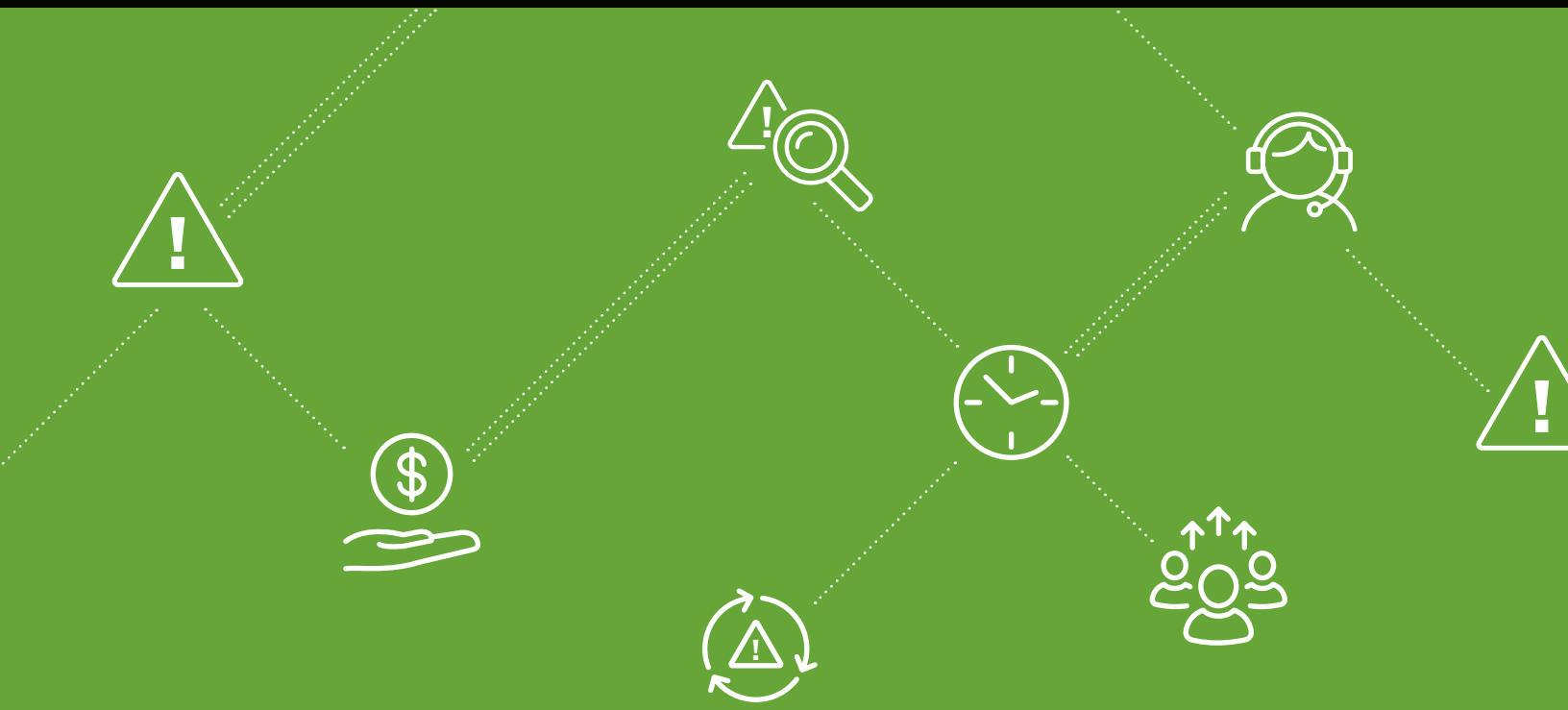
splunk>

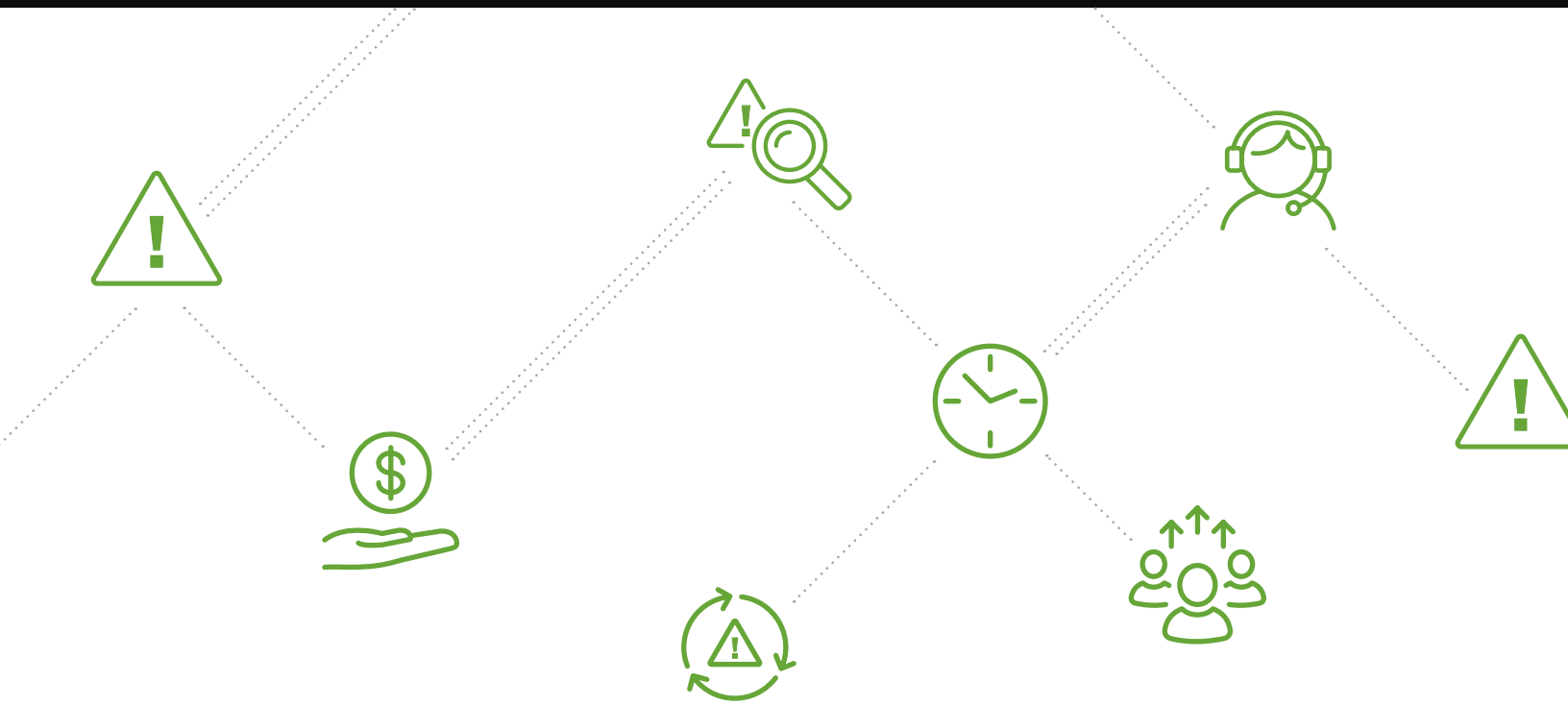
BUYER'S GUIDE



THE SIEM BUYER'S GUIDE

The who, what, where, when and why of buying an analytics-driven security solution

TABLE OF CONTENTS



1. WHAT IS A SIEM

A security information event management (SIEM) solution is like a radar system that pilots and air traffic controllers use. Without one, enterprise IT is flying blind. Although security appliances and system software are good at catching and logging isolated attacks and anomalous behavior, today's most serious threats are distributed, acting in concert across multiple systems and using advanced evasion techniques to avoid detection. Without a SIEM, attacks are allowed to germinate and grow into catastrophic incidents.

The importance of a SIEM solution to today's enterprise is magnified by the growing sophistication of attacks and the use of cloud services which only increase the surface of vulnerability.

In this buyer's guide, we aim to explain what a SIEM solution is, what it isn't, its evolution, what it does and how to determine if it is the right security solution for your organization.

So what is a SIEM?

Gartner defines SIEM "as a technology that supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources."

What does that all mean in simple English?

In short, a SIEM is a security platform that ingests event logs and offers a single view of this data with additional insights.

The evolution of a SIEM

SIEM is not a new technology. The fundamental capabilities of the platform have been around in some form for almost 15 years.

Over time, SIEM solutions became more of an information platform – its use expanded to include compliance reporting, aggregating logs from firewalls and other devices. But SIEM technology was often complex and hard to tune, and to identify attacks, IT pros had to know what they were looking for. However, the technology had become difficult and not scalable.

This drove SIEM solutions to evolve to be more flexible and easier to use. This is especially important today as organizations have embraced cloud solutions and digital transformation touches every aspect of our lives.

So, this is why it's important to understand the difference between a legacy SIEM and a modern analytics-driven SIEM solution, which we will get into later.

But it is also important to understand the use cases associated with a SIEM and whether your organization actually needs a SIEM solution or something else.

This leads to a need to make the distinction clear between legacy SIEMs compared to modern analytics-driven SIEM solutions.

Legacy SIEMs are stuck in the past

Finding a mechanism to collect, store and analyze security-only data is relatively simple. There is no shortage of options for storing data. Collecting all security-relevant data and turning all that data into actionable intelligence, however, is a whole other matter.

Many enterprise IT organizations that invested in SIEM platforms have discovered this fundamental truth the hard way. After spending a significant amount of time and money recording security events, the trouble is that not only did it take a long time to ingest all that data, but the underlying data system used to create the SIEM tends to be static.

Worse yet, the data available to analyze is based only on security events. That makes it difficult to correlate security events against what's occurring across the rest of an IT environment. When there's an issue, investigating a security event takes precious time most IT organizations can't afford. In addition, a legacy SIEM solution can't keep pace with the rate at which security events need to be investigated. The continued adoption of cloud services expands the threat vectors and enterprises need to monitor user activity, behavior, application access across key cloud and software-as-a-service (SaaS), as well as on-premise services, to determine the full scope of potential threats and attacks.

The following graphic explains some of the key limitations of a legacy SIEM solution.

Legacy SIEM – Problems and Characteristics

PROBLEM	ISSUE
Cannot use required data	Limits detection, investigation and response
Difficult to maintain and operate	Complexity and skilled staff
High false negative and positives	Burden on SecOps
Unstable	History of outages
Inflexible data	Cannot adapt to critical cases
Static workflows	Limited and restrictive
Cannot detect modern threats	Business risk

The alternative: an analytics-driven SIEM

What enterprise IT requires today is a simple way to correlate information across all security-relevant data. A solution that enables IT to manage their security posture. Instead of merely watching events after they occur, an IT organization should be able to anticipate their occurrence and implement measures to limit their vulnerability in real time. For that, enterprises need an analytics-driven SIEM platform.

Here lies the difference between a legacy SIEM and a modern solution. Gartner says the distinction is that a **"modern SIEM works with more than just log data and applies more than just simple correlation rules for data analysis."**

This is where a specific type of modern SIEM—one we like to call an analytics-driven SIEM solution—comes in. This modern solution allows IT to monitor threats in real time and respond quickly to incidents, so that damage can be avoided or limited. But not all attacks are external—IT needs a way to monitor user activity, so that it can minimize the risks from insider threats or accidental compromise. Threat intelligence is critical to understand the nature of the broader threat environment and put those threats into context for the organization.

An analytics-driven SIEM must excel at security analytics, giving IT teams the power to use sophisticated quantitative methods to gain insight into and prioritize efforts. Finally, a SIEM today must include the specialized tools needed to combat advanced threats as part of the core platform.

Another major difference between an analytics-driven SIEM and a legacy SIEM is the flexible nature of a modern solution, which allows the solution to be deployed on premises, in the cloud or in a hybrid environment.

The following graphic explains the top seven reasons an organization should choose an analytics-driven SIEM solution over a legacy SIEM.

Top 7 Reasons to Replace Your Legacy SIEM

Organizations are often tied to the dated architectures of traditional SIEMs, which typically use a SQL database with a fixed schema. These databases can become a single point of failure or suffer from scale and performance limitations.

1. **LIMITED SECURITY TYPES**	By limiting the type of data that is ingested, there are limits in detection, investigation and reponse times.
2. **INABILITY TO EFFECTIVELY INGEST DATA**	With legacy SIEMs, the ingestion of data can be a massively laborious process or very expensive.
3. **SLOW INVESTIGATIONS**	With legacy SIEMs, basic actions, such as raw log searches, can take a significant amount of time – often many hours and days to complete.
4. **INSTABILITY AND SCALABILITY**	The larger SQL-based databases get, the less stable they become. Customers often suffer from either poor performance or a large number of outages as spikes in events take servers down.
5. **END-OF-LIFE OR UNCERTAIN ROADMAP**	As legacy SIEM vendors change ownership, R&D slows to a crawl. Without continuous investment and innovation, security solutions fail to keep up with the growing threat landscape.
6. **CLOSED ECOSYSTEM**	Legacy SIEM vendors often lack the ability to integrate with other tools in the market. Customers are forced to use what was included in the SIEM or spend more on custom development and professsional services.
7. **LIMITED TO ON PREMISES**	Legacy SIEMs are often limited to an on-premises deployments. Security practioners must be able to use cloud, on premises and hybrid workloads.

Taking your SIEM to the cloud

Running SIEM in the cloud, or as SaaS, can help solve the problems many organizations have with security intelligence, yet many IT leaders still distrust cloud security and reliability. Before eliminating a cloud-based SIEM solution, know that the security practices and technology at most large cloud services can be far more sophisticated than those in the typical enterprise.

SaaS is already widely used for business-critical systems like CRM, HR, ERP and business analytics. The same reasons that SaaS makes sense for enterprise applications—fast, convenient deployment, low-overhead operations, automatic updates, usage-based billing and scalable, hardened infrastructure—make the cloud a great fit for SIEM.

Cloud-based solutions provide the flexibility to use a wide range of data sets from on-premises and cloud. As more enterprise workloads move to infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS) and SaaS, the ease of integrating with third-party systems shows that SIEM in the cloud makes even more sense. Key benefits of taking your SIEM to the cloud include the flexibility of a hybrid architecture, automatic software updates and simplified configuration, instant, scalable infrastructure, and strong controls and high availability.

The SIEM use cases for enterprises

Now that you understand the evolution of a SIEM and the characteristics that differentiate a modern, analytics-driven SIEM solution from a legacy SIEM, it's time that we explain what security use cases are actually solved by the technology.

Early detection, rapid response and collaboration to mitigate advanced threats impose significant demands on today's enterprise security teams. Reporting and monitoring logs and security events is no longer enough. Security practitioners need broader insights from all data sources generated at scale across the entire organization from IT, the business and the cloud. In order to stay ahead of external attacks and malicious insiders, companies need an advanced security solution that can be used for rapid response detection, incident investigation and coordination of CSIRT breach scenarios. In addition, companies need the ability to detect and respond to known, unknown and advanced threats.

Enterprise security teams must use a SIEM solution that not only solves common security use cases, but advanced use cases as well. To keep up with the dynamic threat landscape, modern SIEMs are expected to be able to:

- Centralize and aggregate all security-relevant events as they're generated from their source
- Support a variety of reception, collection mechanisms including syslog, file transmissions, file collections, etc.
- Add context and threat intelligence to security events
- Correlate and alert across a range of data
- Detect advanced and unknown threats
- Profile behavior across the organization
- Ingest all data (users, applications) and make them available for use—monitoring, alerting, investigation, ad hoc searching
- Provide ad hoc searching and reporting from data for advanced breach analysis
- Investigate incidents and conduct forensic investigations for detailed incident analysis
- Assess and report on compliance posture
- Use analytics and report on security posture
- Track attackers' actions with streamlined ad hoc analysis and event sequencing

Although primarily gathered from servers and network device logs, SIEM data also can come from endpoint security, network security devices, applications, cloud services, authentication and authorization systems and online databases of existing vulnerabilities and threats.

But data aggregation is only half of the story. SIEM software then correlates the resulting repository and looks for unusual behavior, system anomalies and other indicators of a security incident. This information is used not only for real-time event notification, but also for compliance audits and reporting, performance dashboards, historical trend analysis and post-hoc incident forensics.

Given the escalating number and sophistication of security threats, along with the increasing value of digital assets in every organization, it's not surprising that the adoption of analytics-driven SIEM solutions continue to grow as part of the overall IT security ecosystem.

Do you really need a SIEM?

Now that you understand what a SIEM is used for, it's time for a broader conversation. Does your organization need a SIEM—or something else?

Your organization may not be ready for advanced security use cases and, instead, simply need a solution—such as a central log management (CLM)—that gives insights into machine data. Shameless plug: See **Splunk Enterprise for security and log management**.

So, what is a central log management solution? CLM is simply defined as a solution that gives a centralized view into log data.

For further context, let's ask the next question for you: What is log data?

Log data is computer-generated log messages that are a definitive record of what's happening in every business, organization or agency and it's often an untapped resource when it comes to troubleshooting and supporting broader business objectives.

Back to CLM. The aim of log management is to collect these computer-generated logs and make them accessible for searching and reporting. In security speak, that means a CLM can help with things such as incident investigation and alert triage.

Log management has been a central function of SIEM capabilities since the dawn of SIEMs. But if all you need is insights from your log data, is an analytics-driven SIEM solution the right tool for you? Let's turn to **famed SIEM analyst Anton Chuvakin** for an answer:

In short, that translates to if you are using a SIEM solution for log aggregation, you are paying too much. The key point here is that you can use a SIEM to solve both basic and advanced use cases.

On the other end of the maturity line, there is the **Gartner coined term** user and entity behavior analytics (UEBA). There are other names for this same category, such as **Forrester's preferred** security user behavior analytics and the **Splunk preferred user behavior analytics (UBA)**—the latter being the term that we will stick with for this report. They are all essentially different ways of referring to the same technology.

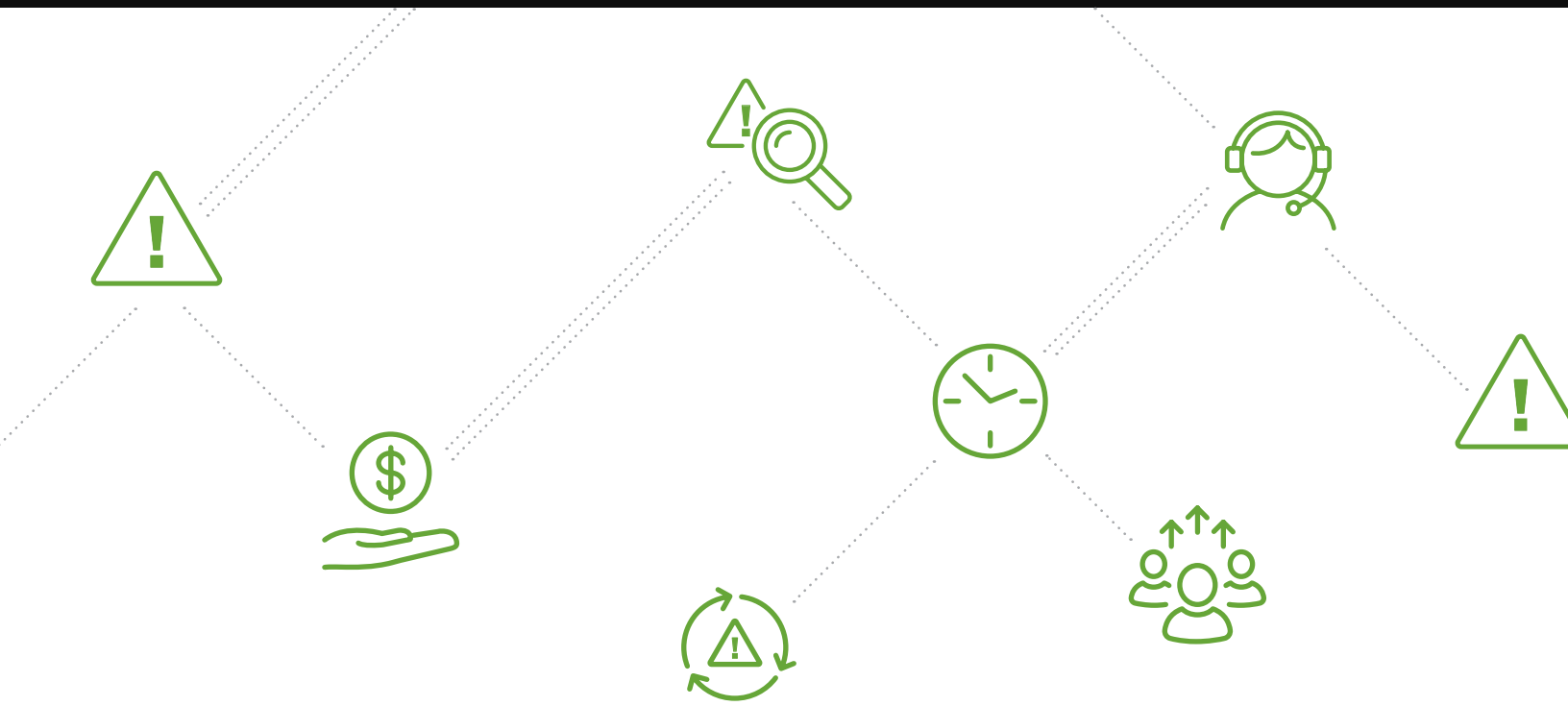
UBA is used for threat detection to discover and remediate internal and external threats. UBA is often seen as a more advanced security use case, in part, because it has the ability to learn and baseline a user's normal habits and then send an alert when something outside of the norm happens, as one example.

Sticking to this one example, to establish a baseline, a UBA solution would track the habits of such activities as:

- Where do users normally log in from
- What permissions do users have
- What files, servers and applications are users accessing
- What devices do users normally log in from

For context, some UBA vendors are trying to compete in the SIEM marketplace. These are the new entrants when it comes to SIEM. UBA is a useful solution but a UBA solution alone cannot replace a SIEM solution. And UBA is not a new category of SIEM. It is a security technology all on its own. And, ideally, a UBA solution should be able to work in concert with an analytics-driven SIEM solution.

More plainly: just like a CLM solution is not a SIEM, a UBA solution is also not a SIEM. Now, if only Dr. Chuvakin had sent **a tweet about that**.



2. THE SIEM ESSENTIALS

Now, we get into the meat of what makes up an analytics-driven SIEM solution. There are six essential capabilities of an analytics-driven SIEM:

REAL-TIME MONITORING	Threats can move quickly, and IT needs the ability to monitor threats and correlate events in real time to find and stop threats.
INCIDENT RESPONSE	IT needs an organized way to address and manage potential breach as well as the aftermath of a security breach or attack in order to limit damage and reduce recovery time and cost.
USER MONITORING	Monitoring user activity with context is critical to pinpoint breaches and uncover misuse. Privileged user monitoring is a common requirement for compliance reporting.
THREAT INTELLIGENCE	Threat intelligence can help IT recognize abnormal activity, assess the risk to the business, and prioritize the response.
ADVANCED ANALYTICS	Analytics are key to producing insights from mountains of data, and machine learning can automate this analysis to identify hidden threats.
ADVANCED THREAT DETECTION	Security professionals need specialized tools to monitor, analyze and detect threats across the kill chain.

These capabilities give organizations the ability to use their SIEM for a wide range of security use case, as well as compliance. They are also a way to define a modern SIEM based on capabilities. Let's take a deeper look at each essential capability that makes up an analytics-driven SIEM.

Real-time monitoring

The longer it takes to discover a threat, the more damage it can potentially inflict. IT organizations need a SIEM that includes monitoring capabilities which can be applied in real time to any data set, regardless of whether it's located on premises or in the cloud. In addition, that monitoring capability needs to be able to retrieve both contextual data feeds, such as asset data and identity data, and threat intelligence feeds, which can be used to produce alerts.

An analytics-driven SIEM needs to able to identify all the entities in the IT environment, including users, devices and applications as well as any activity not specifically attached to an identity. A SIEM should be able to use that data in real time to identify a broad range of different types and classes of anomalous behavior. Once identified, that data needs to then be easily fed into the workflow that has been set up to assess the potential risk to the business which this anomaly might represent.

There should be a library of customizable, predefined correlation rules, a security event console to provide a real-time presentation of security incidents and events, and dashboards to provide real-time visualizations of ongoing threat activity.

Finally, all those capabilities should be augmented with out-of-the-box correlation searches that can be invoked in real time or scheduled to run regularly at a specific time. Just as relevant, these searches should be available via an intuitive user interface that eliminates the need for IT administrators to master a search language.

Finally, an analytics-driven SIEM needs to provide the ability to locally search real-time and historical data locally in a way that serves to reduce the amount of network traffic accessing search data generates.

Autodesk saves time and capex costs with Splunk on AWS

Customers across the manufacturing, architecture, building, construction and media and entertainment industries—including the last 20 Academy Award winners for best visual effects—use Autodesk software to design, visualize and simulate their ideas. Given its large global footprint, Autodesk faced two distinct challenges: the need to gain business, operational and security insights worldwide across multiple internal groups, and the need to choose the right infrastructure to deploy operational intelligence software. Since deploying the Splunk platform, the company has seen benefits including:

- Savings of hundreds of thousands of dollars
- Critical operational and security-related insights
- Real-time visibility into product performance

Why Splunk

Splunk first found a home at Autodesk in 2007 as a way to harness machine data for operational troubleshooting. Today, that usage has expanded to include real-time monitoring, detailed security insights and executive-relevant business analytics across three Autodesk divisions, including:

- Enterprise Information Services (EIS)—responsible for global corporate IT management, including information security and information management.
- Autodesk Consumer Group (ACG)—responsible for all of Autodesk's consumer-facing products.
- Information Modeling & Platform Products (IPG)—responsible for Autodesk's solutions for commercial customers, including designers and engineers across all industries.

Autodesk is using Splunk Enterprise Security (Splunk ES) to reduce the time to identify and resolve security issues. The company also uses the Splunk App for AWS to deliver and manage flexible resources for Splunk Enterprise and other critical applications.

Empower data-driven decisions

Splunk Enterprise, the Splunk App for AWS, Splunk Enterprise Security and other Splunk solutions are enabling Autodesk to gain important, real-time insight into operational, security and product performance. Splunk's flexible, data-driven analytics and AWS-based platform are saving Autodesk time, reducing capital costs, and enhancing the scope and depth of critical decisions. **Read more**.

Incident response

At the core of any effective incident response strategy is a robust SIEM platform that makes it possible not only to identify distinct incidents, but also provide the means to track and re-assign them as well as add annotations.

IT should be able to provide other members of the organization with varying levels of access based on their roles. Other key capabilities include the ability to either manually or automatically aggregates events, support for application programming interfaces (APIs) that can be used to pull data from or push information to third-party systems, an ability to gather legally admissible forensics evidence, and playbooks that provide organizations with guidance on how to respond to specific types of incidents.

Most importantly, an analytics-driven SIEM needs to include auto-response capabilities that can disrupt cyberattacks in progress.

In effect, the SIEM platform needs to be the hub around which a customizable workflow for managing incidents can be crafted. Of course, not every incident has the same level of urgency attached to it. An analytics-driven SIEM platform provides IT organizations with the means to categorize the severity of any potential threat via dashboards that can be used to triage new notable events, assign events to analysts for review, and examine notable event details for investigative leads, an analytics-driven SIEM arms IT organizations with the contextual insight needed to determine the appropriate response to any event.

Those response capabilities should include the ability to identify notable events and their status, indicate the severity of events, start a remediation process, and provide an audit of the entire process surrounding that incident.

Finally, the IT team should have a dashboard where they can intuitively apply filters to any field during an investigation to expand or reduce the scope of analysis with a few clicks of their mouse. The end goal should be nothing less than enabling any security team member to place events, actions and annotations into a timeline that makes it simple for other members of the team to easily comprehend what is occurring. Those timelines can then be included in a journal that makes it simple to review attacks and to implement a repeatable kill chain methodology to deal with specific types events.

PagerDuty ensures end-to-end visibility with Splunk Cloud and Amazon Web Services

Customers turn to PagerDuty, an enterprise incident response service, to manage and resolve their IT incidents quickly and efficiently. When the cloud-native company needed a solution to meet its operational analysis and triage needs, it adopted Splunk Cloud running on Amazon Web Services (AWS). With Splunk Cloud and AWS, PagerDuty ensures high availability of its services and can scale to meet customer demand. Since deploying Splunk Cloud, PagerDuty has seen benefits including:

- Ensured customer satisfaction and highly available cloud services
- A 30 percent gain in cost savings over prior service
- Reduced IT and security incident resolution time—from tens of minutes to single-digit minutes or seconds

Why Splunk

Arup Chakrabarti is director of infrastructure engineering at PagerDuty, covering site reliability, internal platform and security engineering. His organization's charter is to promote productivity and efficiency across the company's entire engineering organization, consisting of multiple engineering teams within the company's product development organization.

Prior to adopting Splunk Cloud, PagerDuty relied on a logging solution that could not scale as the company began indexing hundreds of gigabytes of logs daily. What's more, the team found it difficult to get actionable information out of its data to make decisions and solve problems quickly. After running its previous service and Splunk Cloud side by side, the team determined that Splunk Cloud provided the speed required to resolve issues quickly and ensure high availability to its customers. Within days, the engineers migrated to Splunk Cloud.

"With the previous solution, some queries took up to 30 minutes to crunch the data and give us the information we needed, and that was simply unacceptable," Chakrabarti says. "From a customer impact standpoint, we ended up shortening that time to resolution from tens of minutes to single-digit minutes or seconds with Splunk Cloud."

Chakrabarti notes that while cost was not the primary driver in selecting Splunk Cloud, **"My accounting team was absolutely ecstatic when I told them, 'We're going to get the best solution, and by the way, it's 30 percent cheaper compared to what we are currently using.'" Read more.**

User monitoring

At a bare minimum, user activity monitoring needs to include the ability to analyze access and authentication data, establish user context and provide alerts relating to suspicious behavior and violations of corporate and regulatory policies.

It's critically important that user monitoring be extended to privileged users who are most often the targets of attacks, and when compromised, wind up doing the most damage. In fact, because of this risk, privileged user monitoring is a common requirement for compliance reporting in most regulated industries.

Achieving those goals requires real-time views and reporting capabilities capable of leveraging a variety of identity mechanisms that can be extended to include any number of third-party applications and services.

Travis Perkins PLC adopts analytics-driven SIEM to enable hybrid cloud transition

Travis Perkins PLC is a British builders' merchant and home improvement retailer with 2,000 outlets and 28,000 employees. In 2014, the organization embarked on a "cloud-first" journey; however, its existing security information and event management solution couldn't provide the necessary security insights across a hybrid environment. Travis Perkins PLC reviewed the alternatives available and selected Splunk Cloud, Splunk Enterprise and Splunk Enterprise Security (ES) as its SIEM. Since deploying the Splunk platform, Travis Perkins PLC has seen benefits including:

- Improved visibility over hybrid infrastructure
- Gained ability to detect and respond to complex cyber threats
- Reduced IT costs due to more efficient resourcing

Why Splunk

Faced with challenging market conditions during the recession, Travis Perkins PLC de-prioritized investment in technology. Recently, with business conditions improving, the company went through a strategic review of all technology infrastructure and adopted a cloud-first approach to reduce costs and increase flexibility. As Travis Perkins PLC rolled out a number of cloud services including G Suite from Google Cloud, Amazon Web Services and Infor CloudSuite, it quickly became apparent that its existing SIEM wasn't capable of providing the required insights into security events across a complex hybrid environment. Having reviewed alternatives including offerings from HP, IBM and LogRhythm, Travis Perkins PLC selected Splunk Cloud, Splunk Enterprise and Splunk ES to provide a single view of security-relevant activity.

Building security from the ground up

Travis Perkins PLC used the opportunity presented by the Splunk ES implementation to improve the security awareness of all individuals in IT, rather than focusing just on the security team. Employees in the IT operations teams now have access to specific dashboards and alerts so they can act as first responders to potential threats, instigating immediate action before escalating to the dedicated security team where necessary. As a result, Travis Perkins PLC has developed a highly effective and lean security operations center (SOC), without needing to invest the considerable resources this might usually require.

Automating threat defense

With 24,000 employees based across the U.K. using a variety of devices to access corporate data, it has become crucial for Travis Perkins PLC to automate a large part of its cybersecurity. With Splunk ES, Travis Perkins PLC now calculates risk scores on different threat activities based on previously correlated data or alerts from the company's existing security solutions. With the business facing a particular problem with phishing emails, if an infected client is identified through correlation searches in the Splunk platform, it produces an automated alert. The relevant teams then react using a preset playbook response. The swimlanes in Splunk ES provide a holistic view into an asset or user and dramatically reduce the time it takes for security incidents to be investigated and resolved. **Read more**.

Threat intelligence

An analytics-driven SIEM must provide two distinct forms of threat intelligence. The first involves leveraging threat intelligence services that provide current information on indicators of compromise, adversary tactics, techniques and procedures, alongside additional context for various types of incidents and activities. This intelligence makes it easier to recognize such abnormal activity as, for example, identifying outbound connections to an external IP address known to be an active command-and-control server. With this level of threat intelligence, analysts have the information needed to assess the risks, impact and objectives of an attack—which are critical to prioritizing an appropriate response.

The second form on intelligence involves assessing asset criticality, usage, connectivity, ownership, and, finally, the user's role, responsibility and employment status. That additional context is often critical when it comes to evaluating and analyzing the risk and potential impact of an incident. For example, an analytics-driven SIEM should be able to ingest employee badging information and then correlate that data with VPN authentication logs to provide context on an employee's location on the corporate network. To provide even deeper levels of analysis and Operational Intelligence, a SIEM also should be able leverage REST APIs to retrieve via workflow action or script to bring it into a system as well as combine structured data from relational databases with machine data.

Threat intelligence data ideally should be integrated with machine data generated by various types of IT infrastructure and applications to create watch lists, correlation rules and queries in ways that increase the success rate of early breach detection. That information should be automatically correlated with event data and added to dashboard views and reports or forwarded to devices such as firewalls or intrusion prevention systems that can then remediate the vulnerability in question.

The dashboard provided by the SIEM should be able track the status and activity of the vulnerability detection products deployed in the IT environment, including providing health checks of scanning systems and the ability to identify systems that are no longer being scanned for vulnerabilities.

In short, a comprehensive threat intelligence overlay needs to provide support for any threat list, automatically identify redundant intelligence, identify and prioritize threats that have been listed in multiple threat lists, and assign weights to various threats to identify the real risk they represent to the business.

City of Los Angeles integrates real-time security intelligence sharing across 40+ city agencies

To protect its digital infrastructure, the City of Los Angeles requires situational awareness of its security posture and threat intelligence for its departments and stakeholders. In the past, the city's more than 40 agencies had disparate security measures, complicating the consolidation and analysis of data. Los Angeles sought a scalable SaaS security information and event management solution to identify, prioritize and mitigate threats, gain visibility into suspicious activities and assess citywide risks. Since deploying Splunk Cloud and Splunk Enterprise Security, the city has seen benefits including:

- Creation of citywide security operations center (SOC)
- Real-time threat intelligence
- Reduced operational costs

Real-time situational awareness

Splunk Cloud provides Los Angeles with holistic views of its security posture. Splunk forwarders send raw logs and other data from the city's departments to Splunk Cloud, where they are normalized and returned to the integrated SOC, and then analyzed and visualized in Splunk dashboards.

Using pre-built, easily customizable dashboards in Splunk ES, executives and analysts have always-available, real-time situational awareness of security events across the city's networking infrastructure. With all security data in one continuously updated database, Lee's team views and compares any machine-generated data, including disparate logs and both structured and unstructured data, to extract all-inclusive, actionable security intelligence.

Timely threat intelligence

The city's integrated SOC does more than collect information; it also provides information. It translates data from Splunk Cloud into timely threat intelligence. The city shares its findings with its agencies as well as external stakeholders like the FBI, the Department of Homeland Security, the Secret Service and other law enforcement agencies. With this information, the city collaborates with federal agencies to identify risks and develop strategies for deterring future network intrusions.

"With situational awareness, we know ourselves," says Lee. "But with threat intelligence, we know our enemy. We're now operating an integrated threat intelligence program and our Splunk SIEM is one of the key solutions for a centralized information management platform that we deploy at our Integrated Security Operations Center (ISOC)."
Read more.

Advanced analytics

An analytics-driven SIEM can apply advanced analytics by employing sophisticated quantitative methods, such as statistics, descriptive and predictive data mining, machine learning, simulation and optimization, to produce additional critical insights. Key advanced analytics methods include anomaly detection, peer group profiling and entity relationship modeling.

Just as significantly, an analytics-driven SIEM needs to provide tools that make it possible to visualize and correlate data by, for example, mapping categorized events against a kill chain or creating heat maps to better support incident investigations.

Making all that possible requires access to a SIEM platform that makes use of machine learning algorithms capable of learning on their own what represent normal behavior versus an actual anomaly.

That level of behavioral analytics can then be used to build, validate and deploy predictive models. It should even be feasible to employ a model created using third-party tools in the SIEM platform.

Innovative cloud-based SIEM deployment delivers actionable security intelligence for Equinix

Equinix, Inc. connects the world's leading businesses to their customers, employees and partners in 33 markets across five continents. Security is of paramount importance at Equinix as thousands of companies worldwide rely on Equinix data centers and interconnection services. To gain a unified view across its security infrastructure, Equinix needed a cloud solution with centralized visibility and SIEM functionality that could be implemented easily, quickly and without significant operational effort. Since deploying Splunk Cloud and Splunk Enterprise Security (ES), Equinix has seen benefits including:

- Full operational visibility
- Enhanced security posture
- Time and cost savings

Overarching visibility into infrastructure with Splunk Cloud and Splunk Enterprise Security

Before Splunk Cloud, Equinix was overwhelmed by more than 30 billion raw security events generated every month. With Splunk ES and Splunk Cloud, the security team can now reduce the 30 billion raw security events down to about 12,000 correlated events, and then to 20 actionable alerts, thus providing actionable security intelligence and the foundation for a dedicated SOC.

With all the data aggregated within the Splunk platform, the security team can cross-reference data between systems, enabling them to research, investigate and respond to incidents 30 percent faster than before. "Our ultimate goal is to protect our customers, employees and data. With ES and Splunk Cloud as our SIEM platform, the information we want is always at our fingertips," says George Do, Equinix CISO.

"Whenever we need to investigate an incident, we simply display the relevant data in Splunk dashboards, so the information can be accessed by everyone on our security team as well as our C-level executives. The savings in time and effort are huge, as is the savings of 50 percent in total cost of ownership (TCO) compared to deploying a traditional on-premises based SIEM."

Thanks to Splunk ES, Equinix is now armed with comprehensive security analytics. For example, whenever a user account shows signs of suspicious activity, such as a local employee unexpectedly logging in from another continent, high priority alerts are immediately triggered and sent to the security team. Also, using Splunk Cloud with ES enables Equinix to prevent the leakage of sensitive business information. In particular, administrators use correlations to determine whether a departing employee might be seeking to steal confidential data. **Read more**.

Advanced threat detection

Security threats continually evolve. An analytics-driven SIEM can adapt to new advanced threats by implementing network security monitoring, endpoint detection and response sandboxing and behavior analytics in combination with one another to identify and quarantine new potential threats. Most firewalls and intrusion protection systems can't provide these capabilities on their own.

The goal should be not only to detect threats, but also to determine the scope of those threats by identifying where a specific advance threat may have moved to after being initially detected, how that threat should be contained, and how information should be shared.

SAIC gains visibility and threat detection

Science Applications International Corp. (SAIC) is a leading technology integrator that specializes in technical, engineering and enterprise information markets. With expertise in domains such as scientific research, program management and IT services, SAIC derives most of its income from the U.S. government. The company needed to build out a robust security operations center (SOC) and computer incident response team (CIRT) to defend against cyberattacks. Since deploying the Splunk platform, the company has seen benefits including:

- Improved security posture and operational maturity
- 80+ percent decrease in incident detection and remediation times
- Comprehensive visibility throughout the enterprise environment

Why Splunk

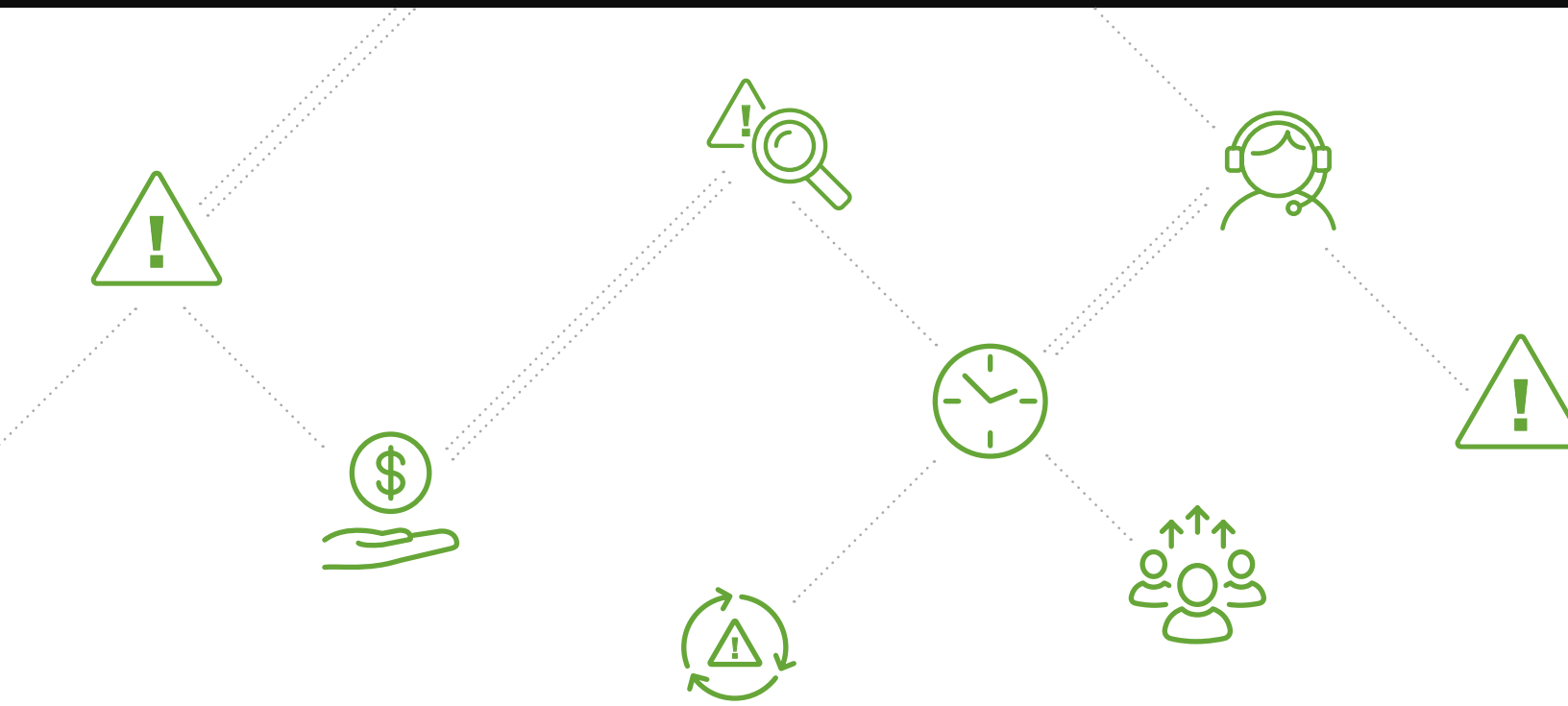
After the original SAIC split into two companies in 2013 to avoid organizational conflicts of interest, SAIC needed to build a SOC as part of its new security program. Although it had most of the security tools it needed, SAIC lacked a security information and event management solution to anchor its defenses. The traditional SIEM used by the original company as its core tool for security investigations had limitations. SAIC supplemented the SIEM with Splunk Enterprise, using the platform for incident detection via correlation searches, as well as for incident investigations. SAIC's IT operations staff is now also using the Splunk solution for network monitoring, performance management, application analytics and reporting.

Once SAIC began building its new SOC, the company decided to rely on Splunk as the single security intelligence platform for all of its SIEM-like needs, including incident detection, investigations and reporting for continuous monitoring, alerting and analytics.

Full visibility and threat detection across the environment

SAIC now uses Splunk software to monitor its environment for any threats. In the SOC, analysts monitor custom Splunk dashboards for alerts and signs of anomalous or unauthorized behavior. They're now immediately aware of known, signature-based threats (such as those logged by the IDS or malware solution), and unknown threats (such as a privileged account with atypical activity).

Traditional SIEMs generally search using pre-built, rigid searches, which fail to catch advanced threats and generate substantial false positives. With the Splunk platform, SAIC analysts have built new, highly accurate correlation searches to detect threats and indicators of compromise specific to SAIC, allowing the team to measure and manage risk at a high level. Executives, including the CISO, can now see key metrics around threat activity, including trends, the aggregated source location and newly seen indicators of compromise. **Read more**.



3. THE 9 TECHNICAL CAPABILITIES OF A MODERN SIEM

Now that you understand the **six essential capabilities of an analytics-driven SIEM**, we dive deeper into the technology that makes up an analytics-driven SIEM solution, to help you further differentiate a modern SIEM from legacy SIEMs, open source SIEMs, and new entrants in the SIEM market, such as UBA vendors.

Gartner's annual Magic Quadrant for Security Information and Event Management report is recommended reading for anyone exploring the SIEM market. As the report has evolved, it has grown to include open source SIEM vendors and new technologies, such as UEBA vendors.

The analyst firm also puts out supplemental SIEM reports and, in another research note, it highlights nine technical capabilities that differentiate a modern SIEM, such as what Splunk can provide, from these other categories.

The nine technical capabilities that differentiate a modern SIEM solution from the broader categories are:

	SPLUNK	LEGACY SIEM	OPEN SOURCE	NEW ENTRANTS
1. Collect logs and events	Yes	Yes	Yes	Yes
2. Real-time application of correlation rules	Yes	Yes	DIY	Yes
3. Real-time application of advanced analytics and machine learning	Yes	Limited	DIY	Yes
4. Long-term historical analytics and machine learning	Yes	Limited	DIY	Limited
5. Long-term event storage	Yes	Limited	Yes	Limited
6. Search and reporting on normalized data	Yes	Yes	Yes	Yes
7. Search and reporting on raw data	Yes	Complex	Yes	Complex
8. Ingestion of context data for additional correlation and analytics	Yes	Limited	Yes	Limited
9 Address non-security use cases	Yes	No	DIY	No

1. Collect logs and events

An analytics-driven SIEM solution should be able to collect, use and analyze all event logs and give a unified view in real time. This gives IT and security teams the ability to manage event logs from one central location, correlate different events over multiple machines or multiple days, tie in other data sources like registry changes and ISA Proxy logs for the complete picture. Security practitioners are also given the ability to audit and report on all event logs from a single place.

2. Real-time application of correlation rules

Event correlation is a way to make sense of a large number of security events and then drilling down to focus on those that actually matter by linking multiple events together to gain insights.

3. Real-time application of advanced analytics and machine learning, and (4.) long-term historical analytics and machine learning

There is a basic form of analytics, which in the context of a SIEM provides the insights behind data to reveal patterns. This allows security analysts to dig deeper and detect threats before they happen or do incident forensics.

A recent **Forrester survey** found that 74 percent "... of global enterprise security technology decision makers rate improving security monitoring as a high or critical priority" and "...vendors are adding security analytics features to existing solutions, and newer vendors are building (security analytics) solutions that leverage newer technologies without the baggage of legacy solutions."

Machine learning (ML) takes data analysis even further. ML empowers organizations with an analytics-driven SIEM solution to use predictive analytics that get smarter from historical data. This benefits security practitioners to detect incidents, predict or even prevent attacks, and more.

5. Long-term event storage

An analytics-driven SIEM solution has the ability to store historical log data for the long term. This enables the correlation of data over time and it also helps meet compliance mandates.

Why does this matter in terms of security specifically? Long-term machine data retention enables security analysts to perform security forensics to retrace the attack route of a network breach, for example.

6. Search and reporting on normalized data

Searching and reporting in terms of a SIEM allows users to search their data, create data models and pivots, save searches and pivots as reports, configure alerts, and create dashboards that can be shared.

7. Search and reporting on raw data

Searching and reporting of raw data, in terms of a SIEM, is the collection of data from various sources and centralized by an analytics-driven SIEM solution. An analytics-driven SIEM solution, unlike a legacy system, can ingest raw data from almost any source. That data can then be turned into actionable intelligence, and further, it can be turned into easy to understand reports, distributed directly from the SIEM platform to the appropriate people.

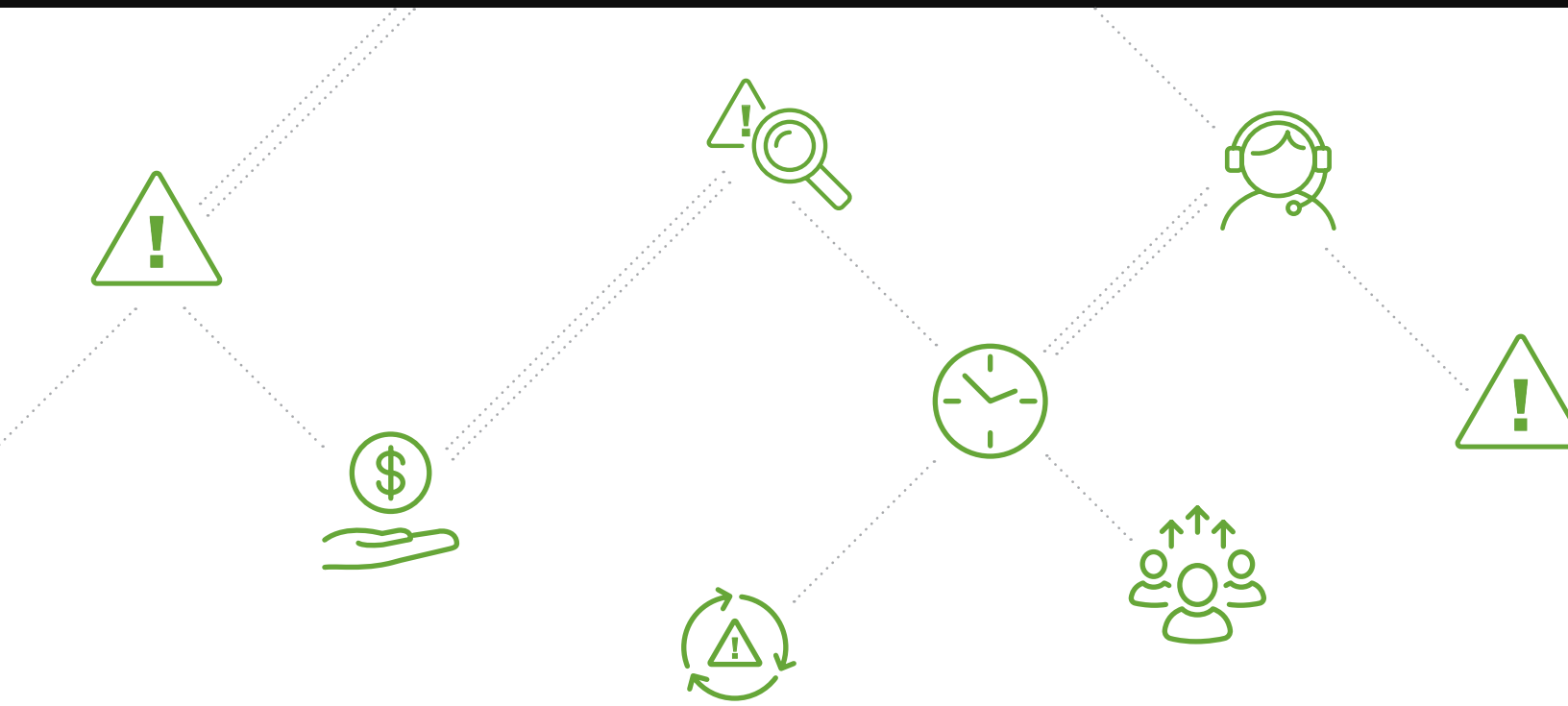
8. Ingestion of context data for additional correlation and analytics

After an analytics-driven SIEM solution collects data, the user needs additional context to know what to do with that data and what it means. This is critical to be able to differentiate real threats from false alerts and to be able to effectively detect and respond to real threats.

An analytics-driven SIEM solution is able to add context to external threat intelligence, internal IT operations and events patterns. This allows a user to further drill down and respond to threats in real time.

9. Address non-security use cases

Another distinction between an analytics-driven SIEM solution and a legacy SIEM solution is its ability to be used for multiple use cases, including non-security uses, such as IT Ops.



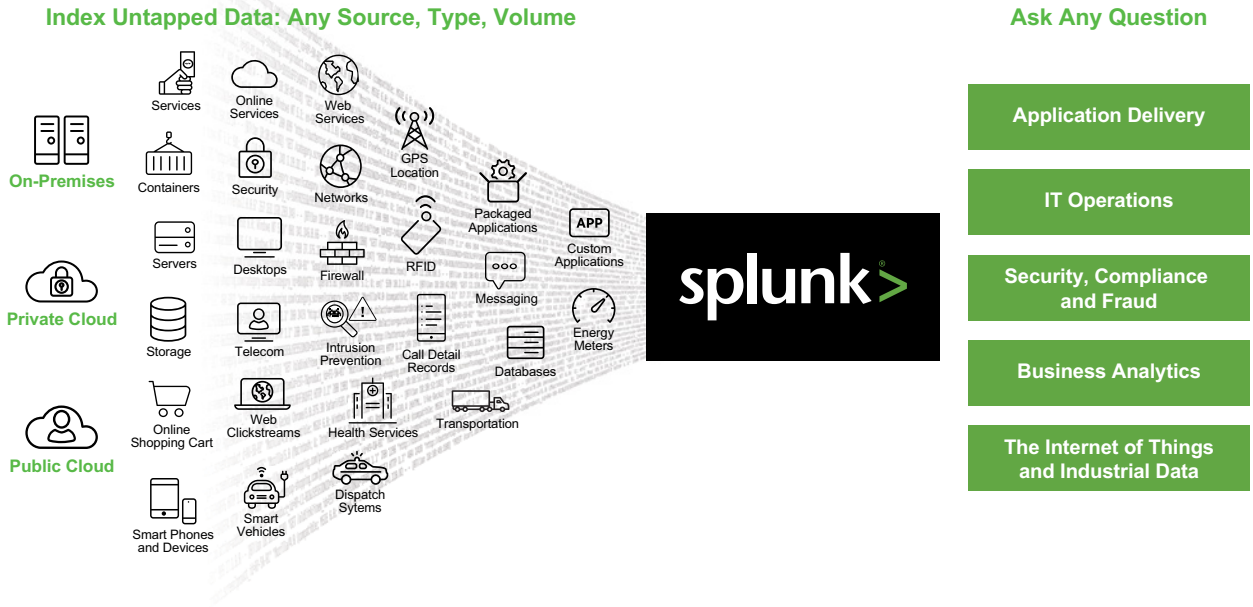
4. ENTER SPLUNK

Machine-generated data is one of the fastest growing and complex areas of big data. It's also one of the most valuable, containing a definitive record of all user transactions, customer behavior, machine behavior, security threats, fraudulent activity and more. Splunk turns machine data into valuable insights no matter what business you're in. It's what we call Operational Intelligence.

Splunk Enterprise monitors and analyzes machine data from any source to deliver Operational Intelligence to optimize your IT, security and business performance. With intuitive analysis features, machine learning, packaged applications and open APIs, Splunk Enterprise is a flexible platform that scales from focused use cases to an enterprise-wide analytics backbone. Splunk Enterprise:

- Collects and indexes log and machine data from any source
- Powerful search, analysis and visualization capabilities empower from across an organization
- An expansive Splunkbase app ecosystem provides solutions for security, IT ops, business analysis and more
- Available as on-premises software or as a cloud service

Turn Machine Data Into Business Value



Operational Intelligence gives you a real-time understanding of what's happening across your IT systems and technology infrastructure so you can make informed decisions. It is enabled by the Splunk platform, the foundation for all of Splunk's products, premium solutions, apps and add-ons.

Splunk as your SIEM

Splunk security solutions not only meet the new criteria for today's SIEM, but also deliver security analytics capabilities, providing the valuable context and visual insights that help security teams to make faster and smarter security decisions.

Splunk offers several options for enterprises looking to deploy their SIEM or to migrate from their legacy SIEM, and offers the choice of on-premises, cloud or hybrid deployment options.

Customers can solve their basic SIEM use cases using either Splunk Enterprise or Splunk Cloud. Splunk Enterprise and Splunk Cloud are core Splunk platforms, providing the collection, indexing, search and reporting capabilities, or CLM. Many Splunk security customers use Splunk Enterprise or Splunk Cloud to build their own real-time correlation searches and dashboards for a basic SIEM experience.

Splunk offers a premium solution, Splunk Enterprise Security (ES), which supports advanced SIEM use cases with ready-to-use dashboards, correlated searches and reports. Splunk ES runs on Splunk Enterprise, Splunk Cloud or both. In addition to pre-built correlation rules and alerts, Splunk ES contains incident review, workflow functionality and third-party threat intelligence feeds that help your investigations. Additionally, there are over 300 other security-related apps on Splunkbase with pre-built searches, reports and visualizations for specific third-party security vendors. These ready-to-use apps, utilities and add-ons provide capabilities ranging from monitoring security, next generation firewall, advanced threat management and more. These increase the security coverage and are provided by Splunk, Splunk partners and other third-party providers.

Splunk ES is also an analytics-driven SIEM made of five distinct frameworks that can be leveraged independently to meet a wide range of security use cases including compliance, application security, incident management, advanced threat detection, real-time monitoring and more. An analytics-driven SIEM platform combines machine learning, anomaly detection and criteria-based correlation within a single security analytics solution.

Splunk ES lets you visually correlate events over time and communicate details of multi-stage attacks.

The platform also makes it possible for organizations to discover, monitor and report in real time on threats, attacks and other abnormal activity from across all security-relevant data with business context. With advanced analytics, customers realize accelerated threat detection and rapid incident response across the entire security ecosystem.

Splunk ES is part of a broader security portfolio that provides CLM with Splunk Enterprise and advanced UBA features with Splunk User Behavior Analytics (UBA).

What Makes Splunk Work as a SIEM

- Splunk software can be used to operate security operations centers (SOC) of any size (large, medium, small)
- Support the full range of Information Security operations – including posture assessment, monitoring, alert and incident handling, CSIRT, breach analysis and response, and event correlation
- Out-of-the-box support for SIEM and security use cases
- Detect known and unknown threats, investigate threats, determine compliance and use advanced security analytics for detailed insight
- Proven integrated, big data-based security intelligence platform
- Use ad hoc searches for advanced breach analysis
- On-premises, cloud, and hybrid on-premises and cloud deployment options.

Splunk UBA

Splunk UBA is a machine learning-powered solution that delivers the answers you need to find unknown threats and anomalous behavior across users, endpoint devices and applications. It not only focuses on external attacks but also the insider threat. Its machine learning algorithms produce actionable results with risk ratings and supporting evidence that augment security operation center (SOC) analysts' existing techniques for faster action. Additionally, it provides visual pivot points for security analysts and threat hunters to proactively investigate anomalous behavior.

Splunk UBA at a glance:

- Enhances detection footprint by using a behavior-centric, purpose-built and configurable machine learning framework that leverages unsupervised algorithms
- Augments SOC analyst UEBA capabilities by automatically stitching hundreds of anomalies into a single threat
- Provides enhanced context by visualizing threats across multiple phases of the attack
- Supports bi-directional integration with Splunk Enterprise for data ingestion and correlation and with Splunk Enterprise Security for incident scoping, investigation and automated response

InfoTeK and Splunk deliver a security intelligence platform for the public sector

Many organizations depend on SIEM software to monitor, investigate and respond to security threats. But at one U.S. government agency its mission was hampered when its legacy SIEM software from HP ArcSight failed to live up to expectations. The agency turned to InfoTeK, a leading cybersecurity, software and systems engineering firm, to replace its SIEM tool. Since deploying the Splunk platform, the customer has seen benefits including:

- Deploying in one weekend and stopping an attack the next day
- Achieving a 75 percent cost reduction to support its SIEM
- Reducing number of tools required, including log aggregators and endpoint solutions

With Splunk Enterprise and Splunk ES, the agency has an analytics-driven SIEM that provides the IT team with actionable security intelligence at an affordable cost. InfoTeK deployed Splunk software over one weekend for the customer.

Starting the very next day, the software proved its value. The IT team was able to search security events and immediately thwarted an attack vector.

"Something that used to take hours, days or even weeks with other products or jumping between multiple tools can be done in seconds, minutes or hours with Splunk," says Jonathan Fair, senior incident handler and security engineer at InfoTeK. "We were able to provide a ROI before the product was even fully purchased because the customer successfully stopped a threat that would have required a complete rebuild of the network." Read more.

Click here to see how InfoTek reduced its SIEM costs 75 percent.

MONITOR REPORT	DETECT ALERT	ANALYZE INVESTIGATE	RESPONSE COLLABORATE	SIEM
Pre-defined views and rules	Correlation rules, threshholds	Analysis investigation & context enrichment	Enterprise-wide coordination and response	Security Ops management alert, and incident management, policy-based rules, out-of-box security rules & analysis

US government cabinet-level department saves $900,000 on legacy software maintenance

Citizens expect government agencies to not only spend taxpayer dollars wisely but also make every effort to ensure resilient operations to deliver services effectively. One large U.S. cabinet-level department previously had HP ArcSight, a slow and expensive security information and event management tool that did not stand up to the needs of the agency. Since replacing it with Splunk Enterprise for security and compliance the department has seen benefits, including:

- Saving $900,000 annually on software maintenance
- Improving security detection, response and remediation
- Reducing security investigation time from hours to minutes

Proactive security approach

Margulies and his team support the department's SOC, including 40 analysts who use Splunk Enterprise to investigate security incidents, as well as a large enterprise IT team that depends on the software for troubleshooting and reporting. Additional customers include staff who must ensure the department complies with security regulations.

Heartland Automotive protects brand reputation, secures data with Splunk platform

Known for its signature oil change, Heartland Automotive Services, Inc., dba Jiffy Lube, is the largest franchisee of quick lube retail service stores in the U.S. Heartland Automotive needed a cybersecurity platform to protect its brand and its most important resource—its data. Since deploying Splunk ES and Splunk UBA as its integrated SIEM platform, Heartland Automotive has seen benefits, including:

- Realized time to value by implementing a SIEM and insider threat protection solution in only three weeks
- Gained platform to drive innovation with 25 percent less TCO
- Established real-time security investigations and insider threat protection

SIEM implementations are often complex, as large organizations have many data sources and it may require weeks to configure alerts. According to Alams, the Splunk professional services team made the entire process of identifying the company's data sources, fleshing out the SIEM design and configuring alerts seamless.

"Fast time to value is everything—we were able to implement a SIEM and insider threat detection solution in three weeks in what would normally take three months," says Chidi Alams, head of IT and Information Security, Heartland Automotive Services. "The chief financial officer and other members of our senior leadership team have been impressed with time to value—to see it one day and almost be implemented the next—increased their confidence in us to deliver quickly." Read more.

Click here to learn how Heartland Automotive drove innovation using Splunk with 25 percent less TCO.

The Splunk ROI story

An analytics-driven SIEM solution is often criticized for being an expensive investment. But the reality is the expense is in the eye of the beholder.

How expensive does an analytics-driven security solution seem after your organization has fallen victim to an insider attack? Or a ransomware attack that steals headlines.

So, there is the immediate return on investment (ROI) of not being breached and proactively protecting your organization from both insider and outside malicious actors.

But that is not where the return on investment from a SIEM ends.

An analytics-driven SIEM solution supports common IT use cases, such as compliance, fraud, theft and abuse detection, IT operations, service intelligence, application delivery and business analytics

As security teams work in concert with other IT functions, the visibility from other use cases results in a centralized view across the organization with cross-department collaboration and stronger ROI.

The best way to understand the real ROI of an analytics-driven SIEM solution is to hear from those who already have one.

The future of SIEM

The basic underlying technology that drives a SIEM may have been around for years but that does not mean that all SIEMs are a dinosaur technology.

In fact, not all SIEMs are created equal as this buyer's guide highlights. And this is best shown by understanding the differences between a legacy SIEM solution and a modern analytics-driven solution.

It is these analytics-driven SIEMs that present the brightest light for the future of the market. These modern security solutions still are a great for threat detection, remediation, alerting, compliance reporting, while delivering a demonstrable ROI.

And as the modern threat landscape continues to evolve, analytics-driven SIEM solutions have proven they are able to adapt and stay ahead of these threats.

Do you want to learn more about Splunk's analytics-driven SIEM solution and how it can help improve your organization's security posture? **Speak with a Splunk expert now**.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

WP-Splunk-SIEM-Buyers-Guide-101