splunk>

accenture

MATURE YOUR CYBER DEFENSE OPERATIONS

with Accenture's SIEM Transformation Services

THE NEED FOR MATURE CYBER DEFENSE CAPABILITIES

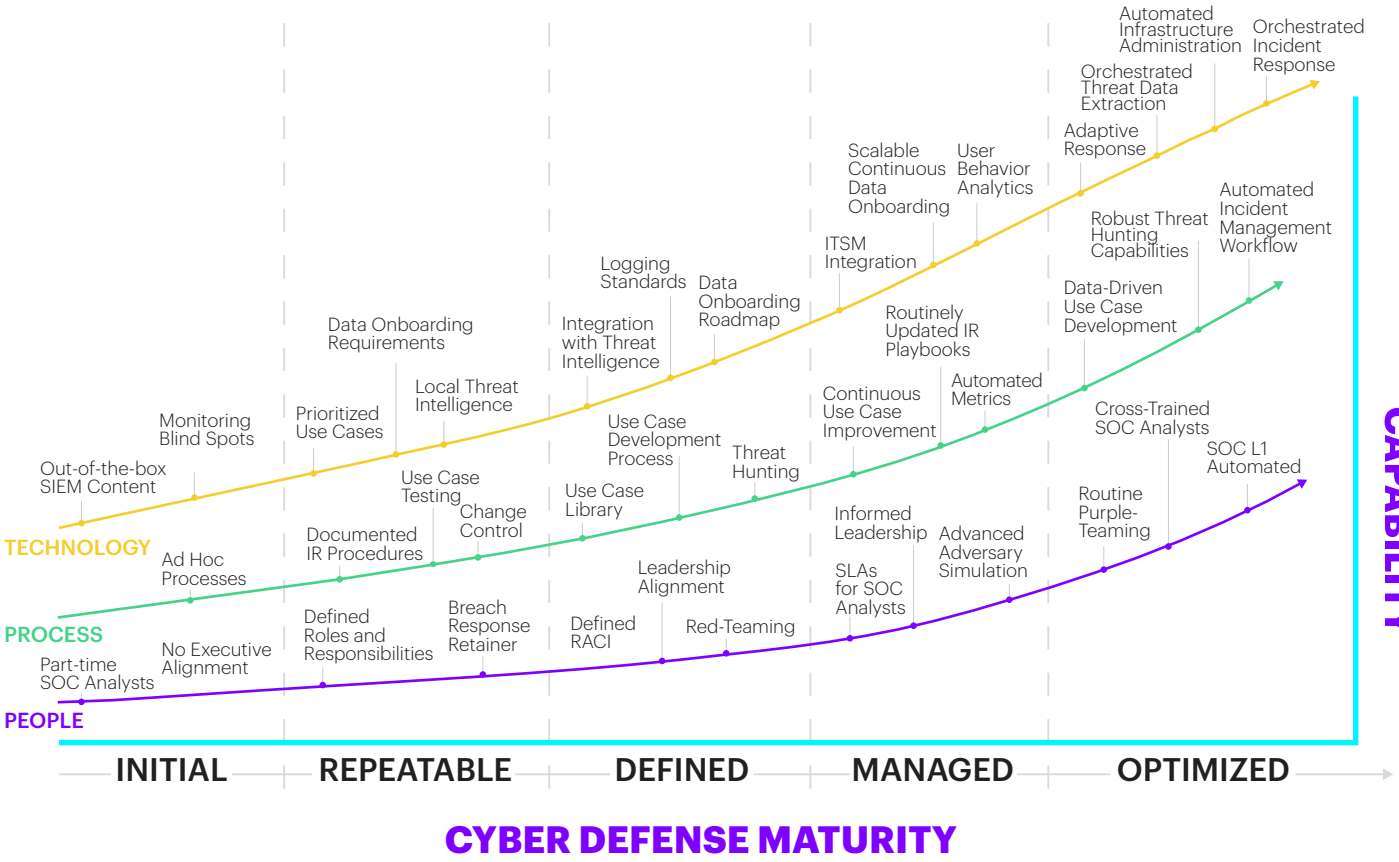
The average annual cost of cyber crime reached $11.7 million per organization in 2017 and continues to increase[1]. With the number of breaches escalating, cybersecurity stakes are high. FedEx estimates it incurred $300M in losses due to the NotPetya malware attack[2] and Equifax estimates a total of $87.5 million in losses due to a data breach[3], both occurring in 2017.

To better protect themselves, organizations are investing more than ever in improving visibility and cybersecurity capabilities—specifically their Security Information and Event Management (SIEM) solution and cyber defense operations. Security spend is projected to hit $92 billion in 2018 (a 9% increase from the previous year)[4] across their security operations, with a trend towards increasing and enhancing their existing Security Operations Center (SOC).

BUILDING ON THE FOUNDATION

For organizations to protect themselves from ever evolving threats, they must seek to continuously improve not only their cyber defense capabilities, but the efficiency at which they operate. The first step on the journey to maturing cyber defense capabilities is having an industry-leading SIEM, which provides advanced analytics, enables automation, and is highly versatile—such as Splunk Enterprise Security (ES). Once that foundation is in place, organizations can continuously build out their cyber defense organization and improve efficiency to create a lean and effective security nerve center to swiftly combat cyber threats.

Accenture has identified the key components of maturing cyber defense operations across People, Process, and Technology—from the initial implementation of a SIEM with a brand new team of SOC Analysts to proactive threat-hunting experts who can focus on high value activities while automation and advanced integrations drive routine tasks. Where does your organization fall on the maturity curve? How do you plan to get to the next level?



STRUGGLING TO KEEP UP

Organizations face many challenges as they seek to improve their SIEM capabilities. Depending on the organization, these challenges can either hamper continuous progress or even halt maturity initiatives altogether.

CHALLENGE AREA	DISCRIPTION OF CHALLENGE	BUSINESS IMPACT
DOMAIN KNOWLEDGE	Lack of necessary security resources leading to a technical skills deficit	Hampered ability execute transformation goals and achieve strategic security objectives
DATA INUNDATION	Difficulty in onboarding and gaining valuable insights from the vast amounts of enterprise data (e.g. infrastructure, cloud, IoT, endpoints)	Inability to collect the necessary data to provide organization-wide visability
IDEATION & DEVELOPMENT	Lack of sustainable ideation/development processes which empower the SOC to continuously innovate towards protecting the enterprise	Technology assets and processes produce low value output
THREAT HUNTING	Reacting to incidents (i.e putting out fires) rather than proactively identifying new threats	Increased exposure to advanced threats
INCIDENT RESPONSE	Non-existent or non-standardized incident response processes	Inadequate response to incidents, leading to increased time to remediation
BREACH RESPONSE	Lack of deep expertise to quickly investigate, contain, and remediate a major breach	Increased costs associated with longer breach response times
DISPARATE SYSTEMS	Employing multiple technologies as point solutions that are not properly integrated	Inefficient spend and lack of holistic capabilities
INSIDER THREATS	Limited abilities to monitor employees' application/ data usage and detect anomalous bahavior	Increased exposure to internal threat actors

IMPROVING SIEM MATURITY WITH ACCENTURE

In order to help our clients overcome some of the fundamental challenges associated with improving SIEM maturity, Accenture has developed a suite of services focused on efficiently and effectively streamlining cyber defense operations towards more advanced functionality and greater cyber defense capabilities.

SIEM Maturity Assessment

Seasoned Splunk professionals with experience architecting, deploying, maintaining, and operating highly complex Splunk environments can help organizations understand the current state of their SIEM/SOC operations and what is needed to achieve the next level of SIEM maturity.

Data Onboarding Factory

Accenture can deploy cost effective and sustainable data onboarding processes to dramatically increase the speed and scale at which an organization can gain enterprise-wide visibility into their data. Accenture has experience setting up data onboarding factories that ingest 300+ data sources while navigating through complex regulatory requirements.

Use Case Development

Accenture can help an organization develop standardized use case development processes to improve detection and remediation of industry- and organization-specific threats. In addition, Accenture has its own proprietary use case library that is continuously updated based on cross-industry delivery experience.

iDefense Threat Intelligence

iDefense Threat Intelligence features the latest insights from dedicated threat intelligence analysts and vulnerability security researchers. Analysts and researchers directly interact with threat actors across a variety of channels to understand the latest attack methods. Harness this research by integrating iDefense with Splunk Enterprise Security to enrich data and prevent advanced attacks.

Response Process Operationalization

Accenture can develop tailored incident response processes in conjunction with an organization's SIEM/SOC operations. Leveraging seasoned IR experts and a continuously updated response process library, Accenture can help an organization operationalize its incident response capability.

Automation Engineering

Accenture can integrate Splunk Enterprise Security with a wide range of technologies and/or implement orchestration tools to automate detection and response capabilities. This allows for security resources to focus on strategic initiatives while improving the mean time to detect and respond to threats.

User Behavior Analytics

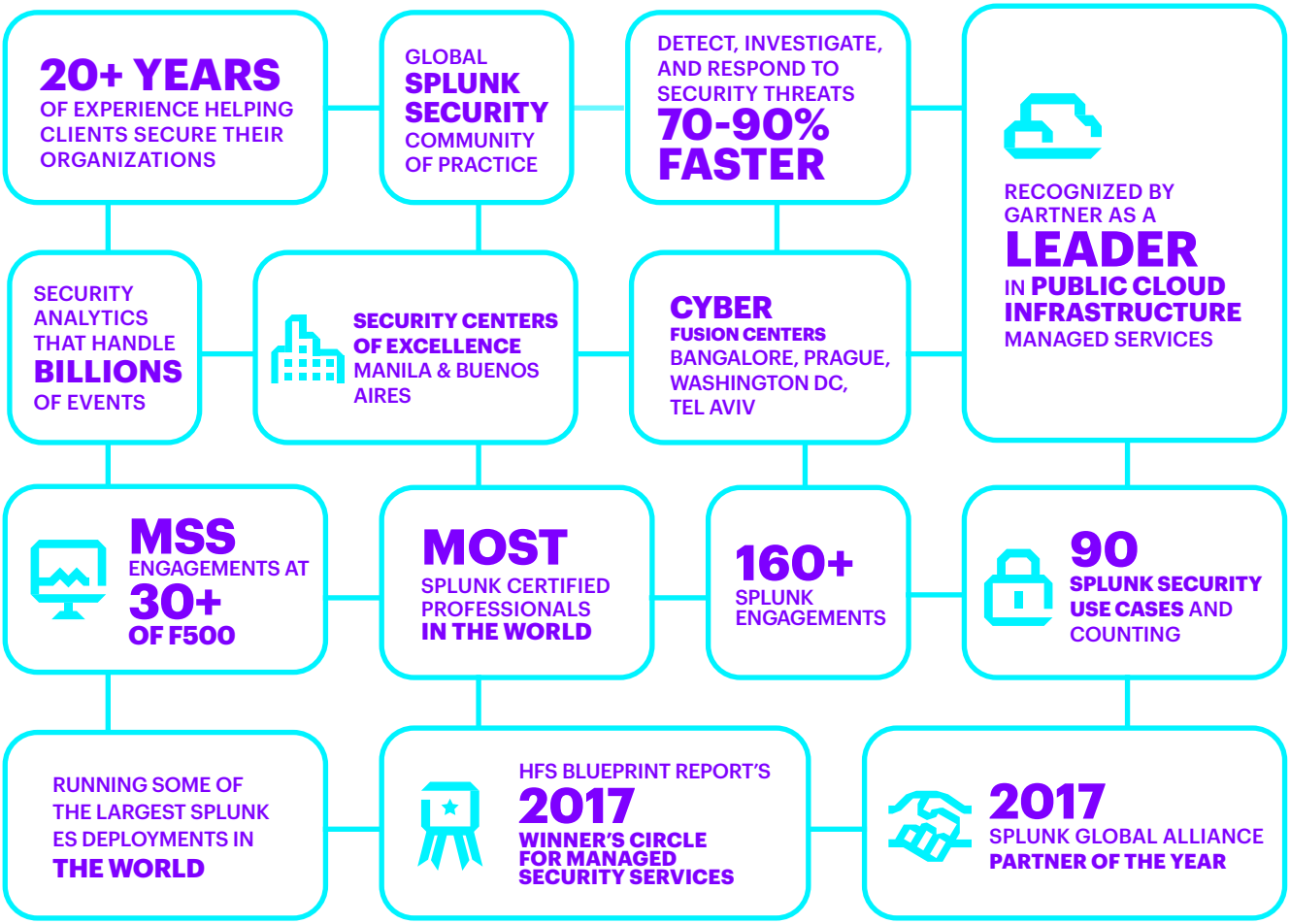
Accenture can implement and fine-tune Splunk User Behavior Analytics (UBA), leading to an advanced internal monitoring capability. Using machine learning, Splunk UBA can detect anomalous behavior and enhance existing use cases to better protect against both internal and external threats.

FusionX Incident Response Readiness

Gain access to a team of experts who can aid your organization in developing and executing a response plan in the case of a major incident. In addition, FusionX can test your SIEM capabilities through adversarial simulation and help your organization improve its' overall cyber defense capabilities.

STREAMLINE YOUR SIEM TRANSFORMATION JOURNEY—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.



Using advanced analytics to monitor internal threats and enhance existing use cases

A large government organization needed to meet compliance requirements as a result of new legislation and wanted to build an insider threat capability. Accenture assessed the organization's nascent Splunk deployment and helped to scale it through implementing a data onboarding factory, developing new use cases, and implementing Splunk User Behavior Analytics. As a result, the government organization now has an advanced threat hunting program.

Enabling scale through an efficient and rapid onboarding process to ensure appropriate visibility into a global organization

A global financial services firm needed help refining its Splunk architecture to create a strong basis to scale. Their current deployment was integrated with only a few log sources despite a two terabyte per day license and they faced increasing demand to onboard new data sources, a complex IT landscape, and an unclear governance model. Using highly experienced Splunk practitioners, Accenture deployed a data onboarding factory to efficiently and rapidly onboard 300+ data sources.

For more information on Accenture's Splunk Transformation 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.**

RESOURCES

[1] 2017 Cost of Cyber Crime, Accenture

[2] Equifax Faces Mounting Costs and Investigations From Breach, NYT

[3] The Hacks that Left us Exposed, CNN

[4] Gartner Forecast: Information Security, Worldwide, 2015-2021, 4Q17 Update, February 2018

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: **http://www.splunk.com/free-trials**