WHITE PAPER

THREATCONNECT™

EMAIL AND THREAT INTELLIGENCE:

FROM INBOX TO ACTION

There is danger in your email box. You know it, and so does everyone else. The term 'phishing' is now part of our daily lexicon, and even if most people don't know exactly what phishing is, most people do know that clicking on a shady link can lead to the installation of malware and viruses on a computer or on a network. The bad guys love email.

But so do the good guys. Email provides a means for threat intelligence (TI) analysts to defend their organizations in two ways. First, TI analysts examine suspicious emails to gain knowledge about malicious actors that can be used to prevent future attacks. And second, TI analysts use email to share operational intelligence in the form of indicators with each other, often via listservs. TI analysts know that combining intelligence derived from emails with a greater set of threat intelligence from feeds, blogs, internal research, and other sources will help them strengthen the tactical, operational, and strategic defenses of their network-based assets. However, because the indicators and intelligence in your inbox exist in an unstructured state, making use of them for detection and prevention has been cumbersome.

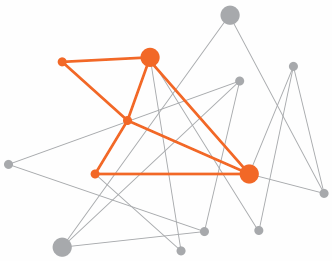
Intelligence is increasingly being produced by vendors and other intelligence-producing organizations in machine readable formats. These are collectively called Machine Readable Threat Intelligence (MRTI) and include proprietary XML, JSON, etc., as well as standards-based formats, such as STIX. MRTI provides benefits in getting intelligence into your sensors in the fastest way possible, but despite this, email as a medium for sharing operational threat intelligence is not going away. For both technological and cultural reasons, email will remain a relevant means of sharing intelligence among trusted groups.

GARTNER INSIGHT

A Threat Intelligence Platform (TIP) with built-in email functionality "significantly improves an organization's agility and process efficiency in dealing with threats by being able to ingest large numbers of sources of TI programmatically".

Aggregate

Analyze



Act

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

P 1.800.965.2708 F +1.703.229.4489

Operational intelligence today can be transmitted in ways that fall into three broad categories:

UNSTRUCTURED	MACHINE-READABLE	MACHINE-READABLE, STANDARDS-BASED
Existing technology	Existing technology	Emerging technology
Easily shareable, but unformatted	Proprietary	Typically open source
Typically IOC's must be copied and pasted into a defensive system before they can be made actionable.	May be ingestible by a TIP or other security system, but may require some reformatting or transforming of the data to be ingested.	When mature, TIPs and security devices that support the standard will be able to ingest and process standard based formatted threat intelligence regardless of source.

Until recently, there was no convenient way for TI analysts to make use of the intelligence shared via email. ThreatConnect, Inc., provider of the leading Threat Intelligence Platform (TIP), recognized this need and has responded with automated features that enable TI analysts to safely and easily share, handle, and process emails for extracting machine readable threat intelligence.

THE ROLE OF EMAIL IN THREAT INTELLIGENCE

Email from Trusted Sharing Groups

To enable sharing, TI analysts form trusted groups, which are informal organizations of peers who share information on recent attacks and emerging threats. Membership in these groups is usually by invitation, based on a vetting of invitees' credentials and reputation. These trusted groups communicate through listservs, which are closed email lists, as well as in person. According to the Ponemon Institute, 54% of organizations still share intelligence mainly via email or in-person discussions (2014).

Email will always be used by TI analysts to share information because it is both easy to use and helpful in strengthening professional relationships among the cyber security community. But an email in someone's inbox is unstructured data. It is retrievable, but not immediately actionable. It is raw material. For an email to become actionable, a TI analyst must spend time copying and pasting its contents into multiple systems for correlation, as well as monitoring and blocking.

Suspicious Emails for Threat Intelligence

Email is one of the most popular vectors for delivering targeted attacks to specific users. Phishing and spear phishing emails represent a huge risk to enterprises. However, they also contain a bonanza of forensic information that can be used as threat intelligence. Email headers contain a great deal of useful information that helps place a suspicious email into a context that shows connections to past events and can be used to help predict future attacks. Processing this information is often still a manual task, and organizations frequently rely on spreadsheets or wikis to correlate the threat intelligence that they do extract. This leaves lots of opportunities for mistakes, omitted data, or missed correlations.

54%

According to the Ponemon Institute, 54% of organizations still share intelligence mainly via email or in-person discussions (2014).

–Ponemon Institute

Processing Emails for Threat Intelligence

Converting an email into useful threat intelligence requires a series of time-consuming and labor-intensive steps, each one of which bears the potential for errors that can expose an organization to risk.

TI analysts know that the manual performance of these tasks is not the best use of their time and expertise; to do their work efficiently and provide the strongest security for their organizations, they need the ability to:

- Use the familiar method of sharing intelligence via email
- Eliminate the manual element of copying and pasting
- Consolidate knowledge from multiple silos (emails, feeds, reports, and internal observations)
- Verify suspicious emails faster
- Coordinate follow-on tasks
- Increase automation and efficiency among teams

ThreatConnect answers these needs with rich email intelligence features that allow analysts to share threat intelligence among themselves via email and to work with suspicious emails that have entered their networks.

SAFE, QUICK, AND COMPLETE EMAIL HANDLING

ThreatConnect's email processing features convert intelligence from emails into structured data that is retrievable, searchable, and actionable.

That translates into easy transporting, correlating, and vetting, which, in turn, enables the extracted intelligence to be pushed into a sensor for alerting and monitoring & blocking.

ThreatConnect users can forward emails into a private mail box that is configured to their needs for processing. Multiple inboxes can be set up for various purposes. For instance, a user might set up one inbox for suspicious emails and one for feeds. The inboxes are private and can only be viewed by authorized personnel within an organization. Once an email is forwarded into an inbox, the extracted intelligence can be sent to the Security Information and Event Management (SIEM) system or other integration for action.

STEP 1

Transform the intelligence from unstructured to structured format

STEP 2

Move intelligence into a security solution for alerting, monitoring and blocking with no loss of context, retrievability, or searchability

STEP 3

Correlate extracted intelligence with other threat intelligence in order to understand where the attack initiated and if it might occur again

STEP 4

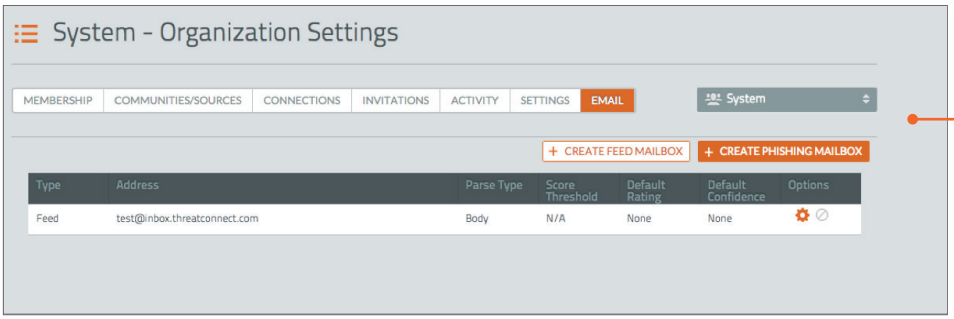
Assign the email and intelligence within it to team members for follow-on work

STEP 5

Track the progress of that follow-on work

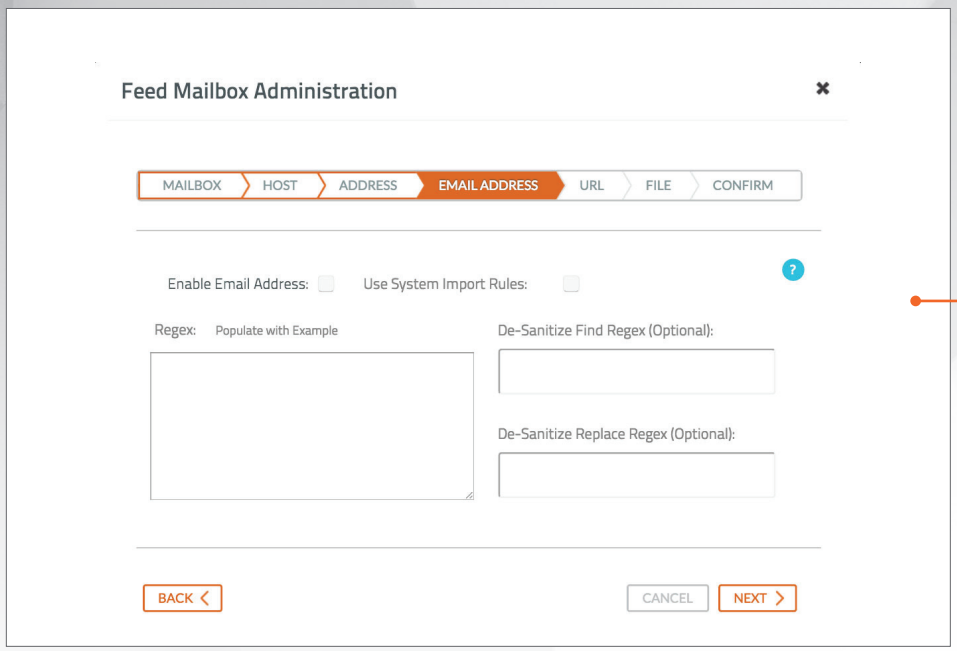
STEP 6

Manage the escalation process if necessary.



CREATE CUSTOM INBOX

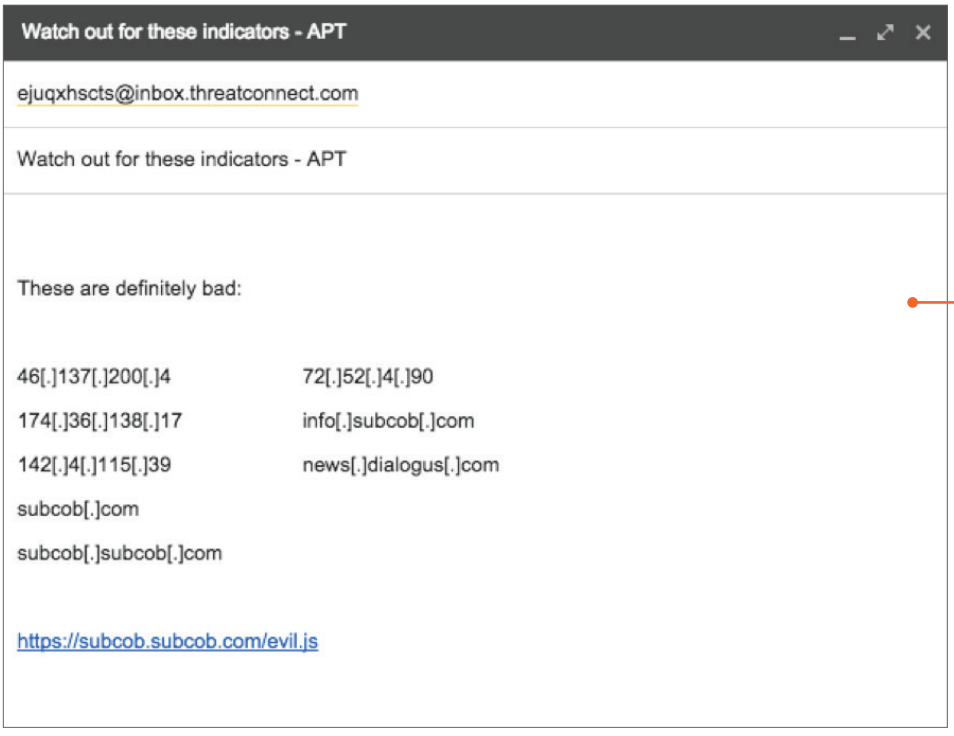
Setup a custom email inbox for threat intelligence email forwarding.



EASILY CONFIGURE MAILBOX

Sort and filter by type, indicator and feed. Set confidence level, rating and threshold, to keep threat data organized and accessible.

When an analyst forwards an email into ThreatConnect for threat intelligence triage analysis, the email is not treated as a trusted source; rather, it is a suspect source that is scored for maliciousness, memorialized with context, and correlated for further context.

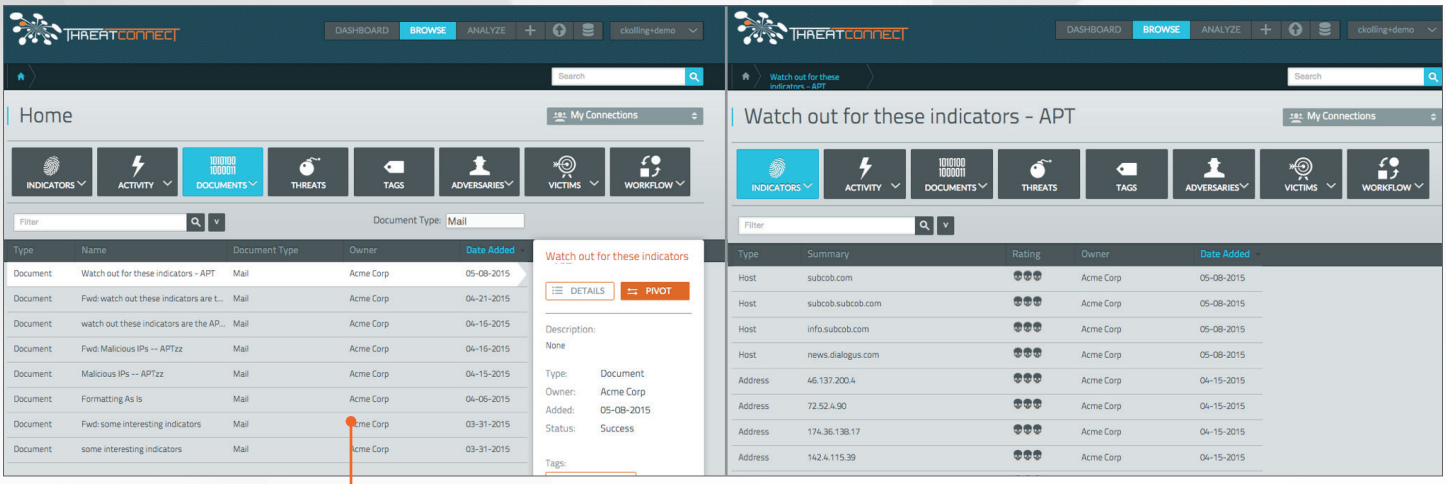


EXAMPLE INDICATOR EMAIL

Sample 'defanged' email. Note indicators of compromise for advanced persistent threats.

If an email forwarded into ThreatConnect is determined to be suspicious, an automated alert can trigger its forwarding to a designated person, who can then mitigate the threat by working with the original recipient, cleaning up malware, warning users and executives that the organization is being targeted, etc. The newly-collected intelligence can be used to help develop future responses to similar threats.

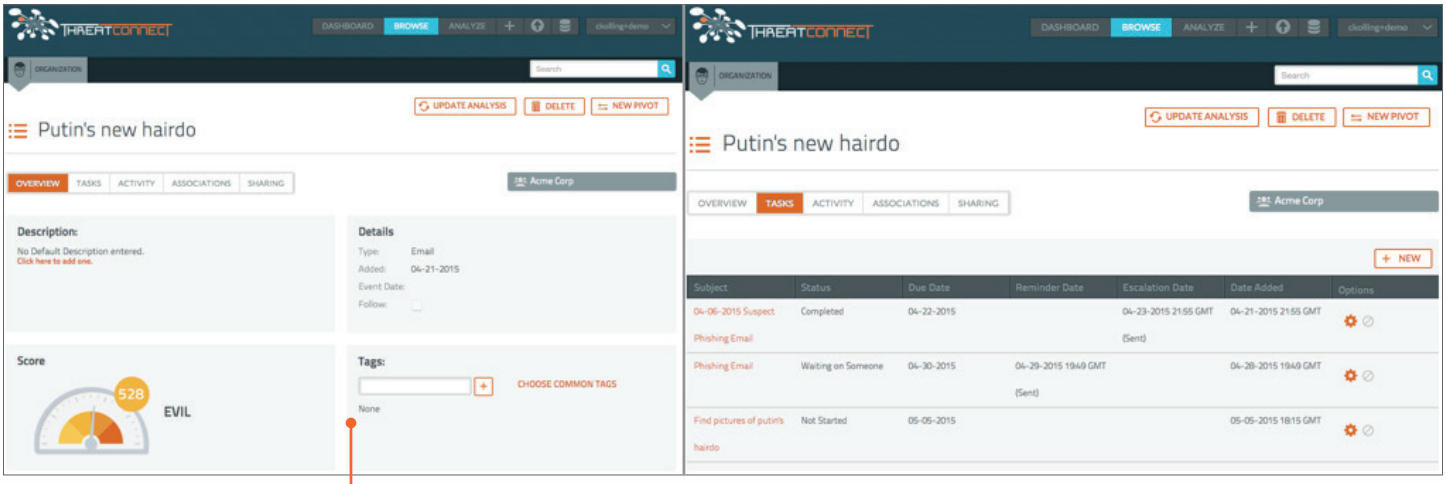
ThreatConnect eliminates the risk that a regular inbox full of malicious emails would present. First, emails forwarded into the TIP are deactivated ('defanged') to prevent accidental clicks. Also, even emails that come from trusted sources are stored as objects, rather than as emails. Even though an analyst is working with the document rather than the original email, he has access to the email's full context. He can pivot on any document to see the indicators that were in the original email and he can correlate those indicators with other sources that are known in ThreatConnect. He can also see which indicators were known to the community at large, as well as the incidents and attributes associated with them.



SORT AND PIVOT

Each email is saved as a document within ThreatConnect. Expand to see details, indicators and threat data. Pivot on the indicator data and identify where within the platform this threat had been seen before.

The TI analyst has many automated tools to help him work with a suspicious email. Custom tasks can be set to direct the suspicious email to any analysts who need to handle it. Tasks can be scheduled, deadlines set, and escalation processes defined. Feed inboxes can be set to include a default rating and confidence score. Many other settings can be customized by using ThreatConnect's library of regular expressions, or custom regular expressions can be written and applied. Automated incident response support is enabled by correlations that help track suspicious emails and associate them with common adversaries. An analyst can initiate a pivot of the email against other intelligence, and he can use an API to push the intelligence into a SIEM, such as Splunk™ or ArcSight™.



IDENTIFY AND ACT

Explore the source, score, address and details of the threat. Workflow features enable teams to collaborate, and take action to counteract the threat.

Objects with ThreatConnect are fully searchable by elements such as email addresses, domains, URLs, or rule-matching. Once found, an overview screen displays header information, scoring, and other intelligence. An analyst can drill down into the analysis to see how it was performed and he can add to it by importing data that was not previously known to ThreatConnect.

EMAIL EFFICIENCY FOR AN AGILE COMMUNITY

According to Gartner, organizations can improve their agility and efficiency by harnessing email, both as a source of threat intelligence and a means of sharing that intelligence. ThreatConnect incorporates built-in email functionality into its community-driven TIP, delivering a solution that meets the challenges of today's escalating threat landscape. ThreatConnect helps TI analysts operate more efficiently and enables organizations to take a proactive stance against their enemies.

WORKS CITED

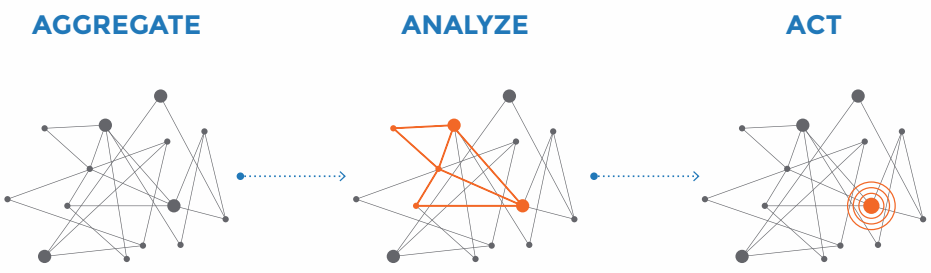
Lawson, C., & McMillan, R. (2014, December 10). Technology Overview for Threat Intelligence Platforms. Retrieved April 10, 2015, from Gartner.com: https://www.gartner.com/doc/2941522/technology-overview-threat-intelligence-platforms

Ponemon Institute. (2014, April). Exchanging Cyber Threat Intelligence: There Has to Be a Better Way. Retrieved 10 2015, April, from Iinternetidentity.com: http://content.internetidentity.com/acton/attachment/8504/f-001b/1/-/-/-/-/Ponemon%20Study.pdf

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.



CONNECT WITH US

Interested in learning more about how ThreatConnect can help unite your security team and protect your enterprise?

www.ThreatConnect.com

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

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550
Arlington, VA 22203