

Deloitte.



Splunk.conf 2020

AI-driven security operations
October 2020

ensemble Threat Detection & Response

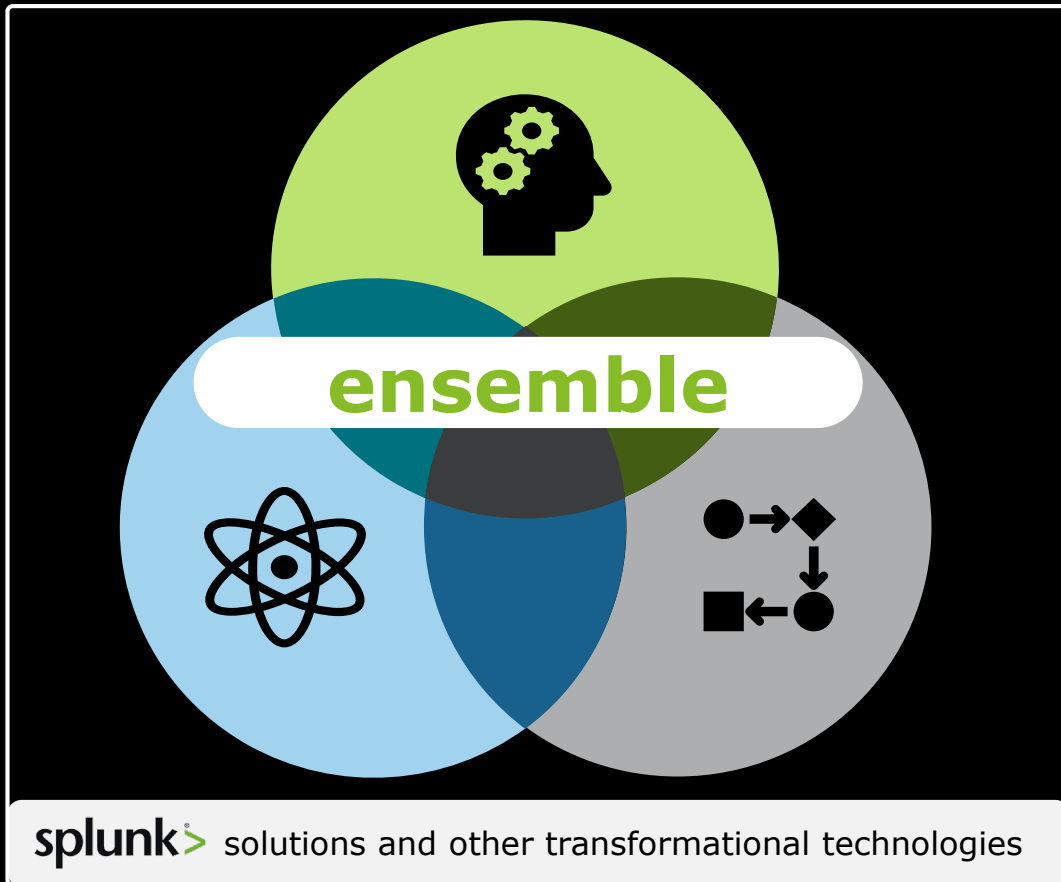
Problem statement

As cyber threats become more complex and frequent, many organizations are challenged with keeping pace with detecting and responding to them



Our approach

In response to these mounting constraints, Deloitte has developed an approach called **ensemble**, which leverages advancements in artificial intelligence (AI) – including data fusion, machine learning (ML), and automation to integrate, enhance and augment threat detection and response capabilities



Machine learning

Enhance and optimize current rules-based based alerts while expanding detection reach with advanced unsupervised, semi-supervised and supervised machine learning models



Automation

Create automated playbooks with combined workflows and processes that standardizes data collection, analytics, and remediation with specific decisions driven by the analyst

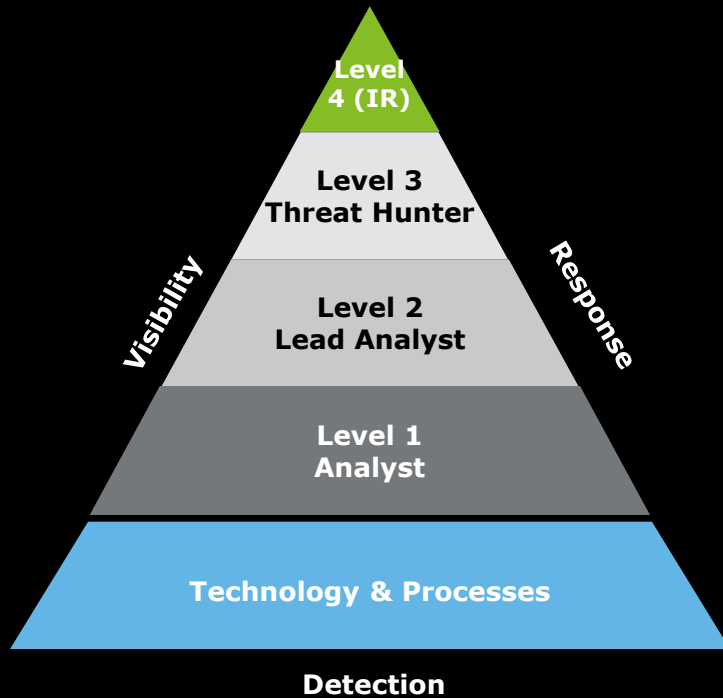


Data fusion

Integrate multiple data sources to produce consistent, well defined, and more useful information than provided by a individual data source thus provisioning scope for an informed analysis

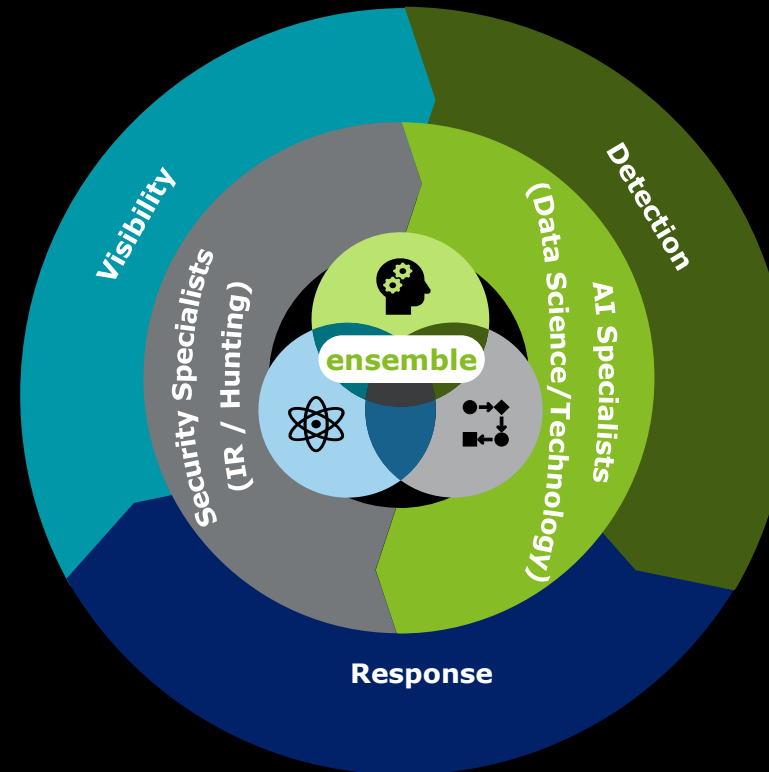
Why ensemble?

Our approach is designed to help Security Operations Centers (SOC) transform from traditional hierarchical and manually-driven processes into perpetually enhancing, AI-driven security operations programs (AI-SecOps)



Traditional SOC Hierarchy

- Separate teams of people with varying degrees of security experience
- Technology stacks are mostly siloed and processes are handled manually



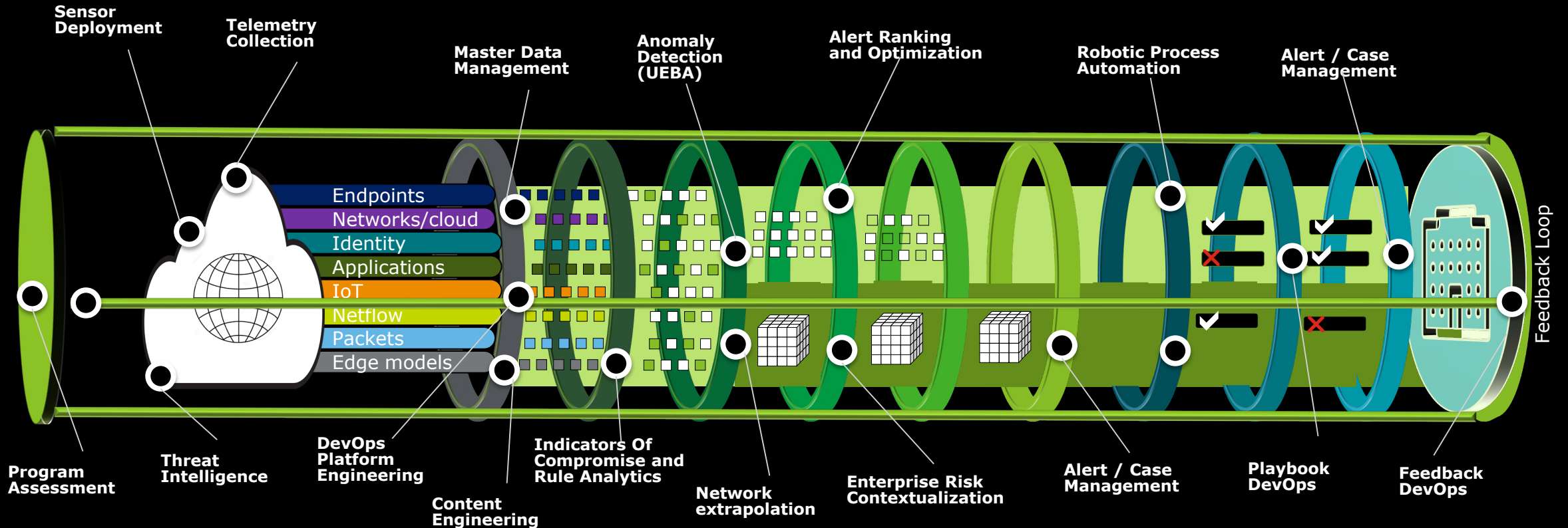
Next-gen Security Operations

- SecOps+DevOps - Technology and analytics personnel and Hunt - Security personnel
- Better integration between technologies to facilitate orchestration and automation across stack

Integrated approach

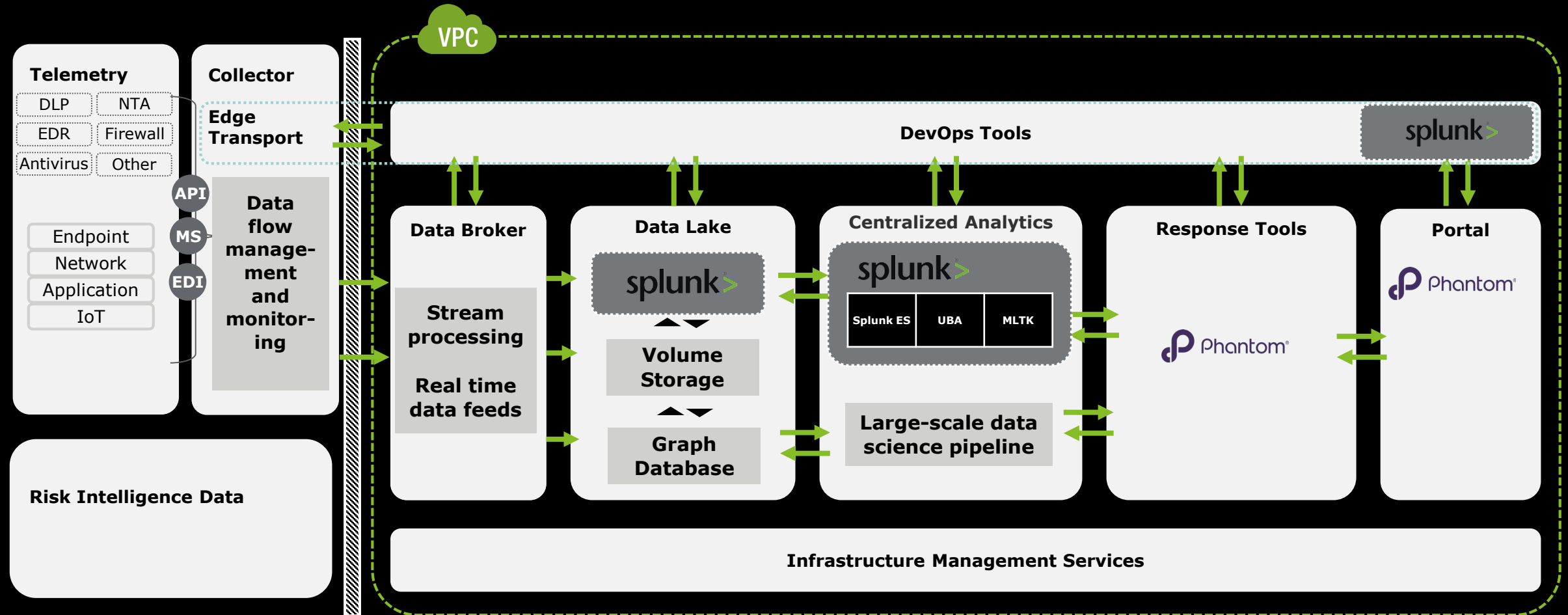
ensemble offers end-to-end assistance for SecOps transformation, embedding data fusion, ML and automation across the threat detection and response workflow

ensemble AI pipeline approach



Representative technologies

Leveraging a combination of core security and emerging analytics, development and processing technologies, Deloitte works with clients to systematically build transformational data and analytics platforms to AI – SecOps leveraging the ensemble methodology. All telemetry, data management, detection and response tools are integrated and managed together



Managing an array of business and security risks

ensemble approaches include use cases for an array of risk areas and our methodology is designed to standardize and integrate risk detection approaches across multiple business and security domains

Business Risk Categories (examples)

<p>Fraud <i>The risk of internal or external actors performing fraudulent activities</i></p>	<p>Reputation Loss <i>The risk of losing reputation due to a publicly announced incident</i></p>	<p>Risk to Business Resiliency <i>The risk of losing availability of applications that are critical to the business and the customers of the organization</i></p>	<p>Data Loss <i>The risk of losing data (sometimes permanently) due to error, equipment failure, or malicious intentional actions</i></p>
<p>Unauthorized Access <i>Threats that are realized due to unauthorized access to organization's data or other IT assets</i></p>	<p>Insider Threat <i>The risk of internal users (actors) trying to steal confidential data for monetary or other gains</i></p>	<p>Regulatory Non-Compliance <i>The risk of non-compliance with regulatory requirements which may result in financial or reputation loss</i></p>	<p>External Espionage <i>The risk of external parties trying to access organization's confidential information and intellectual properties</i></p>
<p>Infrastructure Availability Loss <i>The risk of losing availability of infrastructure that are critical to the business and the customers of the organization</i></p>	<p>Misuse of Privileges <i>The risk of misusing privileged access by admins and other users who have been given unrestricted or privileged access to company's IT assets</i></p>	<p>Data Integrity <i>The risk of losing integrity of organization's data while at rest or in transit</i></p>	<p>Negligence <i>The risk of employees or business partners acting wrongly due to ignorance or disregard (intentionally or unintentionally)</i></p>

Business risk categories - phishing

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker masquerading as a trusted entity, fools a user into opening an email, instant message, or text message.

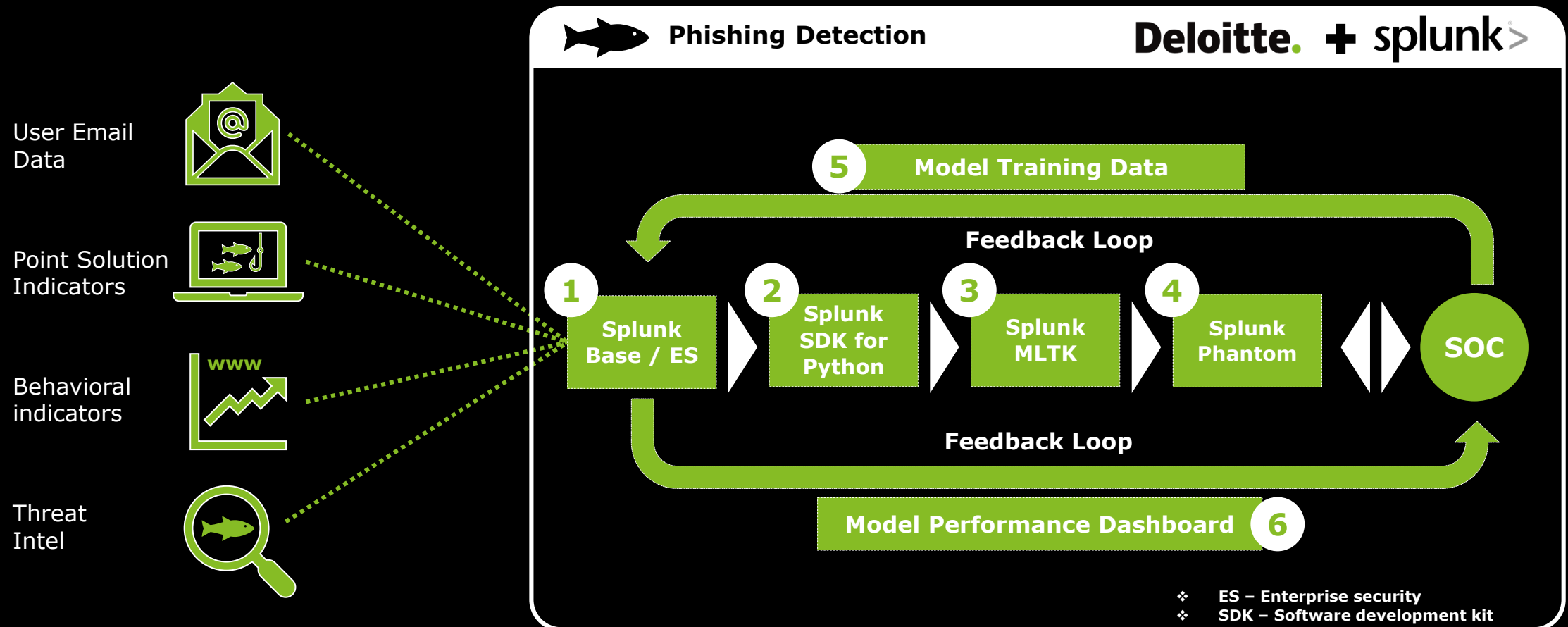
Business Risk Categories (examples)

Fraud: phishing – URL spoofed as legitimate domains with underlying malicious redirections could be major threat to IT organizations	Reputation Loss <i>The risk of losing reputation due to a publicly announced incident</i>	Risk to Business Resiliency <i>The risk of losing availability of applications that are critical to the business and the customers of the organization</i>	Data Loss <i>The risk of losing data (sometimes permanently) due to error, equipment failure, or malicious intentional actions</i>
Unauthorized Access <i>Threats that are realized due to unauthorized access to organization's data or other IT assets</i>	Insider Threat <i>The risk of internal users (actors) trying to steal confidential data for monetary or other gains</i>	Regulatory or Compliance <i>The risk of non-compliance with regulatory requirements which may result in financial or reputational loss</i>	External Espionage <i>The risk of external parties trying to access organization's confidential information and intellectual properties</i>
Infrastructure Availability Loss <i>The risk of losing availability of infrastructure that are critical to the business and the customers of the organization</i>	Misuse of Privileges <i>The risk of misusing privileged access by admins and other users who have been given unrestricted or privileged access to company's IT assets</i>	Data Integrity <i>The risk of losing integrity of organization's data while at rest or in transit</i>	Negligence <i>The risk of employees or business partners acting wrongly due to ignorance or disregard (intentionally or unintentionally)</i>

Example Use Case

ensemble use case - phishing





Phishing attacks can be either user reported or auto-alerted through secure email gateways (SEG). Phishing attack data can be fused with threat intel, and user and entity behavior analytics (UEBA) logs to enrich and classify incidents by SOC analysts. The analyst resolutions will be used to train, test and re-train Splunk machine learning tool kit (MLTK) algorithms to auto-classify phishing alerts



Data sources

Multiple sources of data such as inbound emails, SEG logs, threat intelligence and user browsing histories are collected and indexed in Splunk ES to be used to build the phishing detection model

Fraudulent attempts to obtain sensitive information such as usernames, passwords and credit card details shall be segregated and compared against threat intel sources, and ingested into Splunk along with user behavior patterns for root cause analysis. Proxy logs are collected as well to identify if users clicked on the phishing URLs. The combination of these data sources will provide more context for the model to use to determine whether a URL may be part of a phishing campaign

Data source	Description	Fields to monitor
 User email data	Employee emails from external sender origins	Sender, Recipient, Email Body, Subject, Mail Server IP
 Point solution indicators	Effectively phished users	Proxy Action - Allowed/Blocked
 Behavioral indicators	Employee web browsing behaviors	Phishing URL, Username, Hostname, Target Domains
 Threat intel	Threat intelligence	Reputation against white lists, black lists

ensemble points of contact



Samir Hans
Principal
Deloitte & Touche LLP
shans@deloitte.com



Chris Knackstedt
Senior Manager
Deloitte & Touche LLP
cknackstedt@deloitte.com





This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.