Enterprise Defense at the Speed of Data

Defending today's global organizations is at the mercy of how quickly and efficiently you can turn data into intelligence and make informed decisions.

By: Stephanie Gruber, *Senior Director, CIO Office, SAP*
Kevin D. Heckel, *Managing Director, Deloitte & Touche LLP*
Adam Vincent, *CEO, ThreatConnect*

Table of Contents

SAP NS2 | THREAT CONNECT | Deloitte.

Executive Summary

Today's threats are relentless. While the internet has enabled a global economy to explode, it has also made it easier than ever to access and steal data through connected systems. The internet was built for connectivity, not security. And, as IT systems become more complex, the associated risks continue to increase.

Cyber threat actors are gaining more sophisticated tools, techniques and procedures (TTPs) which are outpacing stand-alone security solutions. It is not surprising they are able get past disparate and uncoordinated defenses. These incursions are not conducted as isolated attempts. They are often multi-year campaigns targeting valuable, sensitive data.

As you can imagine, these attacks have many business implications — brand reputation, lost revenue, etc. Some of the more infamous breaches in recent years had serious impacts. The most notable in the last two years touched retail, government, healthcare, and even political campaigns. But, it doesn't end there. Less known breaches have compromised intellectual property, large contracts, customer lists and any of several other assets. Network World wrote in 2016, "The average cost of a data breach involving fewer than 10,000 records was $5 million."[1]

How do companies protect themselves? In this paper, we discuss how an intelligence-driven security program gives your company or agency a fighting chance to stay ahead of ever-changing threats. It provides a holistic view of the threat landscape, insight into what is relevant to you, and a proactive posture to protect your institution.

Cybersecurity must evolve into a platform-based, intelligence-driven approach to identify, manage and blocks threats faster to effectively manage cyber risk. Every organization will need to centrally compile their threat data, analyze it to determine what threats are most relevant, and then automate their security processes. For many global organizations, an in-memory computing platform will be necessary to process the volumes of data at a speed as fast as adversaries operate.

---

1 http://www.networkworld.com/article/3135522/security/how-much-does-a-data-breach-actually-cost.html

Your Security Risk: Growing in Size and Complexity

The Detection Deficit

The detection deficit gap — the time it takes from when an adversary compromises a system to when it is discovered — isn't closing, it's getting wider.

In 2016, Verizon issued its annual Data Breach Investigations Report (DBIR),[2] a collection of real-world breaches and information security incidents from the prior year. The results for security teams were grim. Threat actors are getting better, faster and more efficient at compromising networks — not only yours but those of your partners and providers — taking only minutes or less to infiltrate systems. Then, it typically takes an organization months or more to discover the intrusions.

Business Applications are No Longer Behind Closed Doors

The focus of traditional IT security teams has been securing networks and communications. They relied on security information and event management (SIEM) solutions to monitor their landscapes and evaluate logs for performance. They concentrated primarily on perimeter protection, malware analysis and network communication. Then, business demands forced them to open their systems which has introduced new threats not covered by those methods.

Take for example, Business Applications. IT security teams recognized they could no longer stay behind four walls due to business needs for connectivity with trusted partners and customers, Internet of Things (IoT) sensor data and cloud solutions. Attacks on Business Applications can result in financial loss, loss of brand reputation, loss of intellectual property (IP) and violation of regulatory requirements, as well as significantly impact strategic goals.

2 Verizon 2016 Data Breach Investigations Report, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

Why Traditional Cybersecurity is Failing

Volume of Data is Increasing Risk

In a 2016 ESG report, 46% of organizations claim to have a problematic shortage of cyber security skills, which is an 18% increase from 2015.[3] It's not surprising then that the sheer volume and variety of threat data, and the velocity at which it pours in can be overwhelming. In fact, 80% of organizations that receive more than 500 critical alerts per day investigate less than 1% of them.[4]

With so much available information, threats can slip through the cracks.

Fragmentation

Throughout an enterprise, there are security personnel using a variety of processes and tools to conduct their incident response, network defense, and threat and risk analysis. These various tools and teams are often disconnected and don't communicate with each other. Fragmented internal systems and people can prevent teams from being effective, even if the team has the capability to resolve the threat.

The lack of documented, automated processes is one large contributor to why cybersecurity is failing. A recent SANS survey of hundreds of cybersecurity and IT administration professionals cites, "Because [only] 20% of respondents have their data 50% automated across security and risk management pillars, expansion of automation and integration represents a big area for improvement."[5]

Further, a 2015 survey by *Dark Reading and Information Week*[6] found that the biggest challenge faced by security teams was not preventing data breaches from outside attackers, but managing the complexity of security itself. In other words, dealing with the outcome of fragmentation is more difficult than managing threats.

---

3 ESG Research Report, 2016 IT Spending Intentions Survey, February 2016

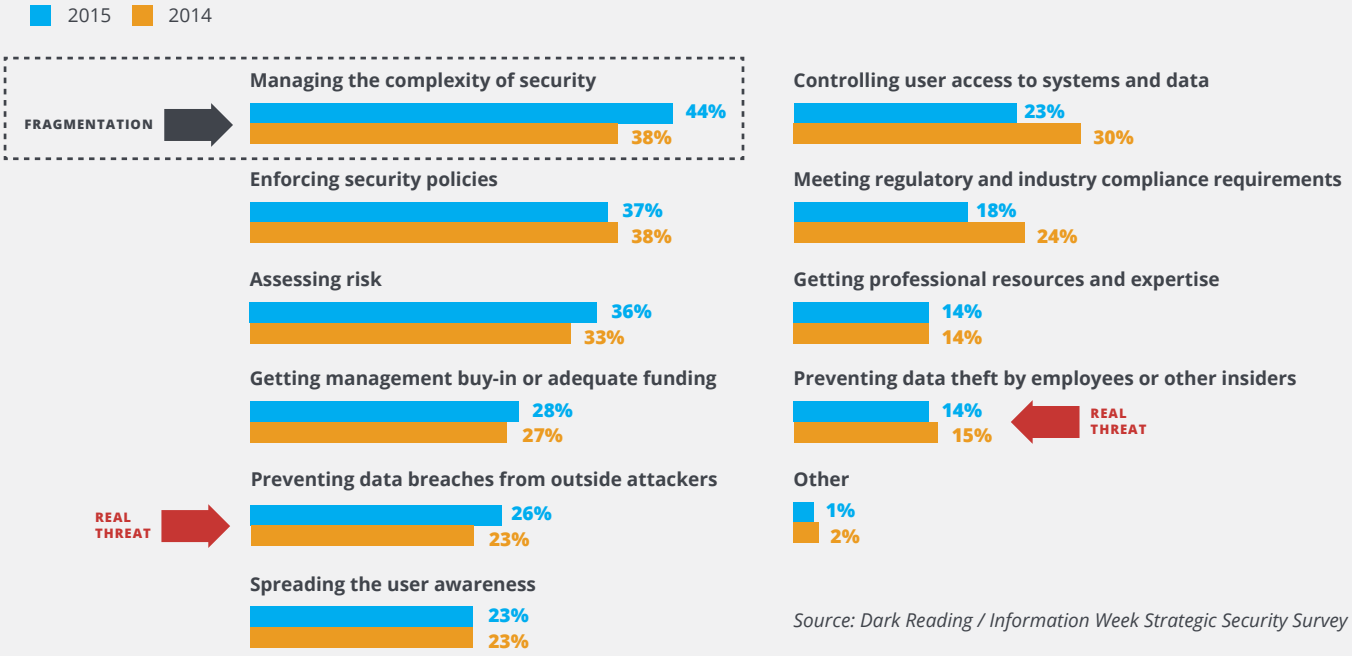
4 http://www.infosecurity-magazine.com/news/less-than-1-of-severe-critical/2016

5 Integrating Prevention, Detection and ResponseWorkflows: SANS Survey on Security Optimization, published April 2017: https://www.sans.org/reading-room/whitepapers/analyst/integrating-prevention-detection-response-work-ows-survey-security-optimization-37730

6 2015 Strategic Security Survey http://reports.informationweek.com/abstract/21/12549/Security/2015-Strategic-Security-Survey.html

Biggest IT Security Challenges

Which of the following are among the biggest information or network security challenges facing your company?



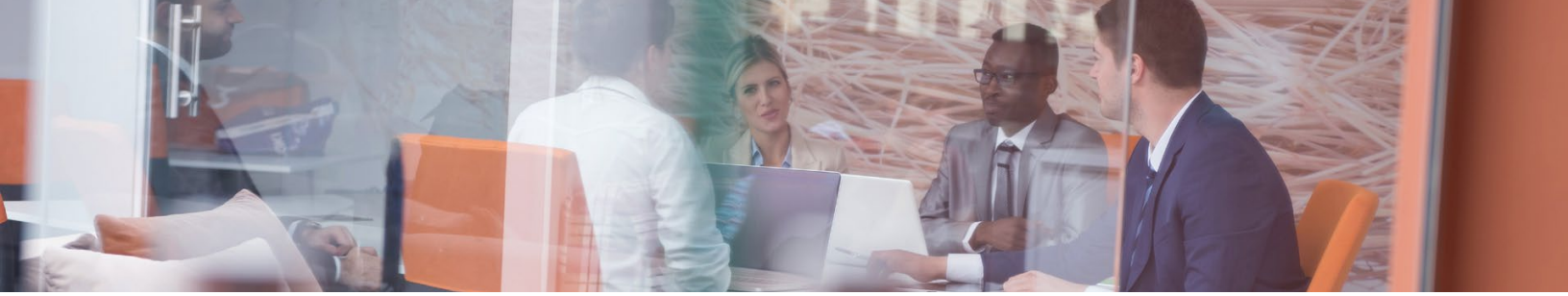
Source: Dark Reading / Information Week Strategic Security Survey

Design Your Architecture to Increase Efficiency & Reduce Complexity

Security Operations Centers (SOCs) historically have taken a control-based approach — focusing on regulatory compliance and change management. It is characterized by its reactive stance — monitoring and acting post event which only addresses historical knowledge of threats. It does not address the rapidly evolving threats to the organization — strategically or tactically. It has become apparent that a new approach and new technology is needed for the SOC to evolve faster than the threats it addresses.

> **Security operations centers (SOCs) must be architected for intelligence, embracing an adaptive security architecture to become context-aware and intelligence-driven. Security leaders should understand how intelligence-driven SOCs use tools, processes and strategies to protect against modern threats.[7]**
>
> – OLIVER ROCHFORD AND NEIL MACDONALD, GARTNER

7 Five Characteristics of an Intelligence-Driven Security Operations Center, Garter, November 2015 - Gartner ID: G00271231



Think of it simply: How can you know what action to take — strategically or tactically — without intelligence?

The Five Key Factors for Efficient Security Operations

Gartner suggests that organizations must employ these five characteristics to have an Intelligence-Driven SOC:

- Use multi-sourced threat intelligence strategically and tactically;
- Use advanced analytics to operationalize security intelligence;
- Automate whenever feasible;
- Adopt an adaptive security architecture;
- And proactively hunt and investigate.[7]

We would take Gartner's position one step further and recommend you architect your security operations with these key factors in mind:

1. Workflows, Automation, and Orchestration

Workflows in an intelligence-driven SOC means more than bringing in a ticketing system. Human capital in security is at an extreme deficit, so SOC automation is necessary to focus your team and their collective skills on the highest priority tasks is crucial. Automation can come in many forms from filtering indicators against data to pushing rules to the firewall for execution. It is a built in capability in many security tools at a micro-level these days, but it may have its greatest value when leveraged as part of a security incident response platform (SIRP), threat intelligence platform (TIP) or security operations and analytics platform.

Orchestration takes automation one step further by connecting existing security tools and driving automation across them by incorporating human intervention as needed. With orchestration, you may use knowledge and data to complete analysis and either react (given high confidence in the data), re-process (get more data), or present a choice to an analyst.

2. Tribal Knowledge

Getting your entire team to work together in one platform is a key component of an intelligence-driven SOC, but it goes further than that. Your organization should participate in communities — both public (e.g., Information Sharing and Analysis Centers or ISACs) or private (e.g., your supply chain partners) — through a platform to capture peers' knowledge of threats, actors, motivations, and how they were addressed effectively.

7 Five Characteristics of an Intelligence-Driven Security Operations Center, Garter, November 2015 - Gartner ID: G00271231

3. In-Platform Analytics

Analyzing data should not be an afterthought or secondary system to your security operations. Analytics are critical to informing strategic management decisions such as what security investments to make next or what risks may be in an acquisition target. In an intelligence-driven SOC, having analytics delivered in the same system in which your team works enables tactical decision-making at the front lines of your defense.

4. Methodology for Intelligence Creation

Threat Intelligence is not something you can simply buy and plug into your system. It is a constant process of analyzing data and turning it into relevant intelligence. An intelligence-driven SOC is built on a platform with threat analysis capabilities and tools inherent in the system. Plus, it must follow an accepted standard for creating threat intelligence. For example, the Department of Defense's Diamond Model of Intrusion Analysis.

5. Reporting

An intelligence-driven SOC should produce reporting that is valuable to the organization both inside and outside of the security team. As mentioned in the In-Platform Analytics section above, intelligence may be produced that has value not just for tactical defense — e.g., blocking an IP at the firewall — but also strategic decision making — e.g., risk associated with a new channel partner. There should be established reporting procedures for the SOC across the organization.

Choosing the Right Platform to Increase Speed

Organizations are clearly feeling the pressure and pain of not having the necessary information in a timely, usable manner.

> **In an IDC survey of security executives, 74% of respondents surveyed stated that they were extremely or very interested in more advanced security analytics capable of aggregating technical events into a single platform to speed decision making.[8]**

As stated earlier in this paper, a common complaint in closing the gap between detection and response, not to mention proactively hunting threats, is the vast amounts of data that must be analyzed, scrutinized, and used. This is especially true for large government agencies and global organizations that must aggregate and analyze not only their own data, but also threat data from other sources — open source, threat intelligence providers, partners, etc.

Historically, databases were created to either process transactions quickly or conduct analytics quickly. For example, an airline needs a database that can handle the data entry of thousands of ticket agents around the globe at one time. That is called Online Transaction Processing (OLTP). Whereas an insurance company needs a database that can crunch large amounts of data through algorithms that calculate risk. That's called Online Analytical Processing (OLAP).

8 IDC Future of Security Survey, sponsored by SAP, May 2016

To close the detection gap and better manage cyber risk, cybersecurity teams must capture, process, and analyze exponentially increasing threat data all in one platform. An In-Memory computing platform should be able to handle consuming (OLTP) and analyzing (OLAP) vast amounts of data in many different formats at the same time, in real-time.

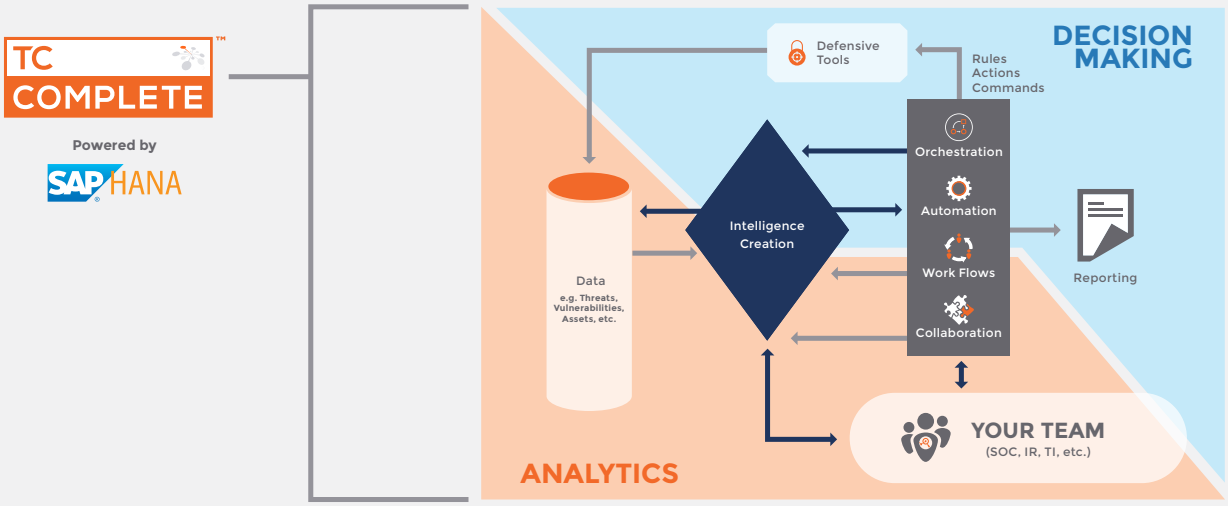
ThreatConnect's TC Complete — Powered by SAP HANA®

A Security Operations & Analytics Platform Built on an In-Memory Computing Platform

The ThreatConnect Platform, the first and industry-leading security operations and analytics platform, empowers you to find cyber threats, evaluate risk and mitigate harm to an organization. It is specifically designed to empower an intelligence-driven security program and mitigate threats faster using intelligence. At ThreatConnect, customers are processing millions of indicators daily and the number is steadily growing.

The latest edition of ThreatConnect's Platform, called TC Complete™, is available powered by the SAP HANA® platform. In product testing at ThreatConnect, TC Complete powered by SAP HANA has proven to be 54 times faster than prior versions on ThreatConnect not powered by SAP HANA. The advanced platform speaks directly to the need to process both transactions (OLTP) and analytics (OLAP) in one place — at the speed of the adversary — to close the detection gap.

As highlighted above one of the most challenging roadblocks to threat intelligence is not having a platform that can adapt to the quantity of data and at the same time being able to perform analytical processing. The in-memory platform of SAP HANA combines a database that complies with the standards for atomicity, consistency, isolation, and durability (ACID) with advanced analytical processing, application development and flexible data integrations. The massively parallel, in-memory paradigm underlying SAP HANA speeds information processing by a quantum leap. This architecture converges online transaction processing (OLTP) and online analytical processing (OLAP) operations on a single data copy in one in-memory, column-based data store. SAP HANA, in short, eliminates data redundancy, disk latency, and data movement among applications and analytical tools. It is the optimal platform for building and deploying next-generation, real-time applications and predictive analytics across the enterprise.



This illustrates how intelligence flows through every aspect of your security program; that your entire team is connected to the intelligence, each other, and the tools; and that a feedback loop from the people and tools is built-in to improve the intelligence. And, throughout the entire process, analytics are constantly enabling sound, fast decision-making.

Real-World Use Case

The following user story is based on real-world data from organizations across multiple industries, but for obvious reasons of confidentiality, the information has been presented as an example use case rather than a customer success story:

Using TC Complete to Analyze >250,000 Threats per Day

As the most obvious target for cyber attackers, a financial institution may observe up to 250,000 potential indicators of threats each day. Often their internal threat response teams do not have a central place to keep track of their tasks and data. Each team member can have multiple windows open and multiple places that he or she stores their data. In addition, they can't properly analyze malware that was attempting to attack their network, because their filters and firewalls were so stringent; everything was being blocked. As a result, the organization's threat response team was not able to capture or analyze the malware, unable to study potential attacks on their network, learn from them for future reference, nor build a knowledge base. Using ThreatConnect, the team established uniform procedures and integrated them into their SIEM, making the data more powerful and strengthening the company's entire security infrastructure.

In addition, simply ingesting observations into a database is not enough. They must be analyzed to prioritize the most immediate threats, as well as look for patterns that can be leveraged for future strategic planning. Adding context based on historical knowledge or external intelligence without orchestration and an in-memory computing platform would take up to 2 minutes per indicator totalling about eight thousand hours (or, just under one year). Clearly, that is not viable. That same data processed with TC Complete powered by SAP HANA could be handled within the day. Now, all the aggregated observations must still be analyzed for strategic insights, which also could be done faster with orchestration and in-memory computing.

That is just one example of how a solution like TC Complete powered by SAP HANA can change the face of security.

Conclusion

As we mentioned earlier, in the IDC survey when asked about future security offerings, an overwhelming majority of security executives wanted more advanced security analytics capable of aggregating technical events into a single platform to speed decision making. TC Complete powered by SAP HANA is that offering. Even better, it also provides the mechanism (orchestration) to speed action on those intelligence-driven decisions. It is time to close the detection deficit once and for all.

Get More Information

www.threatconnect.com/tc-complete
www.sap.com/products/technology-platforms.html
www.sapns2.com/solutions/sap-hana

ABOUT SAP & SAP NS2

As the market leader in enterprise application software, SAP is at the center of today's business and technology revolution. SAP helps you streamline your processes, giving you the ability to use live data to predict customer trends – live and in the moment. Across your entire business. When you run live, you Run Simple with SAP. At SAP National Security Services, Inc. (SAP NS2®), we are driven to defend. We provide innovative computing, analytics, and cloud solutions that accelerate the pace of data fusion, analysis and action. Our solutions help leaders better manage the business of the mission from the back office to the battlefield, delivering a critical offset over the adversary. As an independent subsidiary of SAP, we're backed by game changing technology, staffed by 100% U.S. citizens on U.S. soil, dedicated to meeting the unique mission requirements of U.S. national security organizations.

ABOUT THREATCONNECT

ThreatConnect, Inc.® unites cybersecurity people, processes and technologies behind a cohesive intelligence-driven defense. Built for security teams at all maturity levels, the ThreatConnect platform enables organizations to benefit from their collective knowledge and talents; develop security processes; and leverage their existing technologies to identify, protect and respond to threats in a measurable way. More than 1,200 companies and agencies worldwide use ThreatConnect to maximize the value of their security technology investments, combat the fragmentation of their security organizations, and enhance their infrastructure with relevant threat intelligence. To register for a free ThreatConnect account or learn more, visit **www.threatconnect.com.**

ABOUT DELOITTE

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see **www.deloitte.com/about** to learn more about our global network of member firms.