Deloitte.

The comprehensive approach to security foresight

Security Intelligence Framework

July 2016

Shift from hindsight to foresight

Few modern business leaders can imagine running their business without the internet; it's been at the core of business innovation and disruption in recent decades. However, this global network was designed primarily for sharing information not protecting it. As a result, the internet is often the door that opens an organization's data to risk. And today, as companies extended their networks through vendors, partners, and contractors, controlling access to business data becomes increasingly difficult. Plus, with the explosive growth of structured and unstructured information, many organizations find the job of data protection overwhelming.

All these factors, and more, have the potential to collide and allow cyber criminals to steal personal information, customer records, and credit card information contained in databases in only a few short days; you probably read about similar high-profile breaches in the news (see case study, page 10). This scenario is an executive's nightmare — especially for CISOs who are responsible for data protection. Even though the company was certified as compliant with Payment Card Industry Data Security Standards (PCI DSS) and its malware detection technologies triggered alerts, the breach was undetected for weeks. This company is not alone; the number and complexity of cyber attacks continues to grow. How did this happen? More important, what steps can organizations take to help avoid a similar catastrophe?

To help clients address these questions, Deloitte researched and developed the Security Intelligence (SI) Framework, a comprehensive solution that delivers leading cyber-security practices for intelligence-driven organizations. As we've seen, technology and compliance with industry standards alone are not enough to protect organizations from cyber crimes. What's needed is an enterprise-wide, continuously evolving approach that brings together people, processes, and technology to build a secure, vigilant, and resilient organization.

Path to becoming an intelligence-driven organization

Gaps in traditional risk management systems

Many organizations today have a basic security infrastructure that incorporates traditional detection controls, threat reporting, and security event management (Figure 1). These devices are all necessary, but alone, they do not provide sufficient protection in today's high-risk environment. Here are some of the gaps in this traditional approach to business risk management:

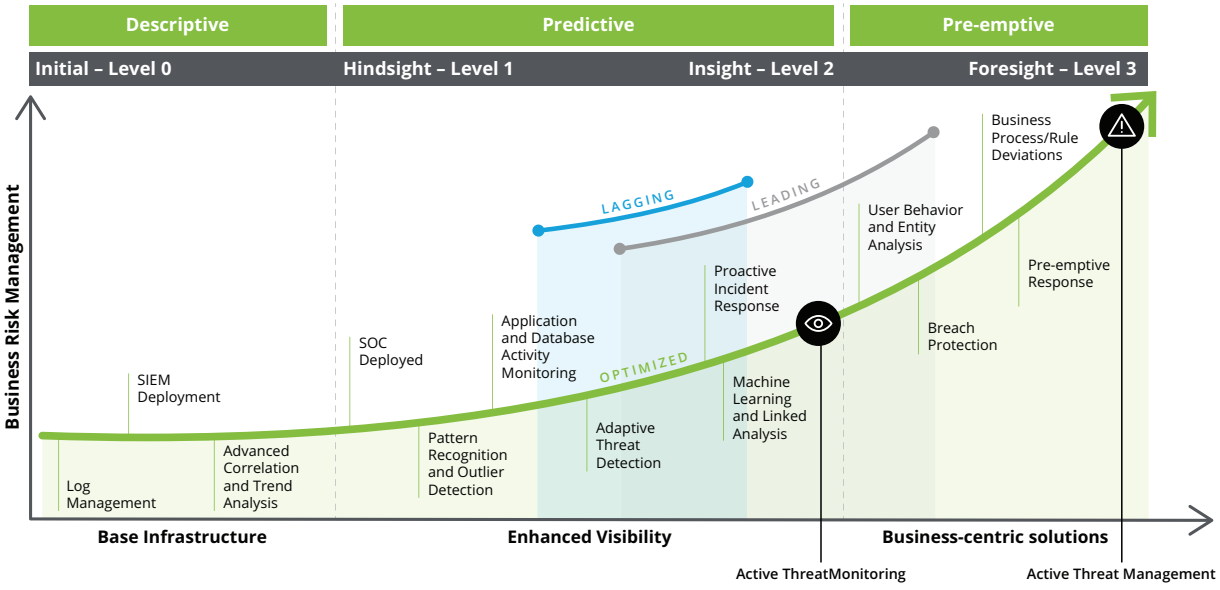
- **Lack of prioritization.** It's nearly impossible to protect and interpret the vast amounts of structured and unstructured data passing through organizations today, so it's important to identify data that are critical to business operations, financial strength, and reputation.
- **Ineffective triage and analysis.** In addition to protecting data, organizations also need to prioritize, interpret — and act on — clues that critical information could be at risk *before* a breach.
- **Lack of visibility.** When an event is identified, security analysts need a clear understanding of the traffic preceding and following to interpret the importance of the event. They also need to understand whether network or business processes can allow the breach to reach critical assets.
- **Assumption of false positive.** Without reliable technology, analysts tend to assume an alert is not real, or that it's not important.
- **Lack of alignment across the organization.** Unless business leaders are aligned and communicate the importance of protecting critical data, employees across the organization may be unlikely to follow processes that enhance data security.

Evolution from reactive to proactive risk management

As Figure 1 illustrates, many leading companies today are striving to attain mid-level maturity where threats are actively managed. These more mature security operations are centralized under a security operations center (SOC) that continually tracks activity, detects patterns and anomalies, and conducts statistical analysis that enables them to actively monitor threats. They have — or are developing — the capabilities needed to collect accurate, relevant, and timely information to determine threat trajectory — the sequence of activities that could exploit a weakness on a critical asset — *before* a data breach occurs.

However, few — if any — companies have become truly intelligence-driven organizations that effectively execute enterprise-wide, business-centric data protection solutions. To reach this level of maturity, security solutions must encompass people, processes, and technology to provide clear visibility across the organization's businesses and functions. These mature organizations are able to effectively detect, manage, and prevent data breaches to protect the organization's operations, financial stability, and brand reputation.

Figure 1: Security Intelligence and Operations Maturity Curve



Deloitte's approach to creating an intelligence-driven organization

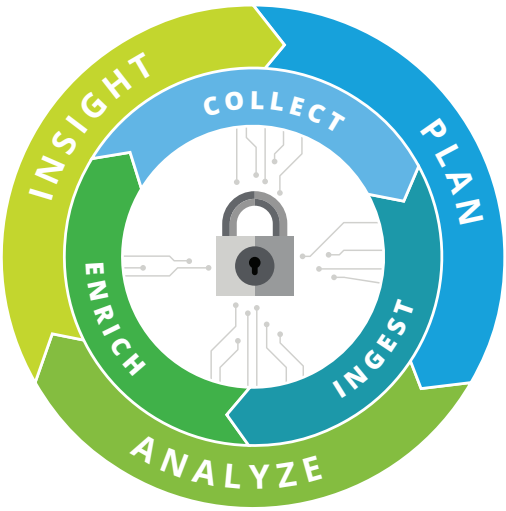
Overview of Deloitte's Security Intelligence Framework

Deloitte's Security Intelligence Framework helps companies systematically move up the risk management maturity curve. Our professionals work with company leaders in their efforts to enhance visibility and develop proactive, comprehensive business-centric solutions. We deliver the business, human capital, and technical experience and knowledge needed to help organizations align their people, business processes, and technologies to provide effective, continuously improving threat detection, monitoring, and management.

The SI Framework has six components: Deloitte professionals work with business leaders, Information Security (IS), and Information Technology (IT) to help them protect their data assets by ***planning, analyzing, and developing insights*** from massive amounts of security-relevant data (see Figure 2). We leverage IBM's Security portfolio of products, including IBM QRadar, an integrated security analytics platform, to ***collect, ingest, and enrich data*** to enable effective analysis and insights (see Figure 4 on page 5). Deloitte's SI Framework framework helps organizations proactively manage data security by delivering a metric-driven, continuous cycle of discovery, learning, and improvement.

Deloitte's SI Framework is an enterprise-wide approach to transforming raw security data into meaningful insights to track adversary actions throughout the entire attack chain, enabling organizations to anticipate threats and react faster and more effectively.

Figure 2: SI Framework



Security Intelligence Framework: Six key components

Plan. Deloitte works with the organization's stakeholders to develop an effective security intelligence plan. The plan identifies and prioritizes data and processes that are critical to business operations and reputation, which will be monitored by a Security Intelligence and Operations (SIO) team.

The plan provides detailed answers to intelligence requirements (IR) to document specific, observable facts, events, or activities that need to be monitored. For example:

- IR #1: What are the greatest threats facing the enterprise in FY16 Q1?
  - IR #1.2: Who are the likely threat actors?
  - IR #1.3: What tools, techniques, and practices are they likely to use?

The answers to these IR questions — and many more — are translated into collection plans that document specific indicators or signals that threat activity or potential threat activity may exist.

Collect. Deloitte works with the IS and IT teams to build out the collection plans that will be used to gather and organize raw information needed to meet each intelligence requirement. The collection phase focuses on security data management, preparation, and governance of the structured and unstructured data needed to satisfy the intelligence requirements. External data, such as global threat intelligence, may be added to provide deeper insights.

A collection plan for each IR is prepared that precisely describes the monitoring goals and objectives required for threat detection, along with documented procedures to manage reliable and repeatable data collection. Figure 3 is a description of the types of information that is documented for each IR collection plan.

Figure 3: Collection plan documentation

Property	Description
Identification number	Provides the unique identification number
Intelligence Requirement (IR)	Describes the monitoring goal (outcome)
Objective statement	Defines the measurable data (observables) needed to achieve the monitoring goal (outcome)
Indicator	Provides positive or negative indication of an observable
Collection resources	Identifies data sources or feeds required to monitor the IR
Essential elements of information	Defines data features (events, properties, or metadata) that must be collected for effective event classification
Detection logic/ signature	Defines the pattern classifier (pattern recognition and detection) used to discriminate between a "legitimate" and a "malicious" observable

Ingest. The massive amount of collected structured and unstructured data from a variety of sources is transferred into the ingestion pipeline for processing. Deloitte leverages the unified ingestion architecture and infrastructure components provided by IBM QRadar Security Intelligence Platform for integrating various security data. Collected data enters the ingestion engine through collection nodes, which enable low-latency transport and continuous uptime for sustained data ingestion and distribution.

Enrich. The enrichment process integrates the internal data stored in the collection nodes with external data feeds, such as threat data, vulnerability information, social and web data. Deloitte provides relevant feeds through subscription-based threat notifications and report. These data feeds enhance internal data with additional information that can transform ambiguous data into actionable information. The enrich phase helps discern real threats from false positives by:

- Applying threat models to adjust priorities
- Integrating diverse datasets to uncover hidden risks
- Providing a threat intelligence feedback loop so that only relevant threat intelligence information is retained

Analyze. The Deloitte SI Framework uses advanced analytics technologies to identify and rank potential threats to determine "what is happening" and "how is this happening," which can enable human security analysts to make more timely and accurate threat assessments. IBM QRadar Intelligence uses a variety of analytical methods — such as data mining, machine learning, and natural language processing — to detect deviations from regular patterns, uncover changes in network traffic, and find activities that exceed defined levels. Deloitte supplements QRadar's analytic capabilities by delivering tailored analytical applications that meet the organization's specific intelligence requirements.

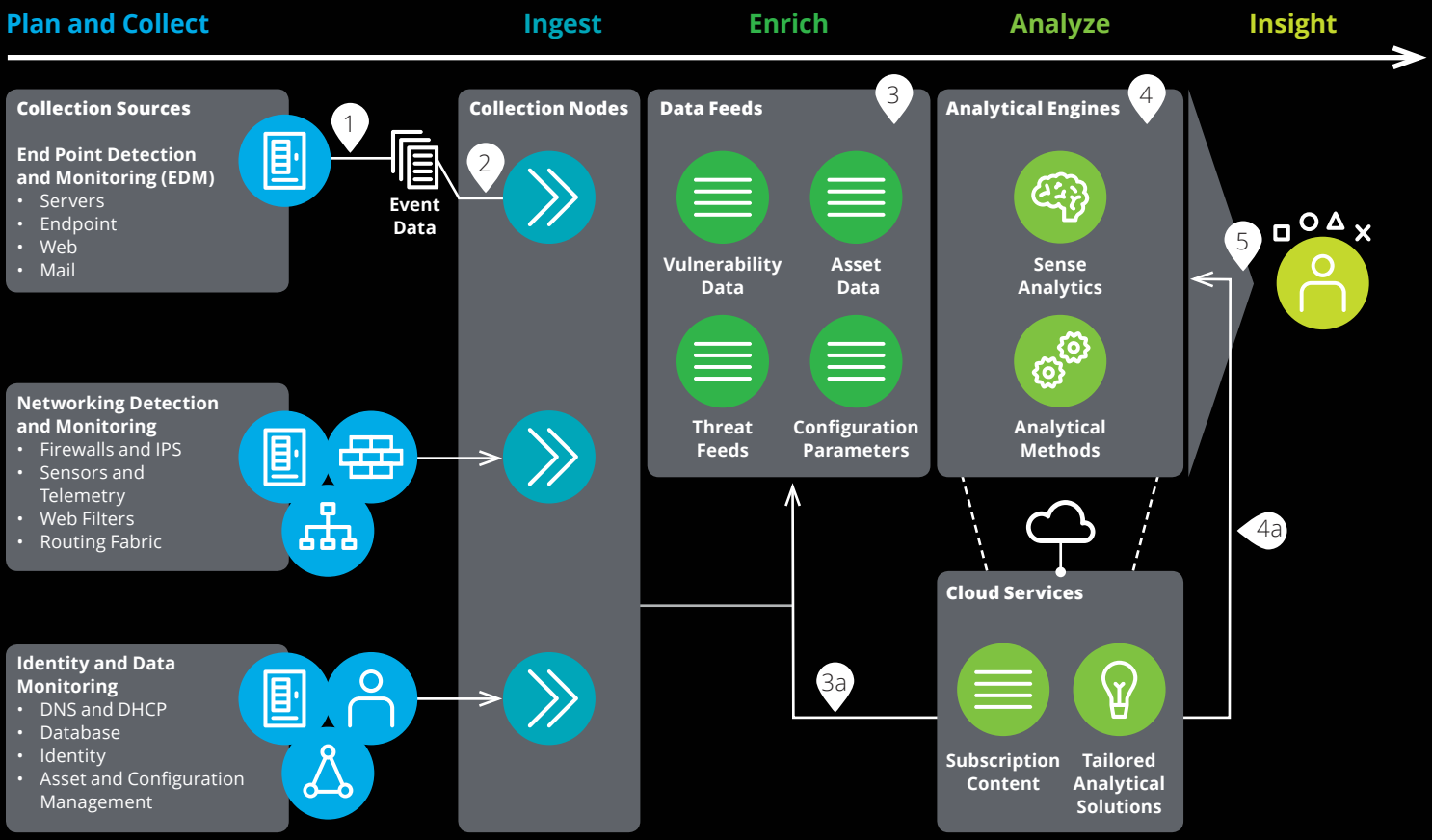
Insight. Curated insights from the analyzed data are distributed to security analysts and other users through customized security content. Deloitte has invested significant resources in diagnosing, evaluating, and converting information into action. Deloitte will bring technology accelerators designed to enhance threat detection and security monitoring quickly. These technology accelerators can help our clients answer the following questions:

- What is the impact of the threat?
- Has a breach occurred, if so is it still occurring?
- Can this vulnerability happen again?
- Who is the threat actor/adversary behind the event?
- What sensitive information or systems were comprised?
- Who do we need to inform?
- What do we do next?

This knowledge (insight) helps reduce the time needed for faster course of action to be taken.

Figure 4: The Deloitte SI Framework: From data to insight

The SI Framework enables organizations to gain the visibility needed to more quickly identify and respond to breaches and security incidents. By analyzing and enriching data with reliable threat intelligence and other contextual information, the SI Framework enables users to more rapidly detect and respond to variations from normal behavior. The graphic below illustrates the SI Framework data flow.



1 During the Plan and Collect phases collection sources are curated enabling the visibility needed to detect abnormalities in users' actions via event data (ex. server, security, or audit)

2 High-capacity Collection Nodes ingest unstructured/ semi-structured event data, from a variety of collection sources, detection and monitoring (surveillance) tools in conjunction with telemetry traffic flow

3 Collected data is integrated with vulnerability integration (scanned data), and threat subscription feeds (atomic indicators, research reports) from providers along with configuration and asset details to enrich events with contextual information

3a Cloud Services enable the discovery of complementary technology extending the value of security investments thereby improving integrations and data sharing with IBM and partner supplied apps and extensions

4 Real-time correlation and analysis of enriched data sets using advanced analytical methods and purpose-built data repositories, allowing for earlier and more accurate detection of advanced threats, and helping to distinguish the signal from the noise

4a Tailored analytical applications are delivered through subscription services that improved existing methods, such as:

- **Analytical Methods:** Data mining, machine learning, advanced statistical analysis techniques, supervised
- **Anomaly Detection:** Baseline current activity and identify meaningful deviations and uncover trends

5 Analyzed data is distributed to end-users for rapid consumption, to help organizations reduce the time to identify and respond to security incidents; insights give analysts an understanding of alerts, behaviors, and potential threats, and executives an understanding of the organization's overall security posture

How we can help

Deloitte is recognized as a leader 'with exceptional client feedback' in information security consulting services.

Forrester Research, Inc., The Forrester Wave: Information Security Consulting Services, Q1 2013

Our capabilities fall within Deloitte's "secure, vigilant, resilient" services structure. Being secure means having risk-prioritized controls to defend against known and emerging threats. Remaining vigilant means leveraging threat intelligence and situational awareness to identify harmful behavior. Being resilient means the ability to recover from, and minimize the impact of, cyber incidents. Across the three pillars, a strong strategy and governance capability enables the organization to enhance resources while protecting the environment.

A sound cyber risk program is an integral element of business success. While security is more important than ever, we emphasize the need to be constantly vigilant and resilient in the face of shifting cyber threats. We understand the current threat landscape and develop strategies to help clients manage cyber risks that are in line with business risk priorities. Our services are designed to help you better prioritize program investments, improve threat awareness and visibility, and be more resilient in the face of cyber incidents. Leveraging our SI Framework, which is built on industry-leading practices, we help our clients gain insights from past cyber incidents for greater visibility and awareness.

Potential bottom-line benefits

- **Business risk management enhancement.** Deloitte's SI Framework helps organizations move from reactive to predictive security capabilities by delivering a codified operating model for enhancing security intelligence and reducing risk of attack damage. The table on page 8 outlines professional services offered by Deloitte to help your organization move from a reactive to a predictive approach to cyber risk management.
- **Choice of house or managed delivery options.** We can help organizations leverage the SI Framework by adapting or enhancing the organization's existing security operations. Deloitte also offers a managed security intelligence service that's tailored to your organization's needs.
- **Full range of security intelligence consulting services.** We can help you develop the security intelligence approach that's right for your organization:
  - Assist with **attack surface identification and threat modeling simulation** activities to provide insights on vulnerabilities that are most likely to be exploited by either external or internal threat actors.
  - Advice on how to **augment existing intelligence capabilities.** This includes providing vendor assessments of threat intelligence vendors and the associated technologies.

Figure 5: Deloitte's Secure.Vigilant.Resilient.™ services structure

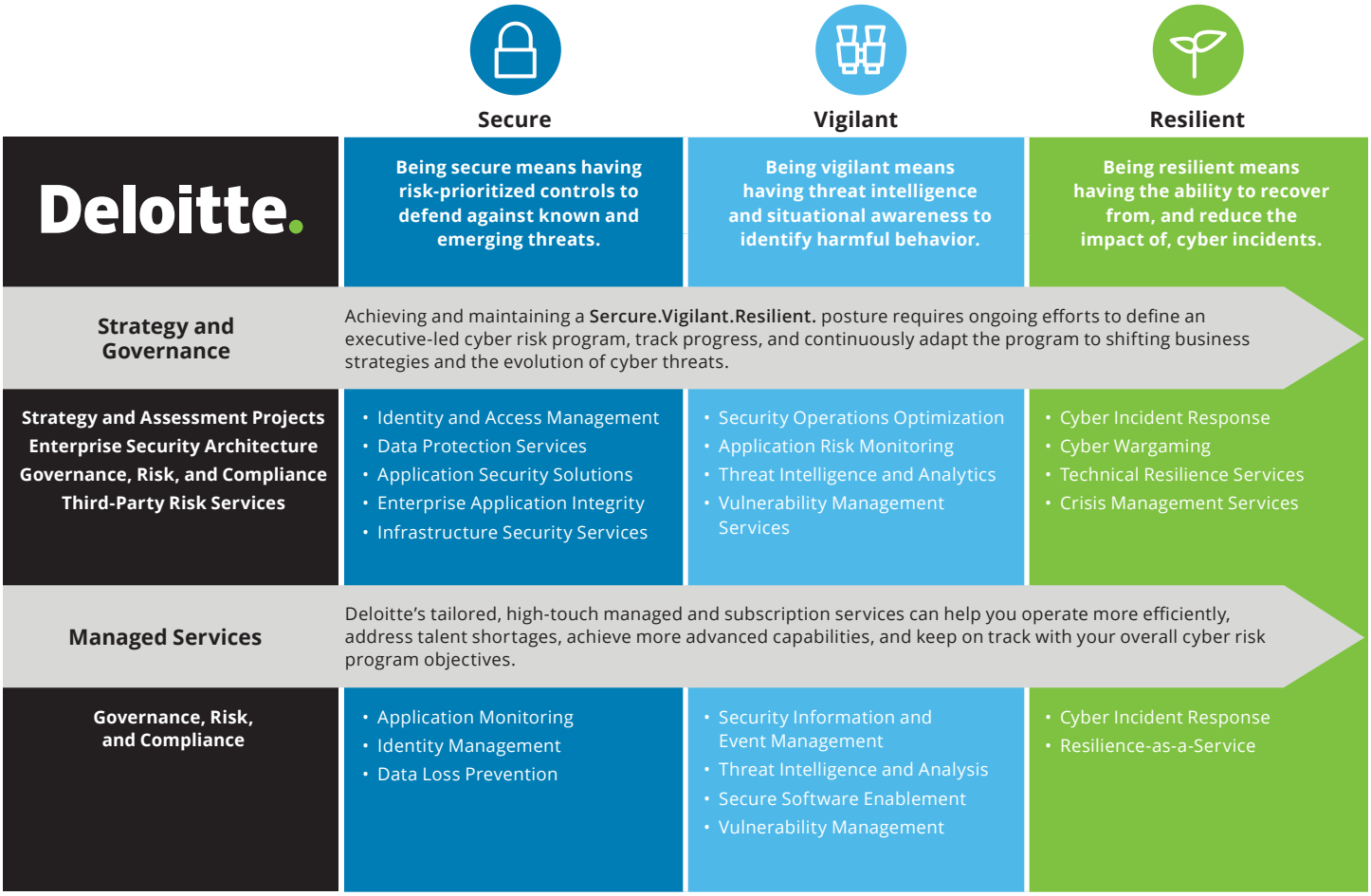


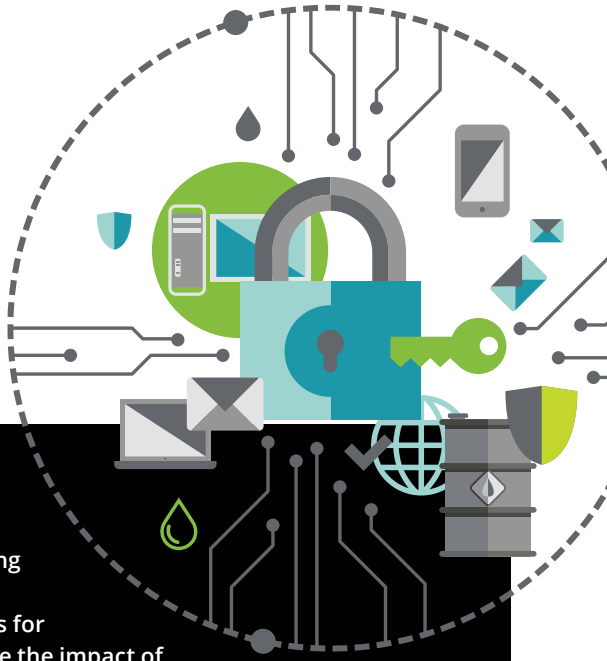
Figure 6: Deloitte SI Framework: Professional service offerings

Phase	Description	Deliverables
Plan	Deloitte professionals work with key stakeholders to conduct a ***Security Intelligence Capability Review*** that informs the overall security strategy and provides a transformational roadmap: • Obtain requirements from stakeholders • Identify intelligence needs and gaps • Formulate collection, processing, analysis, and dissemination requirements Deloitte leverages its extensive Intelligence Requirements Library containing hundreds of IR's across most major industries.	• Security Intelligence Readiness Report (SIRR) • Cyber Threat Landscape Profiles and Attack Surface Identification • Intelligence Capability Assessment • Intelligence Requirements Accelerator Packs
Collect	Deloitte informs and guides the build out of security and threat intelligence collection plans: • Define the organization's specific needs and objectives • Gather and organize raw information needed to produce finished intelligence. • Utilize full-spectrum collection capabilities across multiple domains	• Collection management and plans: – Advanced use-case development – Threat playbook development
Ingest	Deloitte professionals work closely with clients on-site to assess, enhance, and implement intelligence capabilities and technology solutions to build an integrated security intelligence architecture and infrastructure capable of ingesting, enriching, and analyzing security data volumes at scale.	• Technology selection • Architecture planning and solution enablement • Automation and orchestration development
Enrich	Deloitte provides technology accelerators to enrich data required to meet intelligence requirements by delivering subscription-based threat data feeds and reports, including: • Proprietary threat research derived from our global intelligence collections infrastructure to provide clients with strategic and actionable insights, packaged as threat reports • Content Acceleration Packs (CAPs), which are specific indicator feeds curated from our proprietary threat research content implemented on QRadar SIEM platforms to detect emerging threats	• Proprietary threat research • Content Acceleration Packs (CAPs)
Analyze	Deloitte professionals provide tailored security intelligence and analytic methods to help meet the organization's intelligence requirements and strategic goals. If needed, we can also provide dedicated threat analyst security and threat analyst augment services that provide direct access to an assigned TIA analyst for custom threat research, malware analysis, or other investigations.	• Analytical methods: – Risk Analytics – Threat Analytics – Behavior Analytics – Cognitive • Intelligence staff augmentation: – Dedicated on-call threat analyst – Staff augmentation – Cyber hunting services
Insight	In the event of a security incident, Deloitte can provide Rapid Deployment Incident (CSIRT) response research and investigation teams.	• Specific courses of action for threat mitigation • Incident Response Runbooks and Playbooks

Managed Threat Services (MTS)

Deloitte's Managed Threat Services professionals have extensive intelligence experience and knowledge of industry-specific trends from law enforcement, government, military, and cyber intelligence companies. Some of the benefits of our MTS offerings include:

- **Lower operational total cost of ownership (TCO).** Shifts capital asset costs to operating expenses.
- **Increased efficiency.** Redirect scarce security expertise to more strategic activities.
- **Greater access to threat data.** Tap into insights provided by Deloitte's strategic alliances, which enable Deloitte to analyze threat data across numerous sources of information — including dark web, criminal forums, third-party intelligence, and other sources that may provide specific insight into existing and emerging business risks.



A new era of advanced security platforms

Sifting through security-related data to find irregularities is a slow, time-consuming effort for humans — time that's better spent interpreting and acting on findings. IBM is at the leading edge of developing new machine-assisted analytical methods for the enterprise, which will accelerate the discovery of unknown threats to minimize the impact of a cyber attack.

- IBM QRadar Security Intelligence Platform with its Sense Analytics engine helps defend against attacks by applying sophisticated analytics to identify high-priority incidents that might otherwise get lost in the noise. It infuses raw data with historical and real-time context using Sense Analytics to highlight potential threats. By leveraging its threat-sensing capabilities, the platform significantly improves detection rates by rapidly sifting through the mass of data to quickly identify "true positives" with evidentiary support for forensic investigations.
- IBM Watson for Cyber Security uses cognitive computing (including natural language processing and machine learning) to analyze anomalous activities across different vectors to pinpoint attacks before sensitive data can reached. IBM is training this new generation of cognitive systems to understand, reason, and learn about constantly evolving security threats. They are beginning to build security instincts and expertise into new defenses that analyze research reports, web text and threat data — just like security professionals do every day — but with unprecedented speed and scale.

Key benefits:

- Reduces investigative time needed to determine the root cause of an incident
- Helps security analysts accurately remediate threats with minimal business disruption

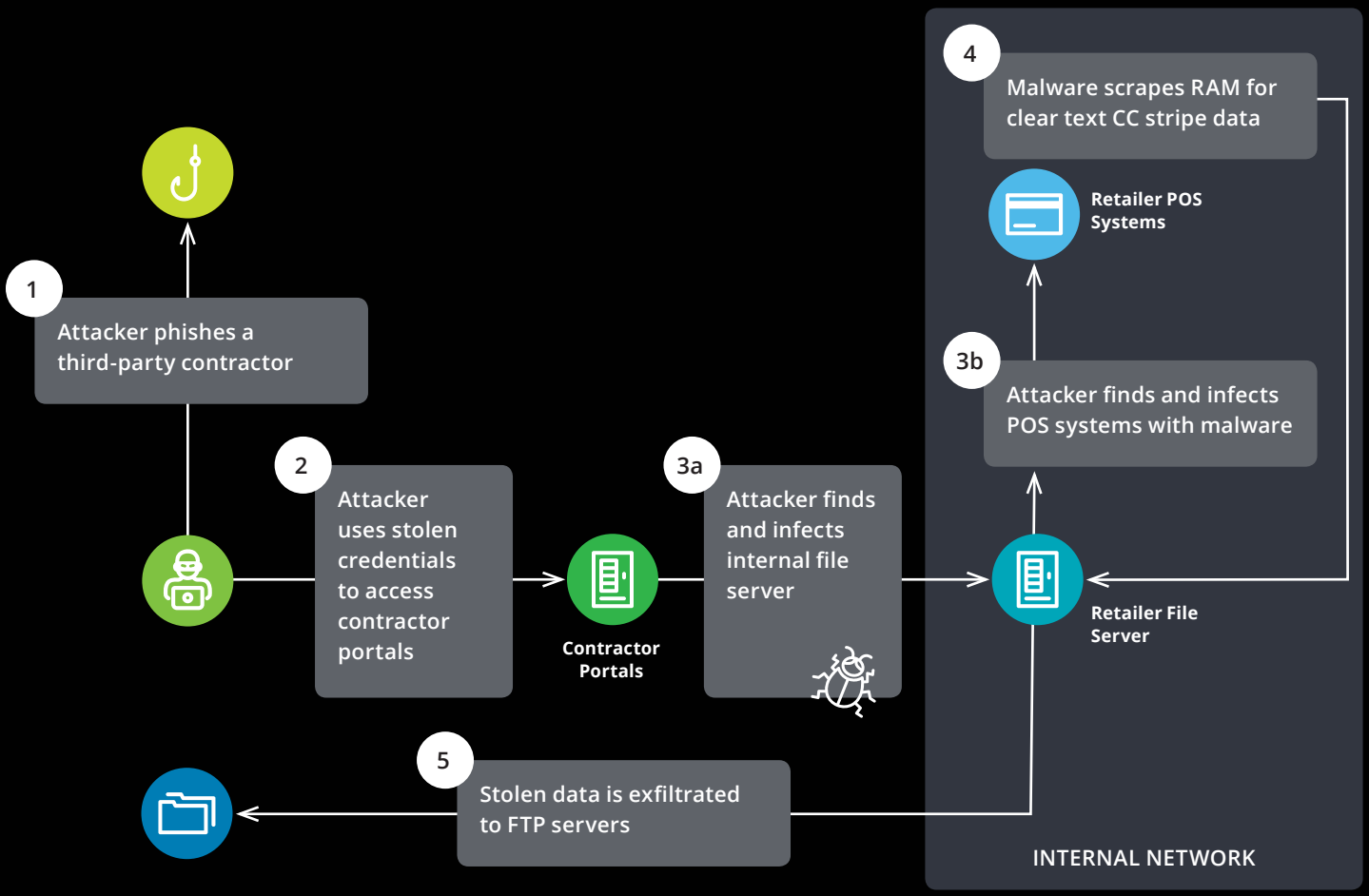
Case example: The need for speed

The 2016 Cost of Data Breach Study[1] indicates that the average total cost paid for each lost or stolen record containing sensitive or confidential information increased from $154 in 2015 to $158 the 2016 study. Additionally, the time to identify and time to contain was higher, taking 229 and 82 days, respectively.

The illustration below captures a potential event that could lead up to the theft of millions of customer records from a retailer's credit card databases over 19 days. In this example, the attacker's malware (malicious software) affected 30% of stores, with a total of approximately 1M credit and debit transactions per day. As the time lapse between detection and defense increases, a retailer is likely to result in significantly greater estimated financial loss:

- **Detection at Day 0** — Minimal impact, remediation effective. Financial impact estimated $10k
- **Detection at Day 2** — 600k cards compromised, identity protection service and remediation costs, estimated $2M to $5M
- **Detection at Day 19** — Estimated 19 million credit and debit cards stolen, 40 million records
- **Detection at Day 30** — Losses could disrupt the business, infection expanded and remediation cost uncontained. Identity protection service and remediation costs estimated $23M+

Figure 7: Detect attacks disguised as normal activity



[1] https://www-03.ibm.com/security/data-breach/

Deloitte and IBM Alliance

For more than 15 years, Deloitte and IBM have formally partnered. With smarter teaming, Deloitte and IBM collaborate when it is advantageous to our joint clients.

Benefits

- **Dedicated alliance team** — Leveraging a dedicated team, we can accelerate the development and delivery of services and solutions.
- **Access to key IBM resources** — Deloitte is a Premier Business Partner with access to software, subject matter specialists, education, and tools.

Accolades

- IBM Global Innovation Award for QRadar Security Operations Center (SOC) 2016
- Winner of IBM's 2015 Security Systems' Vertical Solution Innovation Award
- IBM's highest alliance distinction, the Global Alliance Excellence Award for Business Analytics

Let's talk

If you're concerned about your organization's ability to quickly detect and contain a cyber threat to your business, we should talk. We're helping some of the world's leading institutions bring together people, processes, and technology to build more secure, vigilant, and resilient organizations.

Daniel Poliquin
Principal | Deloitte Advisory
Cyber Risk Services
Deloitte & Touche LLP
+1 312 486 5627
dpoliquin@deloitte.com

Randy Parrow
Specialist Master | Deloitte Advisory
Deloitte & Touche LLP
+1 773 241 4467
rparrow@deloitte.com

Isaac Kohn
Senior Manager | Deloitte Advisory
Deloitte & Touch LLP
+1.201.499.0564
ikohn@deloitte.com

Jerry Jarvis
Sales Executive, Eastern US
Deloitte Services LP
+1 214 263 5480
jjarvis@deloitte.com

Bill Cox
Sales Executive, Western US
Deloitte Services LP
+1 630 215 6763
wicox@deloitte.com

Gillian Dokken
Alliance Manager
Deloitte Consulting LLP
+1 303 249 2339
gdokken@deloitte.com

Deloitte.