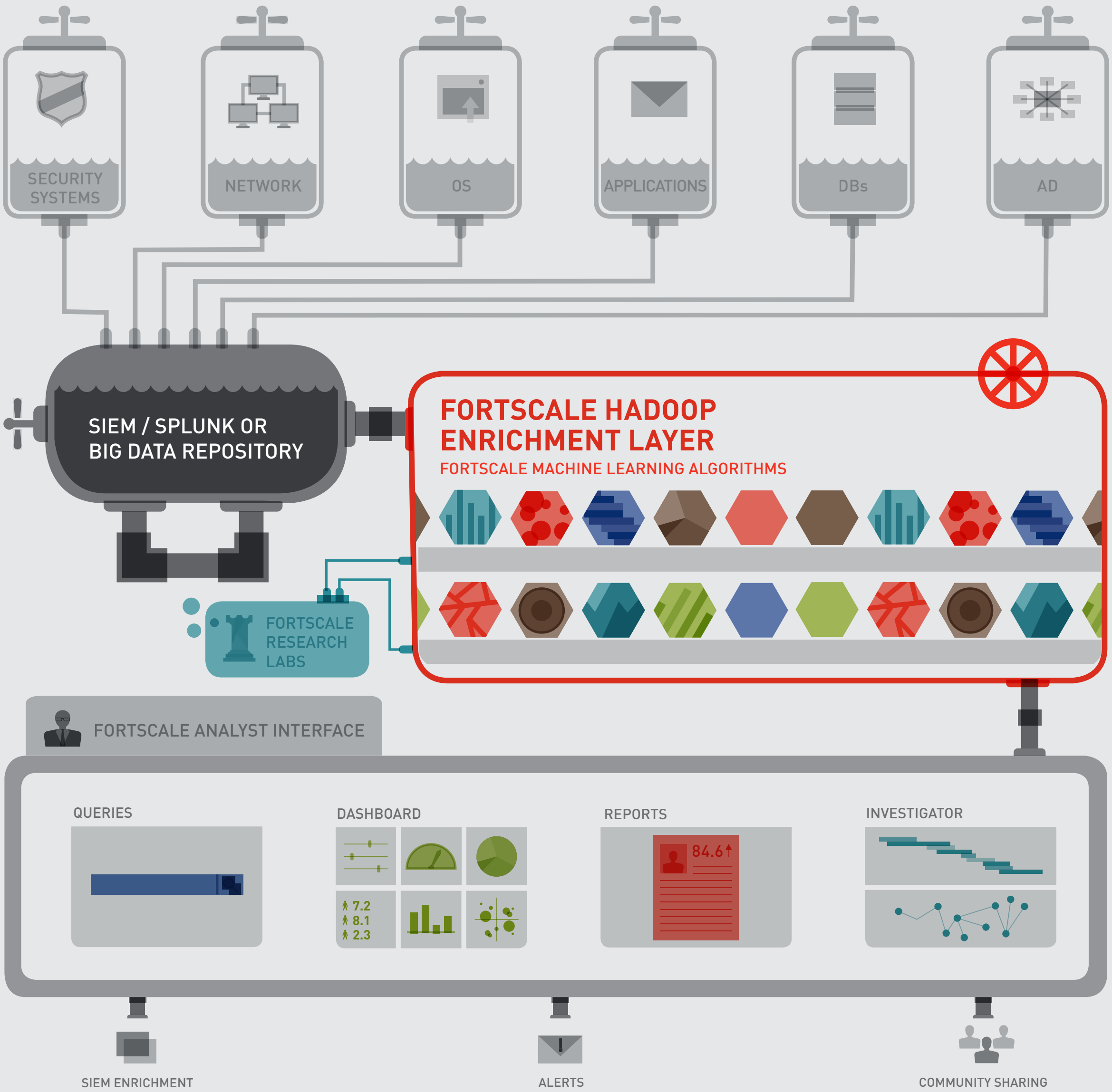
Fortscale's enriched big data based user behavior analytics provide user intelligence that helps enterprise security teams discover insider attacks, users whose identities were compromised by advanced adversaries and suspicious user access to data. These advanced analytics combine dynamic machine learning algorithms, intuitive analyst investigation tools and a scalable Hadoop environment. They are layered on top of the existing capabilities of Big Data platforms to provide timely user intelligence that can be used by security analysts to discover, investigate and remediate security threats.

SOPHISTICATED MACHINE LEARNING ALGORITHMS HELP CORRELATE NETWORK ANOMALIES AND EMERGING THREATS.



FORTSCALE COMPRISES TWO INTEGRATED LAYERS:

- **ROBUST HADOOP CLUSTER**
  featuring machine learning algorithms that extract log repositories (SIEM, Splunk or others) for user profiling and risk identification
- **INTUITIVE INVESTIGATION TOOLBOX**
  for enterprise security analysts and investigators



HADOOP ENRICHMENT LAYER WITH FORTSCALE USER BEHAVIOR ANALYTICS

Using patent-pending machine learning algorithms, Fortscale profiles user behavior across multiple dimensions (e.g., identity, network, application, file access, etc.) and identifies new patterns, anomalies or suspicious behavior of users, without pre-defined security rules, heuristics or thresholds. This is critical for discovering "Snowden-like" insiders and other unknown attack scenarios. By understanding the various dimensions of multi-faceted and targeted attacks, our solution is able to discover abnormal user activity against historical data or peer activity. These insights enrich the current security efforts of SOC teams and threat detection programs.

The strength of the Fortscale integrated Hadoop layer is in its inherent scalability and flexibility. It manages massive amounts of information from various logs, and runs generic, canned or ad-hoc algorithms and queries. Fortscale's machine learning algorithms analyze the behavior of users and entities across multiple log sources (e.g., Active Directory, SSH, Logins, DNS, VPN, proxy, applications, file access, etc.), including comparison against historical data, and produce a risk score indicating the potential risk of a given entity. Fine-tuned to the relevant security context, these algorithms understand what is important or risky even if the security team is not sure what to look for.

ANALYST INTERFACE LAYER

This layer includes visibility and investigation tools specifically designed to help security analysts and data scientists make dynamic queries and gain contextual insights from multiple data sources. These insights facilitate the discovery of compromised users, malicious insiders, suspicious access to sensitive data or risky misconfiguration. The Analyst Interface layer also includes reports and visual investigation tools that provide investigators with fast results, while allowing them to leverage their own expertise and the enterprise's current security measures.
The Analyst Layer allows analysts to display and drill down into a wide variety of outputs from the Fortscale user based risk scores. These include a list of the top 10 suspicious users based on risk score, clustering of risky users, and user activity reports. In addition to sending alerts to investigators for further examination and remediation, Fortscale also sends alerts upstream to SIEM systems for better prioritization of event monitoring that could lead to identification of potentially malicious insiders. It also supports a community environment for sharing analytics and know-how among like-minded cyber security teams.

Powerful visualization tools facilitate the analysis of potential user based threats by visualizing these threats for security analysts in a clear and informative way, which can be further refined using the analyst's input.

SEE HOW FORTSCALE CAN HELP YOU MITIGATE INSIDER THREATS

Fortscale's User Behavior Analytics solution makes it much easier for organizations like yours to mitigate hard-to-discover insider threats. By providing better visibility into user behavior, Fortscale enables your security analysts to:

- Analyze log data for user based threats
- Profile normal and abnormal user behavior and create resulting risk scores
- Discover suspicious and/or malicious user behavior
- Investigate suspicious and/or malicious user activity.

To see Fortscale in action, contact us at sales@fortscale.com to schedule a demo.

ABOUT FORTSCALE

- Fortscale was founded by seasoned security entrepreneurs from Israel's high-tech sector, many of whom served in the IDF's elite intelligence and cyber unit.
- Our team includes a unique fusion of specialists in Big Data Analytics, Machine Learning algorithms, Cyber warfare and security investigations.
- Fortscale User Behavior Analytics solution is being used daily to investigate anomalous user behavior at multiple Fortune 1000 enterprises.
- The company is backed by top-tier investors, among them Intel Capital, Blumberg Capital and the Swarth Group, and a strong advisory board comprising world-renowned CISOs and experts in machine learning algorithms and cyber security.
- Fortscale's headquarters are located in San Francisco, CA, while its R&D is located in Tel Aviv, Israel.

FORTSCALE SECURITY LTD.
WWW.FORTSCALE.COM | CONTACT US: INFO@FORTSCALE.COM

US. 425 MARKET STREET, SUITE 2200,
SAN FRANCISCO, CA 94105
TEL: +1 (415) 955-0530

ISRAEL. 22A RAOUL WALLENBERG ST.
TEL AVIV 69719
TEL: +972 (3) 600-6078

FORTSCALE

INTELLIGENT CYBER INSIGHT

To learn more, please visit:

WWW.FORTSCALE.COM