



BRAND GUIDELINES 2016

TABLE OF CONTENTS

Brand Guidelines 2016.....	1	Colors	12	White Papers and Case Studies	30
Table of Contents	2	Color Palette	13	PowerPoint® and Google Slides	31
Who We Are	3	Representing Innovation, Technology, and Security	13	Digital Ads	32
The Minds Behind the Most Widely Adopted Threat Intelligence Platform	3	Font System	14	Black Hat® 2015	33
How to Use this Guide	4	Print Fonts	15	TIP eBook	34
One Brand. One Voice. One Standard.	4	Web Fonts	16	Graphics Style	35
Our Logo	5	Platform Fonts	17	Illustrating Threat Intelligence	36
The Symbol of ThreatConnect.....	6	Headers	18	Infographics	37
Logo Details.....	7	Messaging Tone of Voice	20	Mini Infographic Suite	38
The Mark:	7	Nomenclature	22	Application Icon Suite	39
The Type:	7	Photographic Style.....	24	Contact	40
Clear Space:	7	Textures, Patterns, and Photography	25		
Color Specification	8	Collateral	26		
Corporate Color Application:	8	ThreatConnect Marketing Materials	27		
Secondary Logo	10	Basic Letterhead	28		
		Business Cards	29		

WHO WE ARE

The Minds Behind the Most Widely Adopted Threat Intelligence Platform

Today, business depends on connectivity. But with connectivity comes vulnerability. It is chaos out there. Together we will bring order.

At ThreatConnect®, we take the vast potential of threat intelligence and make it accessible to Fortune 5000 organizations and allied government agencies around the globe. We have built the only truly extensible platform in the industry. We bring together trusted communities of security professionals and make ThreatConnect users stronger and more agile in order to defend themselves.

We are analysts first. We know what it takes to work at the front lines of cyber defense. We know that we are stronger together than we are apart. And, we are strategic business thinkers. Since 2011, we have led the threat intelligence revolution, building the industry's most comprehensive threat intelligence platform, along with its largest trusted cybersecurity community.

The following guidelines contain the details of our brand.

ThreatConnect® is a registered trademark of ThreatConnect Inc.

Google® is a registered trademark of Google, Inc.

Microsoft® and PowerPoint® are registered trademarks of the Microsoft Corporation.

Black Hat® is a registered trademark of UBM Tech.

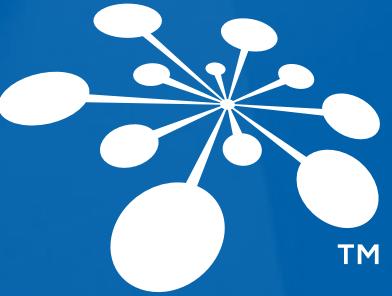


HOW TO USE THIS GUIDE

One Brand. One Voice. One Standard.

The ThreatConnect Brand Guidelines document sets the standard of quality, tone, and identity for the ThreatConnect brand. The document is intended for all ThreatConnect team members to read, internalize, and reference when creating any new internal or external collateral or when presenting the ThreatConnect platform to potential clients. All team members in all departments must adhere to the guidelines contained within so that the ThreatConnect brand can remain powerful, consistent, and distinct across all collateral and channels, now and as the company continues to grow.

Any questions on brand guidelines should be directed to the marketing team. Any new collateral and any exceptions to the guidelines must be approved by the CMO.





OUR LOGO



THE SYMBOL OF THREATCONNECT

The ThreatConnect logo is the center of our graphic identity system. The type and mark concisely represent what we do and who we are. The full logo and logo mark must be consistently applied wherever they are used.

Primary Logo





LOGO DETAILS

The Mark:

The ThreatConnect “bloom” mark is comprised of 11 round figures: each of a specific varying size and each connected to a central hub via slender, tapering arms. The mark represents community—the interconnected threat intelligence networks our platform creates. It represents the notion that we are stronger together, and that only as a united entity, we are able to decipher order from the chaos of the cyber threat landscape. The use of color to highlight particular figures within the mark emphasizes the unique intelligence and perspective of each contributor and, likewise, represents the grave risk of a potential threat.

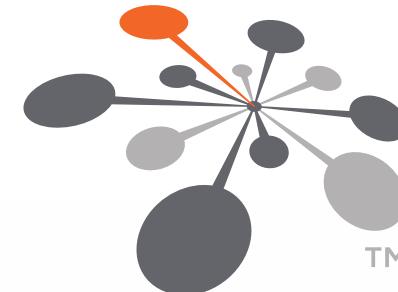
The Type:

The type uses a clean, modern sans-serif font with subtle custom-designed letters to illustrate attributes of the brand. The simple lines and sharp corners denote cutting-edge technology and forward-thinking innovation. The customized “NN” letters symbolize connection and use parallel lines to represent alignment, partnership, and shared purpose.

The mark can be used without the type, but the type should not stand alone without the mark.

Clear Space:

The clear space surrounding the logo should be equal to or greater than the height of the capital “T” in “ThreatConnect.” This allows for appropriate scaling.



Bloom Mark



Mark

Type



Minimum Clear Space



Two-Color Printing



One-Color Printing



COLOR SPECIFICATION

Corporate Color Application:

The two-color ThreatConnect logo should be used in all contexts where a light or white background is present. The two-color reverse logo should be used over a dark gray or dark blue background. The one-color black logo should be used over light backgrounds only when color is not available. The one-color reverse logo should be used over dark backgrounds when color is not an option.

Two-Color Reverse



One-Color Reverse



Two-Color Reverse



One-Color Reverse



Column two should only be used as a last option.



INCORRECT USES

Do Not Use Old Logo



Do Not Alter the Scale of "Bloom"



Do Not Alter Alignment



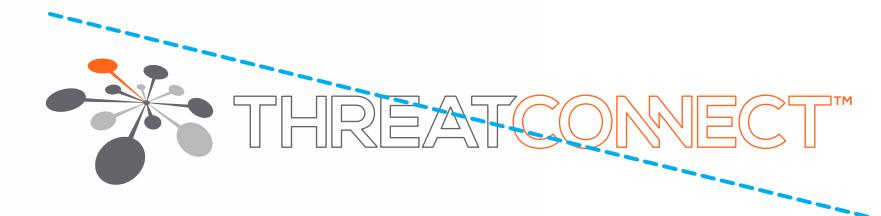
Do Not Apply Effects



Do Not Stretch or Compress



Do Not Use Outlines





SECONDARY LOGO

Use this logo for vertical spaces or when in confined areas.

THREATCONNECT **BRAND GUIDELINES**



Two-Color Printing



One-Color Printing



Column two should only be used as a last option.

Two-Color Reverse



One-Color Reverse





COLORS



COLOR PALETTE

Representing Innovation, Technology, and Security

The ThreatConnect color palette is comprised of three core tones: Pantone 165 (orange), Pantone Cool Gray 10, and Pantone 534 (blue).

These core colors were carefully selected to represent central themes of the ThreatConnect brand. The blue gives a sense of security, confidence, and trust. The orange represents the spark of innovation, and the gray represents the flexibility and compatibility that sets our platform apart. The core color palette is supported by supplementary colors. ThreatConnect-branded collateral should use the following colors:

Primary Colors



PANTONE
165

cmyk: 0, 74, 98, 0
rgb: 242, 103, 36
hex: #f26724



PANTONE
cool gray 10

cmyk: 61, 53, 48, 19
rgb: 100, 101, 105
hex: #646469



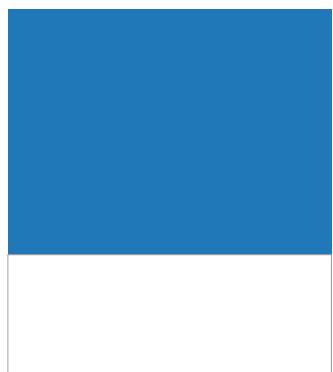
PANTONE
534

cmyk: 97, 81, 47, 56
rgb: 7, 34, 58
hex: #07213a

Secondary Colors



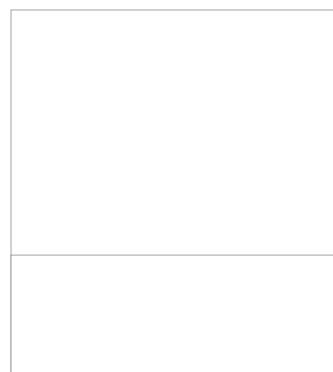
cmyk: 98, 82, 47, 55
rgb: 6, 34, 59
hex: #06213b



cmyk: 83, 48, 4, 0
rgb: 41, 120, 183
hex: #2878b7



cmyk: 19, 15, 16, 0
rgb: 204, 204, 204
hex: #ccccbc



cmyk: 0, 0, 0, 0
rgb: 255, 255, 255
hex: #ffffff



FONT SYSTEM



PRINT FONTS

ThreatConnect uses the Montserrat font family as our primary header typeface and Helvetica Neue LT Std 75 Light for body copy.

Header Copy

Montserrat Bold | Regular

ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
1234567890!@#\$%^&*(.,:)

Body Copy

Helvetica Neue LT Std | Light | Roman | *Italic* | **Bold | **Bold Italic****

ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
1234567890!@#\$%^&*(.,:)



WEB FONTS

Alternate universal typefaces that closely resemble the primary typefaces should be used on the Web. Use Montserrat Bold for headers and Open Sans Light or Regular for body copy.

Header Copy

Montserrat Bold | Regular

ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
1234567890!@#\$%^&*(.,:)

Body Copy

Open Sans Light | *Light Italic* | Regular | *Italic* | **Bold**

ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
1234567890!@#\$%^&*(.,:)



PLATFORM FONTS

The ThreatConnect platform is our core offering. Therefore, its user interface should reflect our brand identity throughout. Within the ThreatConnect platform, use Montserrat Bold for headers and Open Sans Light or Regular for body copy.

Header Copy

Montserrat Bold | Regular

ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
1234567890!@#\$%^&*(.,:)

Body Copy

Open Sans Light | Light Italic | Regular | Italic | Bold

ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
1234567890!@#\$%^&*(.,:)



HEADERS

Headers should alternate in size and color and follow a clear hierarchy on each page. Always begin a new page with H1. Use H2 to indicate sub-sections or paragraph headings. Use H3 to indicate sub-paragraphs, and continue in numerical order as needed, according to the hierarchy, point size, and color use outlined herein.

HEADER 1 | MONTserrat | BOLD | 14PT/14PT

Body Copy 9pt/14pt. Helvetica Neue LT Std (45 light) Bold Body (Helvetica Neue LT Std 75 Bold), Bold Italic (Helvetica Neue LT Std 76 Bold Italic) Italic text (Helvetica Neue LT Std 46 Light Italic) Link Text. Duis mollis, est non commodo luctus, nisi erat porttitor ligula, eget lacinia odio sem nec elit. Maecenas sed diam eget risus varius blandit sit amet non magna. Maecenas faucibus mollis interdum.

Header 2 | Montserrat | Bold | 13pt

Helvetica Neue LT Std (45 light) Morbi leo risus, porta ac consectetur ac, vestibulum [Link Text](#). Duis mollis, est non commodo luctus, nisi erat porttitor ligula, eget lacinia odio sem nec elit. Maecenas sed diam eget risus varius blandit sit amet non magna. Maecenas faucibus mollis interdum.

Header 3 | Montserrat | Regular | 12pt

Helvetica Neue LT Std (45 light) **Morbi leo risus, porta ac consectetur ac, vestibulum** [Link Text](#). Duis mollis, est non commodo luctus, nisi erat porttitor ligula, eget lacinia odio sem nec elit.

HEADER 4 | MONTserrat | REGULAR | 10PT

Helvetica Neue LT Std (45 light) **Morbi leo risus, porta ac consectetur ac, vestibulum** [Link Text](#). Duis mollis, est non commodo luctus, nisi erat porttitor ligula, eget lacinia odio sem nec elit.

HEADER 5 | MONTserrat | REGULAR | 10PT

Helvetica Neue LT Std (45 light) **Morbi leo risus, porta ac consectetur ac, vestibulum** [Link Text](#). Duis mollis, est non commodo luctus, nisi erat porttitor ligula, eget lacinia odio sem nec elit.

HEADER 6 | MONTserrat | REGULAR | 8

Helvetica Neue LT Std (45 light) Morbi leo risus, porta ac consectetur ac, vestibulum Link Text. Duis mollis, est non commodo luctus, nisi erat porttitor ligula, eget lacinia odio sem nec elit.

**BULLETED LIST (BODY COPY)**

- Helvetica Neue LT Std | 45 Light
- Integer posuere erat a ante venenatis dapibus posuere velit aliquet. Vivamus sagittis lacus vel augue laoreet rutrum faucibus dolor auctor.
- Integer posuere erat a ante venenatis dapibus posuere velit aliquet. Vivamus sagittis lacus vel augue laoreet rutrum faucibus dolor auctor.

BULLETED LIST (SIDEBAR)

- Helvetica Neue LT Std | 47 Light Condensed
- Integer posuere erat a ante venenatis dapibus posuere velit aliquet. Vivamus sagittis lacus vel augue laoreet rutrum faucibus dolor auctor.
- Integer posuere erat a ante venenatis dapibus posuere velit aliquet. Vivamus sagittis lacus vel augue laoreet rutrum faucibus dolor auctor.

FOOTER HORIZONTAL

3865 WILSON BLVD. | SUITE 550 | ARLINGTON, VA 22203
www.ThreatConnect.com

NUMBERED LIST (BODY COPY)

1. Helvetica Neue LT Std | 45 Light
2. Integer posuere erat a ante venenatis dapibus posuere velit aliquet. Vivamus sagittis lacus vel augue laoreet rutrum faucibus dolor auctor.
3. Integer posuere erat a ante venenatis dapibus posuere velit aliquet. Vivamus sagittis lacus vel augue laoreet rutrum faucibus dolor auctor.

NUMBERED LIST (SIDEBAR)

1. Helvetica Neue LT Std | 47 Light Condensed
2. Integer posuere erat a ante venenatis dapibus posuere velit aliquet. Vivamus sagittis lacus vel augue laoreet rutrum faucibus dolor auctor.
3. Integer posuere erat a ante venenatis dapibus posuere velit aliquet. Vivamus sagittis lacus vel augue laoreet rutrum faucibus dolor auctor.

FOOTER VERTICAL

TOLL FREE: 1.800.965.2708
LOCAL: +1.703.229.4240
FAX: +1.703.229.4489

www.ThreatConnect.com

FOOTER VERTICAL W/ CON. ADDRESS

TOLL FREE: 1.800.965.2708
LOCAL: +1.703.229.4240
FAX: +1.703.229.4489

www.ThreatConnect.com

THREATCONNECT INC.
3865 WILSON BLVD., SUITE 550
ARLINGTON, VA 22203

THREATCONNECT INC.
3865 WILSON BLVD., SUITE 550
ARLINGTON, VA 22203

FIGURE AND TABLE CAPTIONS

RESOURCE TYPE	PATHS	OWNER ALLOWED	PAGINATION REQUIRED
incidents	/v2/groups/incidents /v2/indicators/<indicator type>/<value>/groups/incidents /v2/tags/<tag name>/groups/incidents /v2/securityLabels/<security label name>/groups/incidents /v2/groups/<group type>/<ID>/groups/incidents /v2/victims/<ID>/groups/incidents	true	true
incidents	/v2/groups/incidents /v2/indicators/<indicator type>/<value>/groups/incidents /v2/tags/<tag name>/groups/incidents /v2/securityLabels/<security label name>/groups/incidents /v2/groups/<group type>/<ID>/groups/incidents /v2/victims/<ID>/groups/incidents	true	true

TABLE HEADER | HELVETICA NEUE LT STD 77 BOLD-condensed | 8PT

Table Body | Helvetica Neue LT Std 57 Condensed | 9pt

Table Body | Helvetica Neue LT Std 57 Condensed | 9pt



MESSAGING TONE OF VOICE

ASSERTIVE TONE

The ThreatConnect team is made up of some of the industry's brightest minds. We are the best at what we do. While we do not boast about it, we do speak and write confidently. We are proactive and look for new ways to solve problems. Therefore, our written content and correspondence should feature an assertive and informed tone; and with it, we communicate accurately and precisely.

PERSON

We speak and write in the first-person plural, unless introducing ThreatConnect for the first time in an article or section, which then we use third-person singular. For example: ThreatConnect is the industry's most-comprehensive threat intelligence platform. We are committed to enhancing our customers' security. This breaks down the barrier between client and company and creates a personal and interactive human-messaging style.

ACTIVE VOICE

Continuing with the theme of an assertive tone, ThreatConnect communications use active voice. For example: It is bad if "passive voice is used by ThreatConnect," but it is good when "ThreatConnect uses active voice." The difference is that in the first set of words in quotes, ThreatConnect is being acted upon, and the emphasis is on the action, not the actor. Instead, the second set of words in quotes places ThreatConnect as the actor, and ensures that the actor takes responsibility for the action. It is subtle, but this creates a style of writing that communicates strength and ownership.

PRESENT TENSE

Whenever possible, ThreatConnect writing and communication uses the present tense. For example: "ThreatConnect delivers insight that clients need" vs. "ThreatConnect has delivered insight..." or "ThreatConnect will deliver insight..." Using present tense creates a sense of tangible reality, removes hypotheticals, does not dwell on the past, and suggests continuity. Present tense complements active voice, and it creates an assertive tone.

SIMPLICITY

ThreatConnect makes it easy for clients to manage threat data. Our message reinforces this sense of ease by being concise and direct. We do not use complex sentences when a straightforward one will suffice. When a complex sentence can be split and shortened, we split and shorten it. The same applies to punctuation. We do not use semicolons when a period will suffice. Currently, ThreatConnect does use the Oxford comma. For example: "There is one thing, another thing, and the Oxford comma." The Oxford comma separates "another thing" and "and."

SPEAKING DIRECTLY

We speak directly to our audience on a personal level. A reader must get the impression that a ThreatConnect team member is speaking directly to him or her, rather than speaking generally about "clients" and "users." For example: "Your team will be better equipped to protect your organization from modern cyber threats."



NOMENCLATURE

THREATCONNECT BRAND NAME

“ThreatConnect” is the correct and only acceptable written form of our company name.

- ✓ **Correct Use:** ThreatConnect, ThreatConnect’s
- ✗ **Incorrect Use:** TC, Threatconnect, threatconnect, Threat Connect, Threat-Connect, or any derivation other than above.

THE DIAMOND MODEL FOR INTRUSION ANALYSIS

The Diamond Model for Intrusion Analysis is our fundamental threat intelligence methodology.

- ✓ **Correct Use:** Diamond Model for Intrusion Analysis, the Diamond Model
- ✗ **Incorrect Use:** DMIA, the Diamond, Diamonds Model, Diamond Methodology, Diamond Model for Threat Detection, or any derivation other than above.

THREATCONNECT PLATFORM

“ThreatConnect” is also the name of our flagship threat intelligence platform. The ThreatConnect platform is not to be called a “tool” or “software” or “product.”

- ✓ **Correct Use:** ThreatConnect platform, the ThreatConnect platform, ThreatConnect’s platform
- ✗ **Incorrect Use:** TC’s platform, ThreatConnect Platform (unless in title case), TCP, or any derivation other than the above.

THREAT INTELLIGENCE PLATFORM

ThreatConnect is the industry’s leading Threat intelligence Platform (TIP).

- ✓ **Correct Use:** Threat intelligence Platform, TIP
- ✗ **Incorrect Use:** TI Platform, Tip, TiP, tip, Threat Intel Platform, or any derivation other than the above.

THREATCONNECT ACRONYM USAGE

The specific acronym TCIRT is to be used only for internal communications to protect the identity of our team. Outside the company, refer to the team on a broader, general level.

- ✓ **Correct Use:** The ThreatConnect intelligence research team, our intelligence research team
- ✗ **Incorrect Use:** TCIRT



PHOTOGRAPHIC STYLE

TEXTURES, PATTERNS, AND PHOTOGRAPHY

The ThreatConnect brand is not particularly photo driven. The photography that we use is abstract and conceptual. We use photography to illustrate the concept of "chaos," represented by vast stretches of outer space and complex geometric patterns. Our graphics style is driven by custom icon illustration, to which the photographs serve as subtle background elements. We use additional high-quality photography of computers, tablets, and smartphones where needed. We use geometric background patterns throughout to communicate the message of "deriving order" from the "chaos" of the outside world.

October 8, 2015 1:55 PM

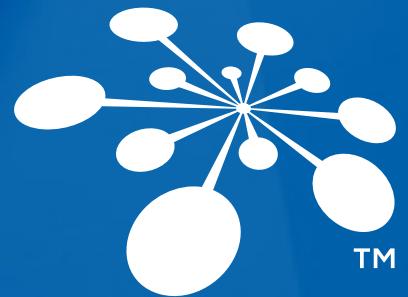




COLLATERAL

THREATCONNECT MARKETING MATERIALS

The following includes examples of ThreatConnect marketing materials. We use templates for these items to ensure consistency when new items are created. Contact the marketing team to locate the template you need for your next project.





BASIC LETTERHEAD

The basic letterhead should be used for all day-to-day correspondence, creation of new Word documents, and marketing materials that use minimal graphics.

Notes:

Do not send Word documents to individuals outside of ThreatConnect. The same holds true for Google® Docs, unless you are using the Google Doc as a collaboration tool with a partner or client.

Save your Word document as a PDF file and then send it. To produce borderless PDF files, please take the following steps in Microsoft® Word:

IN THE WORD FILE, GO TO PAGE SETUP:

- > Settings: Choose Page Attributes.
- > Format: Choose Any Printer.
- > Paper Size: Click here and then click on Manage Custom Sizes.
- > Click + to add new size. Name it PDF borderless.
- > Click in the paper size boxes to set the dimension to 8.5" x 11".
- > Make sure Non-Printable Area states User Defined, and change margins in boxes to "0".
- > Click OK.

GO TO PRINT MENU:

- > Printer: Choose Any.
- > Presets: Choose Standard.
- > Click on PDF, and choose Save as PDF.
- > Choose file name and save location.
- > Click Save.

THREATCONNECT

ABOUT THREATCONNECT

THE MOST WIDELY ADOPTED THREAT INTELLIGENCE PLATFORM

Today, business depends on connectivity. But with connectivity comes vulnerability. It's chaos out there. Together, we will bring order. Founded by analysts fresh from the front lines of cyber defense, a visionary computer engineer and a successful business leader, ThreatConnect looks to take the vast potential of threat intelligence and make it accessible for Fortune 5000 organizations and allied government agencies around the globe. By building the only truly extensible platform in the industry and bringing together trusted communities of security professionals, we make every ThreatConnect user stronger and more agile to defend themselves.

WHO WE ARE

WE'RE ANALYSTS FIRST

We're analysts first. We know what it takes to work at the front lines of cyber defense. We know that we're stronger together than we are apart. And, we're strategic business thinkers. Since 2011, we've led the threat intelligence revolution, building the industry's most comprehensive threat intelligence platform along with its largest trusted cybersecurity community.

THE DIFFERENCE WE MAKE

BRINGING SECURITY TEAMS TOGETHER

With ThreatConnect, analysts can work simultaneously with incident response, security operations and risk management teams to better defend the enterprise against modern cyber threats. Executives can address strategic business needs, mitigate risk and preserve brand integrity. We turn your security operations into a streamlined, united force.

GET STARTED TODAY

CREATE YOUR FREE ACCOUNT

Bring order to the chaos, and take the first step to protect your enterprise. Sign up for our free account today, or visit our pricing page to learn more about ThreatConnect editions and features.

3865 WILSON BLVD. | SUITE 550 | ARLINGTON, VA 22203
www.ThreatConnect.com

P 1.800.965.2708 F +1 703 229 4489
 ©2015 THREATCONNECT, INC. ALL RIGHTS RESERVED

PIONEERING THREAT INTELLIGENCE

ELITE TEAM OF CYBERSECURITY EXPERTS

ThreatConnect is leading the vanguard of threat intelligence research. ThreatConnect's threat intelligence research team is an elite group of globally-acknowledged cybersecurity experts, dedicated to tracking down existing and emerging cyber threats. We scrutinize trends, technology and socio-political motivators to develop comprehensive knowledge of the cyber landscape. Then, we share what we've learned so that you can protect your organization, and your team can take precise action against threats.

3865 WILSON BLVD. | SUITE 550 | ARLINGTON, VA 22203
www.ThreatConnect.com

P 1.800.965.2708 F +1 703 229 4489
 ©2015 THREATCONNECT, INC. ALL RIGHTS RESERVED



BUSINESS CARDS

ThreatConnect business cards include employee's name and title. We allow flexibility as to which social handles and contact numbers are included, based on the employee's position and job requirements.





WHITE PAPERS AND CASE STUDIES

We have developed and continue to produce numerous white papers and case studies that demonstrate our expertise. While the design of each will vary by content, general attributes of logo use, photography and graphics, colors, etc., should always follow the brand guidelines herein.

DRIVE YOUR SECURITY PROCESS WITH INTELLIGENCE

ThreatConnect is the only TIP that was built by analysts for analysts. With ease, your analysts are able to get a 360 degree perspective on your cyber adversaries' tools, infrastructure, techniques and processes. But, we didn't just think about analysts. Security Directors and CISOs are finally able to create tactical playbooks for their teams and continuously test their efficacy, ensuring the best possible defense with their current resources.

You'll also gain efficiency because ThreatConnect improves accuracy by pulling all of your structured and unstructured threat data into one centralized platform including the industry's leading threat intelligence feeds, STIX formatted data and even the most basic email formats. Even better, the threat data is automatically normalized so that your team can pivot between different data points to uncover patterns and commonalities of relevant intelligence.

ThreatConnect's flexible API empowers your team to build applications or integrations with your critical security infrastructure. All of which allows your team to spend their valuable time focusing on resolving real threats, immediately.

Furthermore, **TC Exchange™** allows you to build, host and share secure, customized applications that enable better intelligence gathering, analysis and sharing. TC Exchange also allows you to access open source and premium feeds to enhance your threat intelligence.

www.ThreatConnect.com

CASE STUDY

COMMUNITY COLLABORATION ENABLES THREAT DETECTION

SUMMARY:

This case study illustrates how industry partners benefited using a ThreatConnect® private community to collaborate on intelligence, quickly leading to the detection of a specific threat.

BACKGROUND:

The private community in this Case Study was created by an organization (Organization #1) with a threat intelligence analysis team acting as the chief moderator. The moderator invited five participating organizations within its industry to join after careful vetting. The participating organizations' threat intelligence programs and staff have varying levels of maturity; some do not have a security staff member dedicated to threat intelligence analysis.

Several of the partner organizations had not worked together before the establishment of the ThreatConnect Community. The moderator does not allow for anonymous profiles in the community, which increased trust and transparency amongst the participating members. Organization #1 chose to moderate the community themselves rather than engage with the ThreatConnect Intelligence Research Team (TCIRT). All sharing and collaboration happened within the ThreatConnect Private Cloud platform.

The moderator established rules and guidelines for participation, including but not limited to:

- Intended goals of the community
- Acceptable use of community data for defensive actions,
- Restrictions on use of community data related to internal reporting, public exposure, and malicious intent, timeliness and sanitization of contributed intelligence, and
- Social spirit (citizenship) of community members related to collaborative working, growth and trust.

Sharing communities exist today, but are largely maintained through email and word of mouth. The ThreatConnect platform was designed to enable community collaboration with structured data in a controlled manner. Today's ThreatConnect communities support industry, geographic, and threat-themed sharing partners.

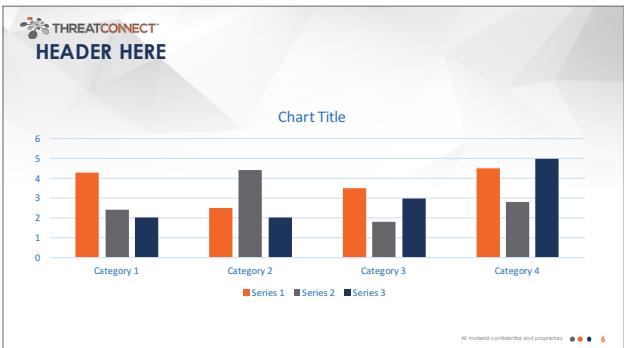
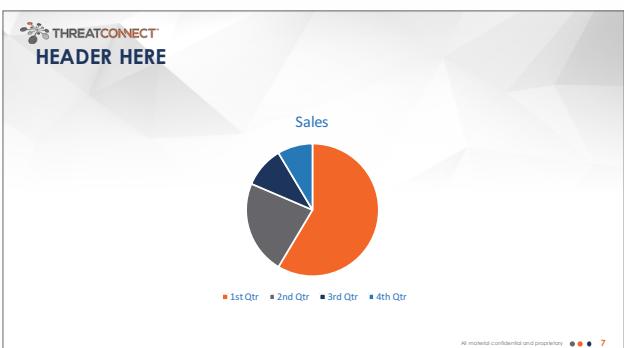
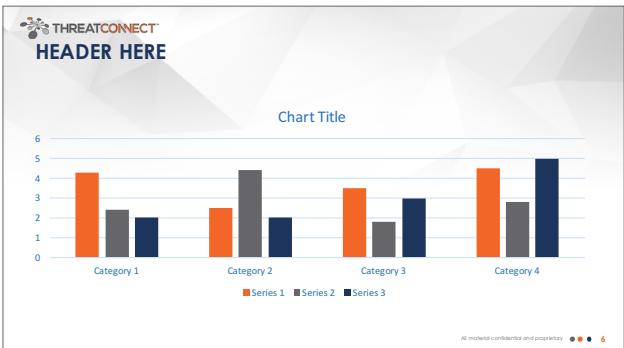
3865 WILSON BLVD | SUITE 550 | ARLINGTON, VA 22203
www.ThreatConnect.com

P 1.800.965.2708 F +1.703.229.4489



POWERPOINT® AND GOOGLE SLIDES

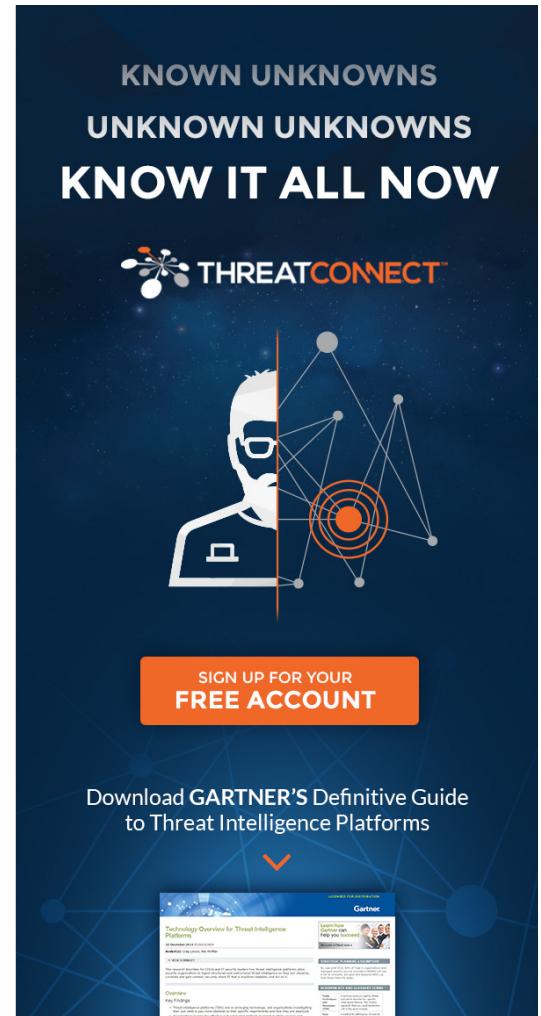
The ThreatConnect PowerPoint and Google Slides template is intended for day-to-day use. All company internal presentations, sales pitch decks, and external presentations must use these standard templates.





DIGITAL ADS

ThreatConnect runs numerous advertising and lead generation (gen) campaigns across relevant publications and the Google Display Network. Advertising creative and messaging must adhere to the visual and tone-of-voice guidelines contained herein.





BLACK HAT® 2015

Special events call for special collateral. The following examples demonstrate how ThreatConnect's brand can be carried across unique concepts while still exhibiting the necessary consistency.





TIP EBOOK

Our Threat Intelligence Platforms eBook is one of the central collateral pieces in our lead gen efforts and should be reproduced only in the final, approved format. Any future documents of this type should demonstrate a similar look and feel.



**CHAPTER ONE:
WHY THREAT
INTELLIGENCE
MATTERS**

**FIRST AND FOREMOST:
KNOW YOUR ENEMY**

Yes, you have an enemy. It's highly probable you have more than one.

Today's threats are relentless and come in all shapes and sizes. While the internet has enabled a global economy to explode, it has also made it easier than ever to steal data. The internet was built for connectivity, not security. Approaches such as intrusion detection systems, anti-virus programs, and traditional incident response methodologies by themselves are no longer sufficient in the face of the widening gap between offensive and defensive capabilities.

**THE DIAMOND MODEL
FOR INTRUSION ANALYSIS**

OVERVIEW:

The Diamond Model for Intrusion Analysis is a methodology for carrying out intrusion analysis that focuses on hypothesis generation and testing to ask questions of intrusion related data to inform decision makers of the best approach for mitigation. Since its goals as a methodology and framework are so closely aligned with that of a Threat Intelligence Platform (TIP), it is quite common to implement one or a TIP model. Analytic techniques defined by the Diamond Model can therefore be performed as a natural aspect of the mature TIP.

**LOW ORGANIZATIONAL
THREAT
INTELLIGENCE
CAPABILITY.**

PROBLEM:

Organizations that are just getting started with threat intelligence rarely have made a large investment in intelligence processes. In fact, they may have invested little to nothing in threat intelligence, and the management of threat intelligence automation. It is tempting to turn on product-integrated feeds, and this will suffice for the most basic needs of threat intelligence. This is a good place to start by the provider. But problems typically arise when hooking threat intelligence directly into the products. The integration can cause as many problems as it solves, resulting in high false positive alerts or blocks that are not relevant to the organization's needs. The security team can be overwhelmed with data in multiple product and organizational silos. Often, these are sprawled across a shared drive's directory structure. Further, when unhandled threat intelligence sources are product-specific, security teams can potentially find themselves being asked to pay for the same feed for each product.

BENEFITS OF A TIP:

A TIP provides aggregation and correlation of multiple external data sources. A TIP can help by aggregating multiple sources into one source of threat intelligence for analysis of API-based product integrations with security products. A TIP should help "wrt the what from the stuff from the various feeds through the use of a single interface. This allows the security team to get threat intelligence from the widest source it is processing when the data is deployed. A good example of this is simple ticket management, in which indicators are given times to live before they are dropped from the backlog.

PRIMARY USE CASES:

Consumption of threat intelligence for alerting and blocking.

**ACTION BEATS
REACTION**

Capture and Deploy Intelligence to Build a Strong Defense

All organizations need to gather intelligence about the threats that endanger their systems. Intelligence provides private and government organizations with a means to fend off threats in progress and, in many cases, to prevent adversaries from ever infiltrating the network at all. The use of threat intelligence leads to both a more holistic and more focused approach to security.

WHAT IS IT:

The Diamond Model looks at each relevant "cyber" event and breaks it into four vertices or nodes. These vertices represent the four main components of an incident: Adversary, Threat, Infrastructure, and Victim. The edges between the vertices form a baseball diamond shape. This is how the model got its name. The model can be described such that an adversary deploys a capability over some infrastructure against a victim.

Events do not typically happen by themselves but are part of a larger set of activity. Within the Diamond Model, each event can then be linked based on a causal relationship to the next to form a chain of diamond events. These events can be further broken down into activity groups. Activity groups are typically used within the model and typically correlate to an incident.

The Diamond Model is flexible to work with existing or emerging ontologies of cyber activity. The Diamond Model can be used as a threat intelligence taxonomy itself, but rather a framework to enable analysis independent of the structure of the data. Each node on the diamond can be further characterized with knowledge about it, or the edges can be characterized to describe the relation between nodes on the same edge or between nodes on separate groups of activity.

Activity groups can be established in just this manner by correlating nodes from events across incidents or knowledge of infrastructure or threat intelligence that is used operationally. Once an activity group is established it can be used for gaining and planning mitigation options.



GRAPHICS STYLE



ILLUSTRATING THREAT INTELLIGENCE

At ThreatConnect, we strive to communicate the details of our value proposition using the clearest possible terms. Sometimes, clarity is easier seen than read. This is why we have developed a suite of graphic icons and a distinct illustration style. Graphics and icons make it easier for our audience to understand the details and benefits of the ThreatConnect platform. We have created target-audience personas embodied in the caricatures of the Analyst, Director, CISO, CEO, and others. These icons, along with the variety of detail icons that represent attributes of the ThreatConnect platform, form our graphics suite.

Graphics Attributes

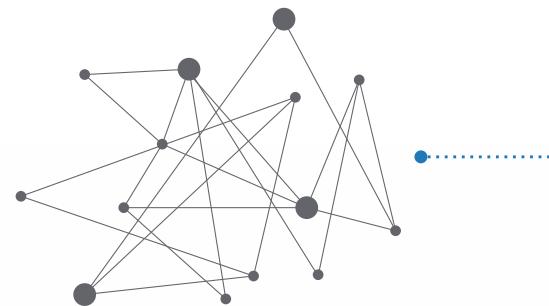
- › Two or three-color palette
- › Simple, clean lines
- › Single concept per icon
- › Avoid including typeface
- › Vector format



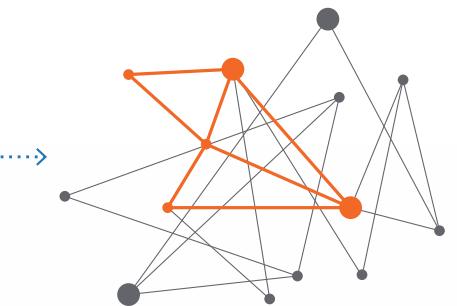
INFOGRAPHICS

Infographics are central to how we communicate the complexities of our platform. ThreatConnect has, and will continue to create, numerous infographics to illustrate aspects of our technology. Infographics should feature two- or three-color palettes, clean lines, simplicity in design, and the ability to work in both full color and grayscale, as needed.

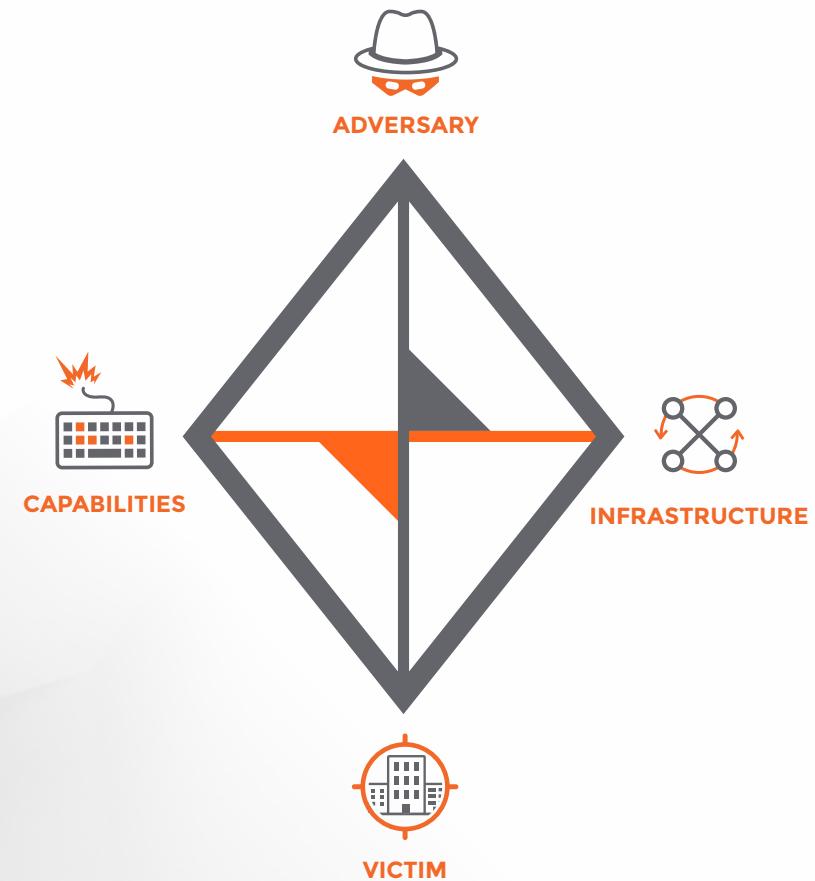
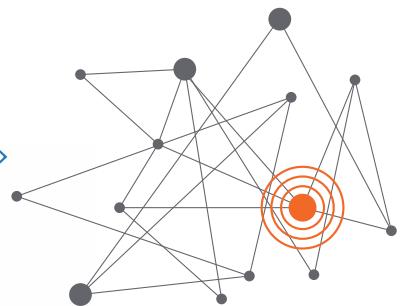
AGGREGATE



ANALYZE



ACT



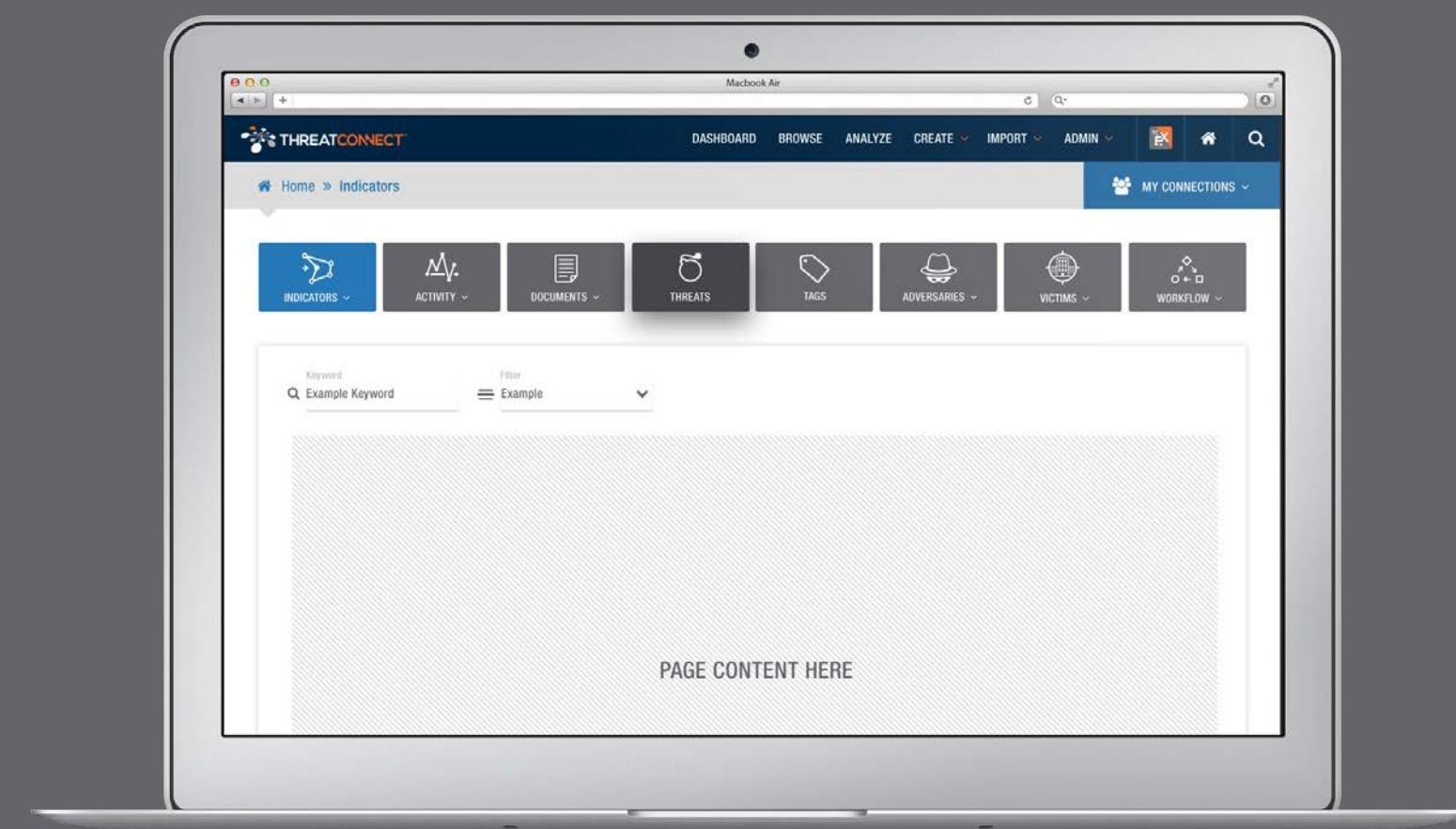
MINI INFOGRAPHIC SUITE

The ThreatConnect icon suite includes nearly 100 unique icons to represent elements of our platform, our users, the benefits of our service, and the threats we detect. All future icons should be created as simple two- or three-color designs with the ability to translate to grayscale, as needed.



APPLICATION ICON SUITE

The ThreatConnect icon suite includes nearly 100 unique icons to represent elements of our platform, our users, the benefits of our service, and the threats we detect. All future icons should be created as simple two- or three-color designs with the ability to translate to grayscale, as needed.





CONTACT



TOLL FREE: 1.800.965.2708

LOCAL: +1.703.229.4240

FAX: +1.703.229.4489

www.ThreatConnect.com

THREATCONNECT INC.

3865 WILSON BLVD., SUITE 550
ARLINGTON, VA 22203