ANALYTICS-DRIVEN SECURITY POWERS NEXT GENERATION SIEMS

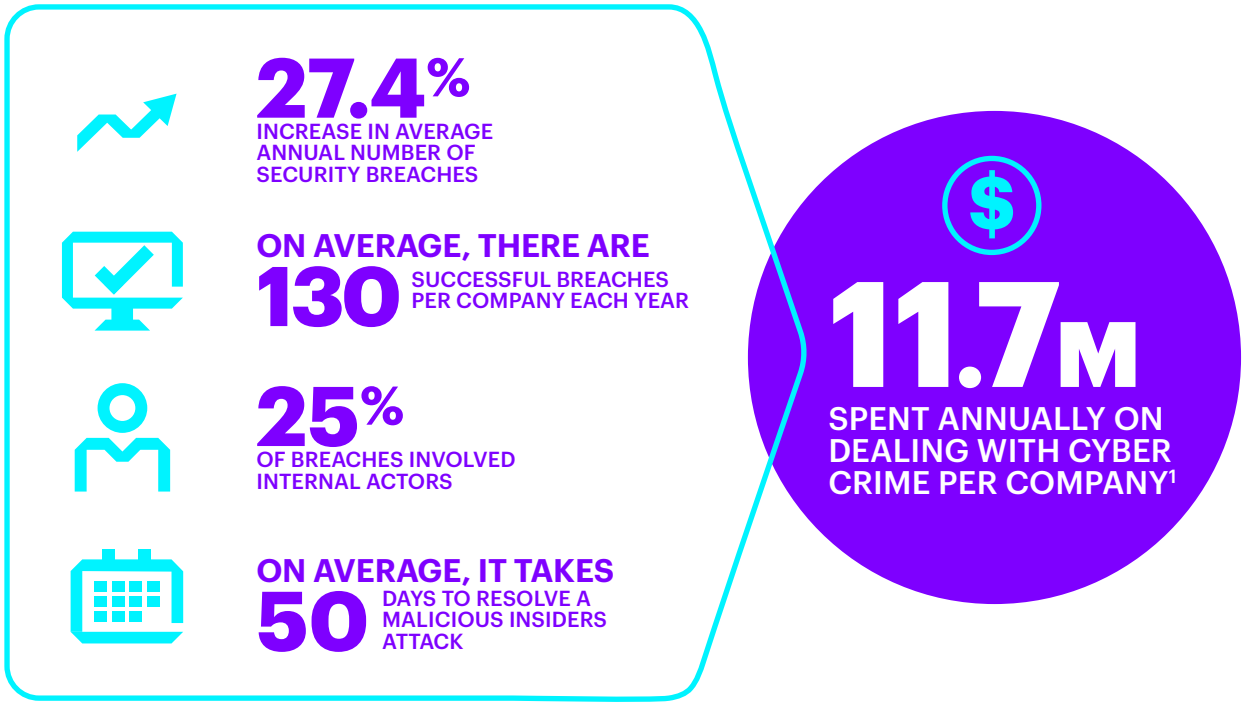
with Accenture's SIEM Transition Services

splunk>

accenture

INCREASINGLY COMPLEX CYBER THREATS DEMAND AN INNOVATIVE APPROACH TO VISIBILITY AND PREPAREDNESS

The complexity and volume of cyber threats has seen explosive growth in the past few years. High profile ransomware attacks and data breaches have plagued some of the largest organizations in the world, leading to the loss of millions of dollars due to halted business operations and remediation activities. For organizations to protect their employees, customers, and brand, they need to implement leading technology Security Information and Event Monitoring (SIEM) solutions to improve their ability to detect and remediate threats.



Source: 2017 Data Breach Investigations Report 10th Edition, 2017
[1]Cost of Cyber Crime Study, 2017

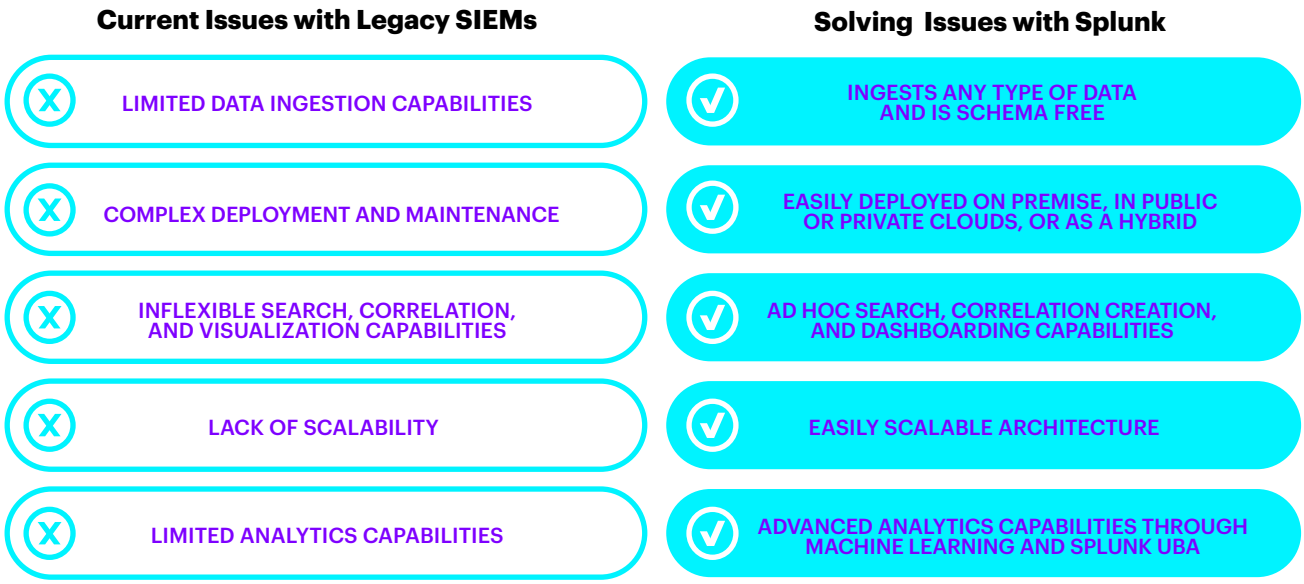
SIEM AS AN ANALYTICS - DRIVEN PLATFORM

In order to address the increasing pace and scale of cyber threats, SIEM solutions must be capable of providing visibility across the entire enterprise using every available data source – not just security data. Advanced analytics can leverage big data to detect threats in unlikely places, but it requires a holistic approach to data ingestion. The good news is that with a more robust platform, this increased data ingestion can serve more than just IT Security use cases, including OT Security, Business Analytics, DevOps, IT Ops, and a myriad of others. Splunk Enterprise Security (ES) is an industry-leading next generation SIEM product that provides organizations

the ability to gain full visibility across the enterprise. Compared to legacy SIEM solutions Splunk is uniquely able to ingest data in real time without a predefined schema, allowing for correlation across both structured and unstructured data sources alike. Not only can organizations monitor petabytes of data with a single deployment, they can also create custom alerts, correlations, and searches using advanced analytics and machine learning frameworks. Based on the requirements of the organization, Splunk is easily scalable on-premise, in the cloud, or in a hybrid environment. Beyond being an analytics-driven SIEM, Splunk solves most major challenges associated with legacy SIEM products.

SOLVING LEGACY SIEM ISSUES WITH SPLUNK

Splunk has a unique approach to data ingestion, with a flexible and easily scalable architecture, and ability to support a wide variety of business-enabling use cases. In December 2017, Splunk was positioned as a Leader in the Gartner Magic Quadrant for Security Information and Event Management for the 5th consecutive year. Organizations often look to improve what their SIEM is capable of by switching to Splunk Enterprise Security. In some cases, that involves a net new acquisition of Splunk, beginning with Security as the first use case. In other instances, an organization that already owns Splunk for IT operations or other use cases, and looks to migrate Security into the platform to consolidate capabilities, reduce total cost of ownership, and simplify their technology footprint. In either instance, transitions from a legacy SIEM to a next generation SIEM can potentially be long and complex, with impacts on cyber security operations. Organizations need the right partner to help them ease through the transition without disrupting critical business functions.



Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

TRANSITION TO SPLUNK ENTERPRISE SECURITY USING ACCENTURE'S PROVEN METHODOLOGY

The process of transitioning from a legacy SIEM to a next generation SIEM requires assessment of the environment, resources, data sources, integrations, and use cases while maintaining the continuity of security operations. Accenture can help organizations streamline the transition process with our proven Accenture Delivery Methodology (ADM) to ensure the continuity of operations during the transition while reducing unnecessary functionality and implementing enhancements.

Core Infrastructure Build/Transition

Security Monitoring and Incident Response services remain operational using the legacy SIEM, while the target state is designed and the transition approach is agreed upon. Accenture will then begin to develop Splunk's core infrastructure while continuing the ingestion of data into the legacy SIEM.

Data Onboarding, Use Case Development, and Capability Operationalization

Once the core platform is developed, data is ingested by both SIEMs to ensure parity while use cases and additional functionality are incorporated into Splunk. Data source onboarding, use case ideation and development, and process operationalization are conducted using an agile approach. Accenture's methodology focuses on only transferring to Splunk what matters – any unused data sources or ineffective use cases are left behind. Focusing on the most apparent threats, Accenture will recommend and implement use cases based industry-specific and organization-specific threats, in addition to the high value use cases that are maintained as part of Accenture's Splunk Security Use Case Library. Once use cases are developed and implemented, Accenture will work with response teams to integrate these use cases into existing and new incident responses processes, verifying that all use cases are actionable with concrete response actions.

Phased Service Transition

Once Splunk achieves parity to the legacy SIEM, Accenture will begin the process to transition Security Monitoring and Incident Response services to Splunk ES. If feeding data directly from the legacy SIEM to Splunk, the transition team will displace those feeds and integrate Splunk directly with data sources. With Security Monitoring and Incident Response services powered by Splunk ES fully operational, the legacy SIEM is decommissioned. The transition team provides maintenance and support while onboarding net new capabilities beyond the capabilities of the legacy SIEM.

Our SIEM Transition Approach

Security Monitoring and Incident Response services remain operational using the legacy SIEM, while the target state is designed and the transition approach is agreed upon.

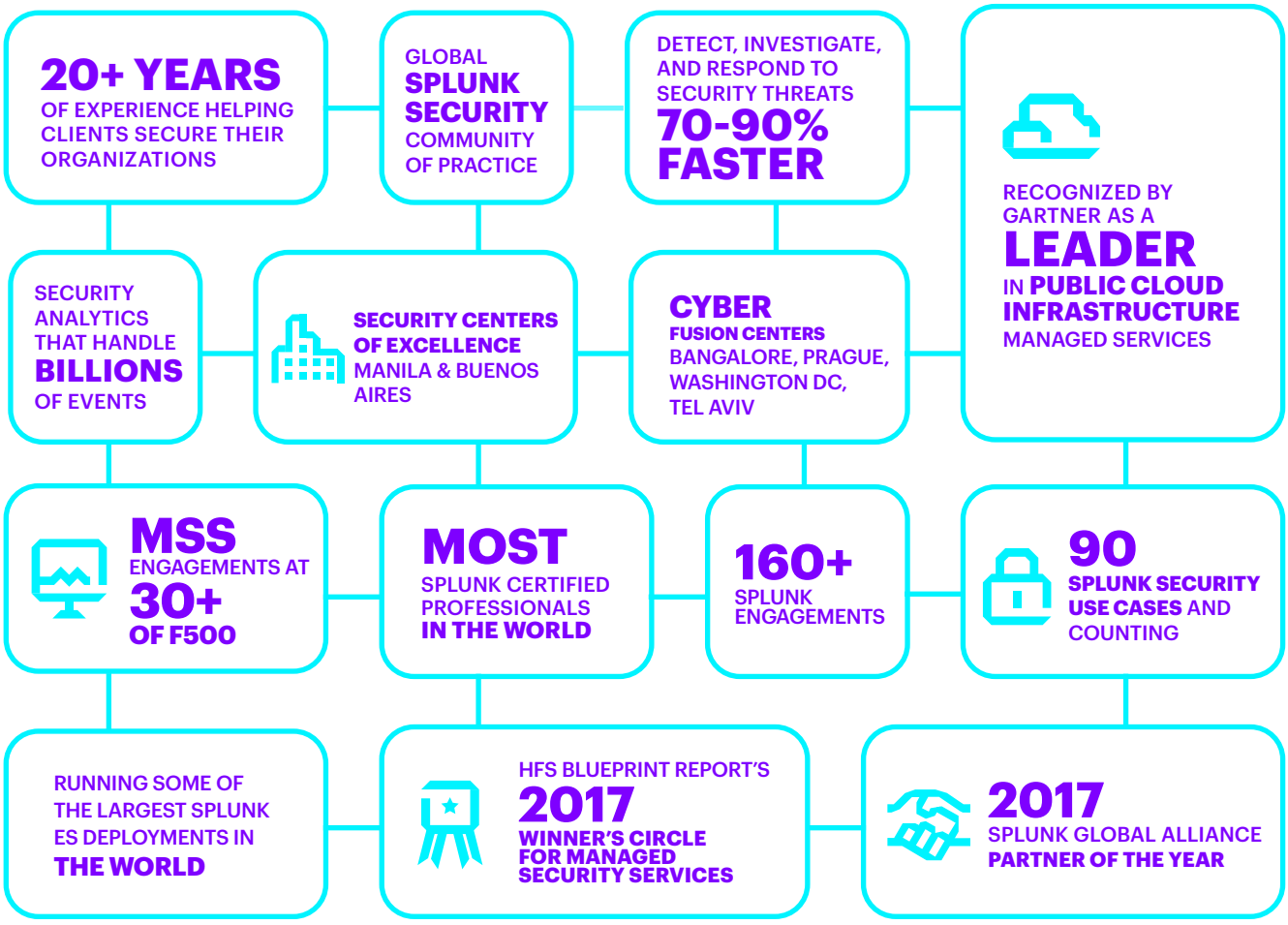
Log data is collected by both the legacy SIEM and Splunk (directly or indirectly). Use cases, data sources, and functionality is onboarded to Splunk while legacy Security Monitoring and Incident Response remain operational.

Once Splunk achieves parity to the legacy SIEM, transition Security Monitoring and Incident Response services. If feeding data directly from the legacy SIEM to Splunk, displace with feeds directly from the data sources.

With Security Monitoring and Incident Responses services powered by Splunk ES fully operational, the legacy SIEM is decommissioned. Onboarding of net new capabilities above legacy SIEM parity begins.

JOIN THE NEXT GENERATION OF CYBER DEFENSE CAPABILITIES WITH ACCENTURE AND SPLUNK

Accenture employs the largest number of Splunk-certified professionals in the world. Our extensive experience transitioning clients to Splunk is matched by our ability to transform Splunk-based organizations into mature, proactive threat-hunting operations. With Accenture, organizations can be confident in their ability to quickly and effectively defend against the latest cyber threats.



SIEM Transition in Oil and Gas

To meet current and future security and regulatory requirements, an international oil and gas company needed a solution to improve the protection of its business-critical applications and information from cybersecurity threats. Accenture helped the organization transition all monitoring capabilities from ArcSight to Splunk Enterprise Security. This included the integration of 40 different data sources, development of custom dashboards and use cases, and scaling the deployment to process 2.5 terabytes of data per day. As a result of Accenture's efforts, the organization has been able to to increase their visibility across the enterprise and reduce time to detect and respond to incidents.

SIEM Transition in Retail Banking

A leading online retail bank was divested from its parent company and needed Accenture's help to stand up an entirely new technology infrastructure, establish security processes, and develop integrations between Splunk Enterprise Security and numerous data sources. Accenture built a highly available and scalable Splunk platform across two data centers while running security operations and training the bank's new cybersecurity personnel. In addition to transitioning to Splunk, Accenture developed standardized processes to ensure regulatory compliance and streamlined operating procedures to govern the new security monitoring infrastructure and operations.

For more information on Accenture's SIEM Transition Services, please contact:

JEFF CHANCEY
Accenture
jeffry.t.chancey@accenture.com

JEFF PENN
Splunk
jpenn@splunk.com

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world's largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 442,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at **www.accenture.com.**

ABOUT SPLUNK

Splunk Inc. is the market leader in analyzing machine data to deliver Operational Intelligence for security, IT and the business. Splunk® software provides the enterprise machine data fabric that drives digital transformation. More than 14,000 customers in over 110 countries use Splunk solutions in the cloud and on-premises. Splunk products include Splunk® Enterprise, Splunk Cloud™ and premium solutions. Join millions of passionate users by trying Splunk software for free: **www.splunk.com/free-trials.**