Course5
Transformative intelligence

Course5 Threat Intelligence Report

Threat Intelligence: Immunizing the Organization against Cybercrime

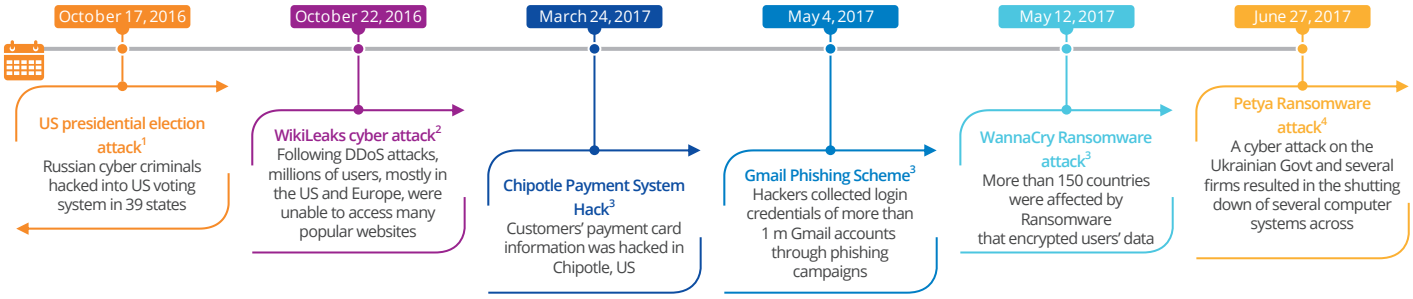
November 2017

Table of contents

Course5
Transformative intelligence

Growing cyber attacks: Worldwide scenario

Major attacks over the recent months...



Users

In 2016, someone's identity was stolen every 2 sec[6]

A total of 1.1 bn total identities were exposed by hackers in 2016[13]

In 2016, 70% who were subject to cyber attacks had to pay to unlock their device[6]

Attacks

73% of malware attacks in 2016 began with phishing emails[5]

Number of cyber attacks on the government sector doubled globally to 14% in 2016[8]

Loses

$4.63 bn losses resulted from 1,407,849 Cybercrimes from 2013 until 2016[9]

40% of breached organizations lost 20% customer base in 2016[10]

Cyber Criminals

Since 2010, hackers have earned £85 bn, with £12.8 bn earnings in 2016 alone[6]

£32.60 is the average earnings of hackers per hour6

Cyber criminals demanded an average ransom of $1,077 per victim in 2016[13]

Attacks across geographies

$3.6 mn is the total cost of global data breaches in June 2017[7]

53% of worldwide phishing attacks in 2016 originated from EMEA[11]

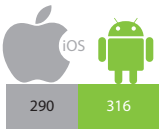
DDoS: Distributed Denial of Service

Targeted platforms and technologies

In today's cyber landscape, new and sophisticated threats continue to emerge on a daily basis across multiple platforms & technologies. Cyber criminals pose different types of threats to organizations across various sectors and geographies, driven by a host of socio, economic and political motivators*

The most targeted platforms and technologies

Technology and businessrelated websites are the most frequently exploited websites[1]



Android OS is the most attacked mobile platform[1]

66% of IoT attacks are detected in video cameras[2]

Most targeted user technologies

Enterprises business incurred $3 bn losses due to Business Email Compromise (BEC) scams[3]

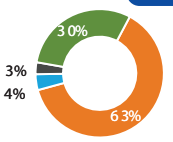
Nearly 30% of attacks targeted end-user technologies are from Adobe, Java, and Microsoft products[3/4]

Most attacked sectors worldwide[2]

Cyber attacks on the Government sector increased from 7% in 2015 to 14% in 2016[5]

Cyber attacks on the finance sector increased from 3% in 2015 to 14% in 2016[5]

Top attacked source countries[2]



US has consistently been the major source of hostile activity since 2013[5]

Most prevalent types of attack[2]

Suspicious activities, with a 30% share, remained the most prevalent type of attack in 2016[5]

Web application attacks up from[5] 3% 6%

DoS/DDoS up from[5] 15% 16%

Course5 Transformative intelligence

Cybercriminals: Who and Why

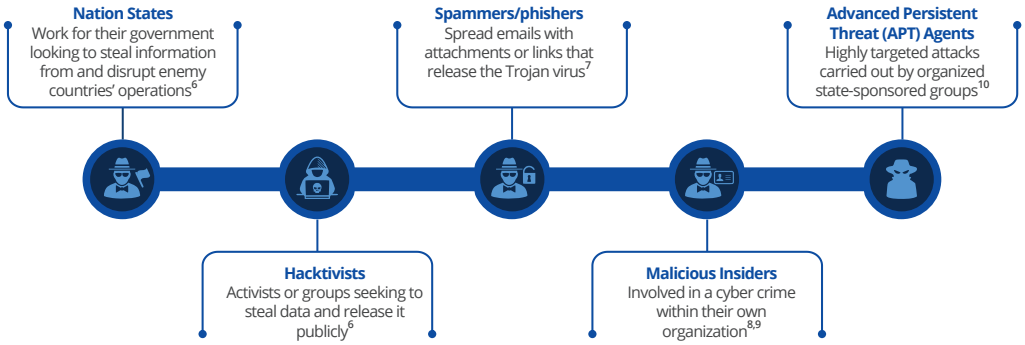
Cyber criminals are professional, organised, better funded, well trained and highly motivated in executing threats and attack s that outweigh security teams capabilities*….

Criminals are using **social media** to sell and share data[1,2]

458% increase in the number of times hackers searched Internet of Things connections for vulnerabilities in 2016[3]

Two types of hackers have been driving increasing **coordination** in dangerous cyber attacks: **Nation-sponsored groups** and **organized cyber criminals**[4]

89% of cyber criminals attack with financial or espionage motivations[5]



"Cybercriminals are increasingly taking a business-based approach toward their activities, with some organizations developing in-house training, disaster recovery, and other business functions, and others contracting for those services in the underground marketplace, **Cybercrime is maturing as a business model"**

-said Shogo Cottrell, a security strategist with HPE Security[11]

A reactive approach in the security domain is in an isolated state; is no longer sufficient to protect against the latest cyber threats[11]

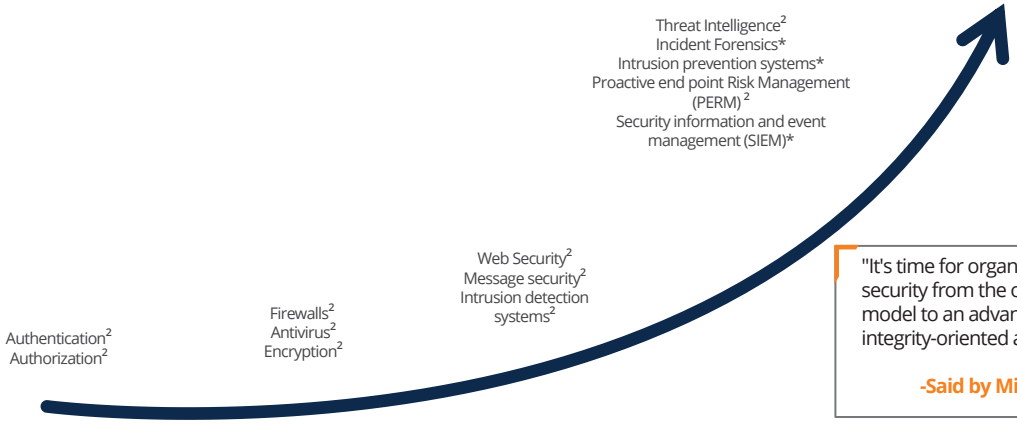
Security solutions: Changing approach

The number of security **breaches and violations are on the rise. And existing reactive security solutions** cannot stop them[*,1]

Reactive security solutions

Organizations are moving from a **Reactive to Proactive approach** that **predicts, isolates, and minimizes the attacks** and also provides visibility into the type of attacks that is likely to take place[*,1]

Proactive security solutions



"It's time for organizations to reframe their security from the old, reactive threat-oriented model to an advanced, proactive, predictive, and integrity-oriented approach" 3

-Said by Mike Rosen, VP of research, IDC

Threat intelligence is the enabler to a more proactive security approach

Threat Intelligence: Why and How

Cyber attackers continuously targeting businesses/organizations*

In this scenario, a sophisticated security solution such as **"Threat Intelligence" is inevitable***

Threat= Capability to Cause Harm

Intelligence= Information, Analysis & Context

Threat Intelligence=Information, its Analysis and Context Regarding 'Things' that might cause Harm[1]

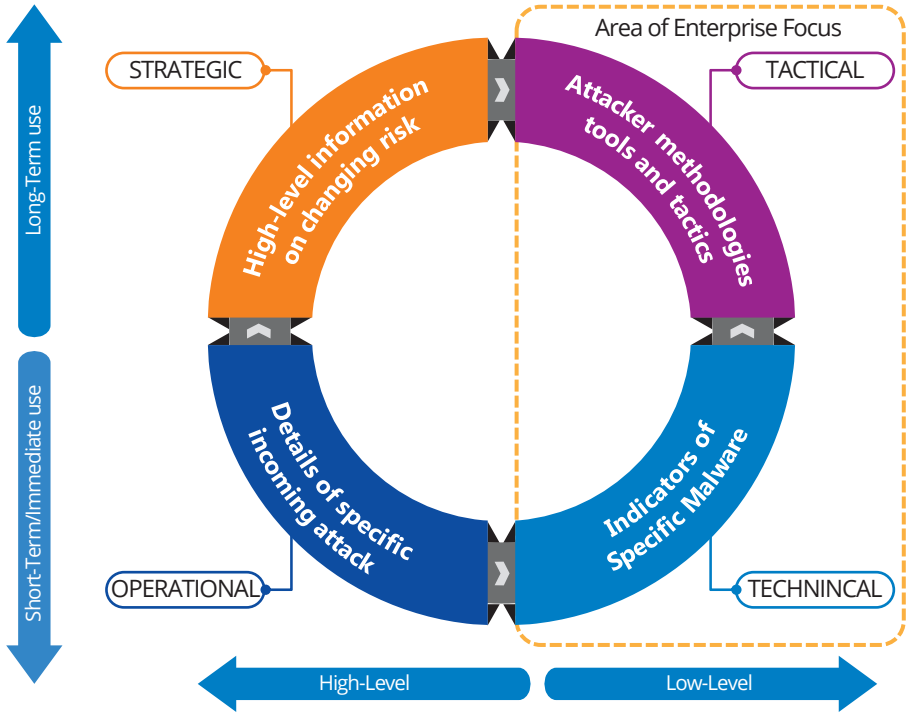
"Threat intelligence" in organizations will manage cyber attacks by being both **proactive and responsive.**

Adopting the life-cycle model, the outcome of the analysis will allow organizations' security teams to keep an eye out for cyber attacks in advance and take remedial measures*

Threat Intelligence life cycle[2]

Threat Intelligence: Need at various organizational levels

Need for Threat Intelligence at different levels of an organization[1]



Strategic Threat intelligence[1]

Target Audience: The board, executive management and decision makers
Focus of changing risks, high level topics: Geopolitics foreign markets and cultural background
Vision timeframe: Years

Operational Threat Intelligence[1]

Target Audience: Strategic security teams and defenders
Focus on threat actors, nations state actors and future attacks, etc. based on infiltration threat actor groups
Vision Timeframe: Hours to months

Tactical Threat Intelligence[1]

Target Audience: System admins, pen testers, Hunters
Focus on TTPs (Tactics. Techniques and procedures, tools, etc.)
Vision Timeframe: Weeks to months

Technical Threat Intelligence[1]

Target Audience: SOC, IR, Firewall Admins
Focus on Indicators of compromise, malware domains, artefacts, signatures, etc.
Vision timeframe: Hours to years

Course5 Transformative intelligence

Defining Threat Intelligence

The Threat Intelligence market is made up of advanced security event monitoring and management technologies that incorporate a variety of threat-related information sources to develop predictive security. Threat Intelligence market is made up of vendors that provide products, services, or professional services (or a combination of these) to meet enterprise demands for APT solutions and actionable advice[1]

"Threat Intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard[2]

Threat Intelligence is an advance process that enables the organization to gather valuable insights based on the analysis of contextual and situational risks and can be tailored to the organization's specific threat landscape, its industry and markets[3]

Threat Intelligence includes specifics on the tactics, techniques and procedures of these adversaries. Threat Intelligence's primary purpose is to inform business decisions regarding the risks and implications associated with threats[4]

The set of data collected, assessed and applied regarding security threats, threat actors, exploits, malware, vulnerabilities and compromise indicators[5]

Threat Intelligence is information about adversarial threats' past, present and predicted attacks against the organisation, produced through analysis of available information to inform decisions and actions

APT: Advance Persistent Threats

Threat Intelligence: The Evolution

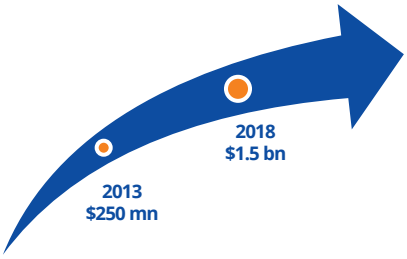
	1980-1990's[1]	late 90s and early 2000s[1]	late 2000 (2005-2013)[1,*]	2013-Today[*,3]
Vulnerabilities created by	Adoption of the PC, enterprise networks, and the Internet[1]	Mainstream adoption of the Internet, web, and eCommerce[1]	Cloud, social, mobile computing, social web, IoT[1]	Cloud, social, mobile computing, social web, IoT[1]
Threats	Micro viruses, email, DoS, limited hacking, worms[2]	Network DoS**, Blended Threat (Worm, virus + Trojan) Widespread system hacking, spyware, spam, phishing[2]	Advanced persistent threats, Zeroday vulnerabilities and cyberware[*]	Advanced persistent threats, Zeroday vulnerabilities and cyberware[*]
Security products	Firewalls, authentication systems, anti-virus and other types of anti-malware products[1,*]	Intrusion detection system, prevention systems designed to detect and prevent attacks in real-time[1,*]	SIEM systems collect, store and analyze security event logs, alert IT personnel for suspicious events, and produce reports to Execute pre-defined policyscripts[1,*]	Advanced SIEM and big data security analytics solutions provide policy management, compliance reporting, incident response, and forensics[1,*]
Evolution	**Threat Detection and Protection**[*]	Threat Detection and **Prevention**[*]	Threat Detection, Prevention and **Proactive approach**[*]	**Threat Intelligence***

DoS: Denial of service; SIEM: security information and event management

**Denial of service DoS

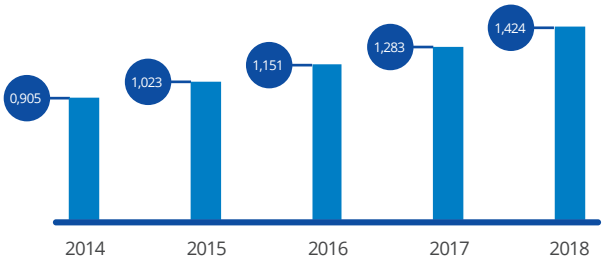
Threat Intelligence: Market landscape and opportunity

Threat intelligence market is growing1.....



Source: Competitive Landscape, Threat Intelligence services, Gartner, Oct 2015

Worldwide Threat Intelligence security services spending in $ bn[2,3]



Source: Worldwide Threat Intelligence Security Services 2014 - 2018 Forecast; IDC Mar 2014

"North America will lead Threat Intelligence security market in the future[4]

SME segment is expected to adopt Threat intelligence at the highest rate during 2017-2022[5]

Incident forensics, a Threat Intelligence segment, is expected to grow at the highest CAGR during 2017-2022[5]

By 2020, Threat Intelligence will be the fastest-growing section of the fifty billion dollar network security market, becoming ten times more valuable than traditional security solutions[6] IDC

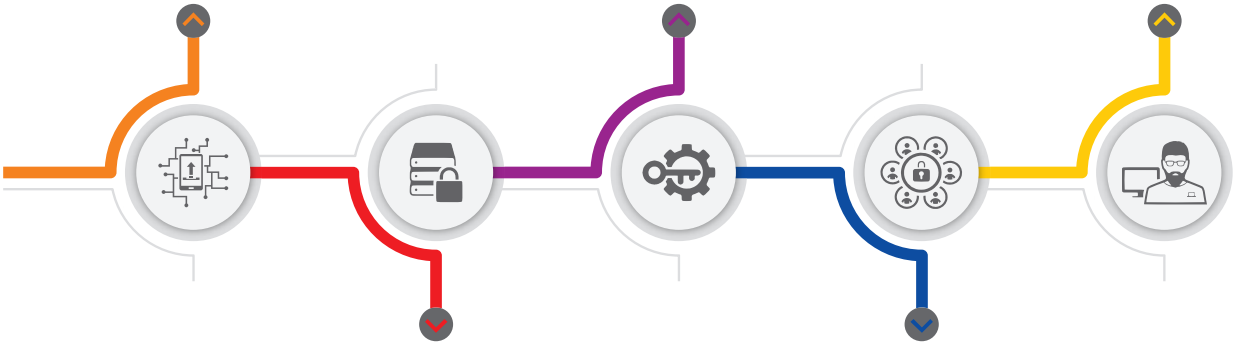
By 2018, 60% of companies worldwide will use outside Threat Intelligence services. These offers are skyrocketing and becoming essential to the security strategy of corporations[7] Gartner

Threat Intelligence: The Evolution

Technology Growth and Usage Changes*
Organizations' use of latest technologies such as BYOD, wireless networking, virtualization and cloud computing, is resulting in exposure to advanced cyber attacks, thus fuelling the need for advanced security solutions such as Threat Intelligence

Obsolete Traditional security tools*
Traditional security tools are becoming less effective in addressing the new and evolving cyber security breaches

Increasing complexity of cyber threats[1]
Companies are targeted with Advanced Persistent Threats (APTs). such as DDoS, Ransomware, thus driving the adoption of Threat Intelligence security services



Growing concerns on data security and across industries[1]
Cyber attacks are rampant irrespective of the type of industry. Therefore organizations across various industries are responding to these cyber threats by issuing strict security regulations and compliance with data security

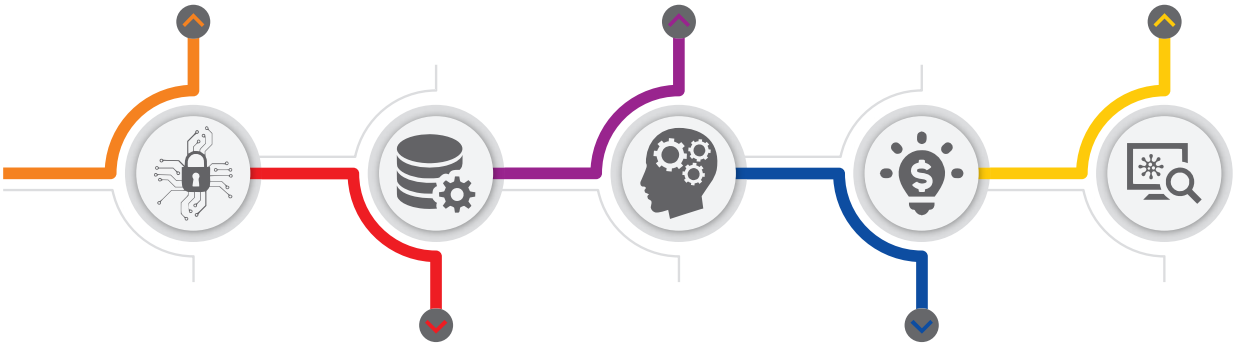
Increasing adoption of crowd sourced Threat Intelligence[2,3]
There has been an increase in the number of security professionals sharing threat data publicly, as well as with trusted peers, which has effected a jump in the adoption of crowdsourced platforms for Threat Intelligence sharing

Threat Intelligence: Major inhibitors

Shortage of skilled cyber security professionals [1,*]
There is a shortage of skilled cyber security professionals to effectively manage large volumes of unstructured threat information. The most skilled candidates are hired by larger organizations

Lack of expertise and technical knowledge [2,*]
Threat management requires experience to identify threats, understand the technicalities, and take prompt legal action to mitigate risks. So it is necessary to train and retain highly experienced Threat Intelligence professionals

Lack of ability to choose right Threat Intelligence platform [1,*]
An organization's ability to choose the right Threat Intelligence platform that best fits with their security infrastructure in the crowded market is still a major concern for the organizations



Data Overload [1,*]
Security operations centers (SOC) are flooded with immense volumes of data from Threat Intelligence sources, and public/private sharing platforms. Hence, digesting threat information feeds from multiple sources can be a slow and painful process

Lack of budget [2,*]
The cost of deployment is still high and many enterprises view budgetary constraints as a barrier. Organisations are now simply rebalancing their investments, without necessarily allocating increased budgets for Threat Intelligence

Leading vendors in the market

Recorded Future · DIGITAL SHADOWS · LOOKINGGLASS · NORSE · CENTRIPETAL NETWORKS

VERISIGN · SecureWorks · CROWDSTRIKE · iSIGHTPARTNERS (Got acquired by FireEye) · Geo IP

Symantec · SURFWATCH · FireEye · RSA SECURITY

THREATQUOTIENT · threatstream · THREATCONNECT · cytegic

SecureWorks · Infoblox (CONTROL YOUR NETWORK) · Vorstack · TREND MICRO

IBM · EMERGING THREATS · anubisnetworks (a BITSIGHT company) · McAfee

Threat Intelligence: Classification of vendors

Classification based on Threat Intelligence cycle

Planning and Collection

OpenSource Intelligence[1]
- Recorded Future
- Digital Shadows
- LookingGlass (acquired Cyveilance)

Human Intelligence[1]
- LookingGlass (acquired Cyveilance)
- Booz Allen Hamilton
- Crowdstrike
- FireEye (acquired iSight Partners)
- Verisign

Technical Intelligence[1]
- Norse Crop
- Anubis Networks
- Emerging Threats

Analysis and production

Adversary Intelligence[1]
- CrowdStrike
- FireEye (acquired iSight Partners)
- Verisign
- Symantec

Strategic Intelligence[1]
- Surfwatch Labs
- Cytegic

Dissemination

Vulnerability Intelligence[1]
- FireEye (acquired iSight Partners)
- Verisign

Threat Intelligence Platform[1]
- Lookingglass solution
- Vorstack Automated
- Threat Quotient
- ThreatStream
- ThreatConnect

Threat Intelligence Enrichment[1]
- Passive DNS
- GeoIP
- Whois data

Threat intelligence Integration[1]
- Norse Application
- Centripetal Networks
- Lookingglass

Classification based on sources, reports and hardware players

Data Feeds[2]
- FireEye: .
- RSA Live
- SecureWorks
- LookingGlass
- Infoblox
- Symantec

Alerts and Reports[2]
- LookingGlass
- SecureWorks
- FIreEye
- McAfee
- RSA
- Verisign
- Symantec

Hardware Players[3]
- IBM
- Symantec
- McAfee
- Trend Micro
- Dell SecureWorks.
- FireEye
-

How are businesses embracing Threat Intelligence currently

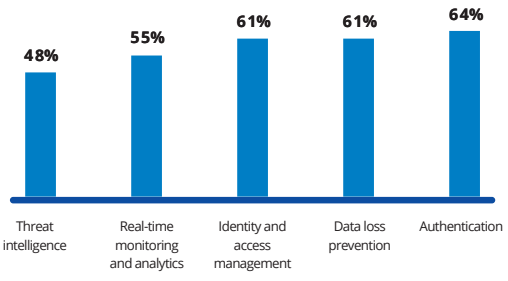
Organizations are starting to move beyond offering reactive security solutions, and embracing proactive Threat Intelligence s

Statement that best describes the maturity of organization's Threat Intelligence program[1]

Organizations do not have a Threat Intelligence program	5%
Organizations have an informal Threat Intelligence program that incorporates information from trusted third parties and email distribution lists	10%
Organizations have a formal Threat Intelligence program that includes subscription threat feeds from external providers and internal sources, such as SIEM tool	20%
Organizations have a Threat Intelligence team that collects internal and external threat and vulnerability feeds to analyze for credibility and relevance in their environment	30%
Organizations have an advanced Threat Intelligence function with internal and external feeds, dedicated intelligence analysts and external advisors that evaluate information for credibility, relevance and exposure against threat actors	36%

Source: A close look at cyber Threat Intelligence, E&Y, 2016

Primary security services that companies use[2]



Source: The Global State of Information Security Survey, PwC, 2017

51% global CIOs and CSOs monitor and analyze Threat intelligence to help detect risks and incidents[3]

20% of organizations outsource their Threat Intelligence collection and/or feeds[4]

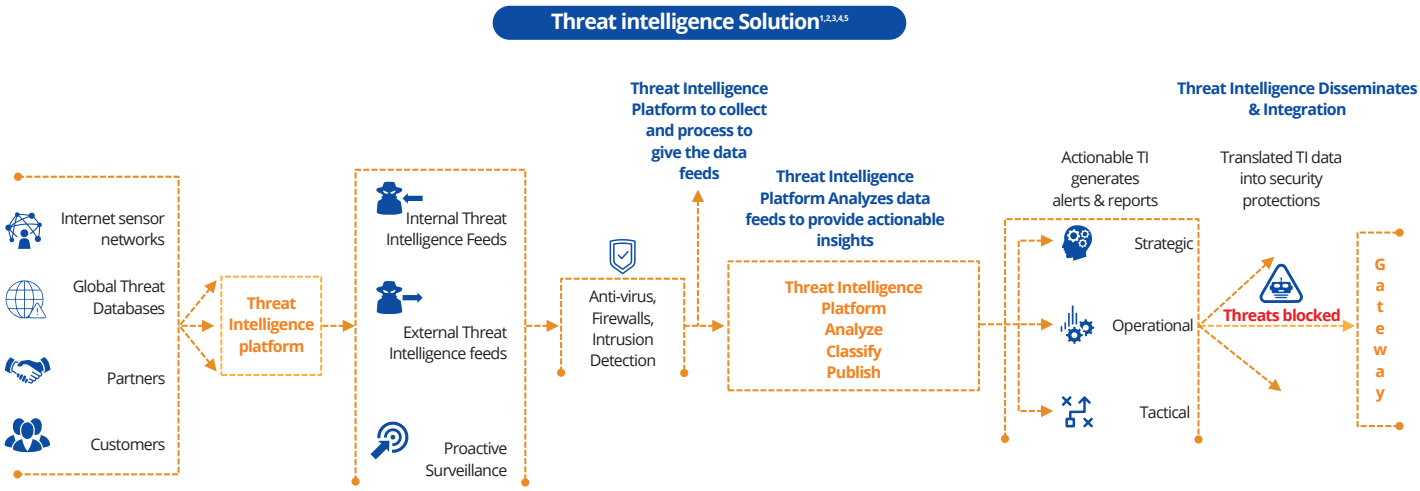
31% of organizations have SOC** dedicated individuals focusing solely on Threat Intelligence[4]

41% of organizations say their SOC* has a paid subscription to Threat Intelligence feeds[4]

14% of organizations outsource their Threat Intelligence analysis[4]

Source: A close look at cyber Threat Intelligence, E&Y, 2016

Threat Intelligence solution fitment in organizations



Threat Intelligence: Existing scenario

Approach towards Cyber Security is shifting from reactive to proactive, which has enabled 'Threat Intelligence' to gain tract ion in the market. In the current scenario*...

Current Scenario

- Increasing adoption of Threat Intelligence is affecting traditional security offerings such as firewalls, antivirus programs, etc.*
- Vendors are offering fragmented Threat Intelligence solutions to customers*
- Financial and government institutions lead in implementing Threat Intelligence solutions. However, it is observed that health care, retail, manufacturing and telecom sectors are also using Threat Intelligence platforms extensively*
- More than half of all organizations at a global level do not have a total Threat Intelligence solution implemented in their networks or systems*
- Cloud-based threat-management capabilities are rapidly evolving, changing the model of on-premise cybersecurity and privacy solutions*

Threat Intelligence: Existing scenario

Approach towards Cyber Security is shifting from reactive to proactive, which has enabled 'Threat Intelligence' to gain tract ion in the market. In the current scenario*...

Market Growth

- There are very few vendors present in the security market who provide complete (end to end) Threat Intelligence solutions. Hence there is an increasing demand for vendors who offer comprehensive Threat Intelligence solutions*
- estimates that Threat Intelligence will protect IoT devices used by consumers that are connected to the internet*
- In the future, most of the large security vendors are likely to offer Threat Intelligence as the default solution in their security solution portfolio*
- With growing concerns over cyber attacks, Threat Intelligence start ups offering niche features will continue to emerge*
- The demand for Threat Intelligence skilled professionals will continue to grow in the future*

Technology Growth

> Threat Intelligence technologies such as advanced threat prevention, security-incident management, SIEM, next generation firewalls and forensic analysis, are expected to witness growth in the coming years*

> Opensource Threat Intelligence data will gain traction in terms of sharing Threat Intelligence feeds to the public domain*

> Threat Intelligence features that are likely to be included in the future are intelligence sharing, machine learning and AI as primary features that will help in blocking future attacks *

About Course5 Intelligence

Course5 Intelligence enables organizations to make the most effective strategic and tactical moves relating to their customers, markets, and competition at the rapid pace that the digital business world demands. We do this by driving digital transformation through analytics, insights, and Artificial Intelligence (AI). Our clients experience higher top line and bottom line results with improved customer satisfaction and business agility. As we solve today's problems for our clients, we also enable them to reshape their businesses to meet and actualize the future.

Rapid advances in Artificial Intelligence and Machine Learning technology have enabled us to create disruptive technologies and accelerators under our Course5 Intelligence suites that combine analytics, digital, and research solutions to provide significant and long-term value to our clients.

Course5 Intelligence creates value for businesses through synthesis of a variety of data and information sources in a 360-degree approach, solution toolkits and frameworks for specific business questions, deep industry and domain expertise, Digital Suite and Research AI to accelerate solutions, application of state-of-the-art AI and next-generation technologies for cognitive automation and enhanced knowledge discovery, and a focus on actionable insight.

Visit : www.course5i.com

Course5
Transformative intelligence