THREATCONNECT™

Prepared Testimony and
Statement for the Record of

Richard Barger
Chief Intelligence Officer, ThreatConnect, Inc.

Hearing on:

"Federal CyberSecurity Detection, Response and Mitigation"

Before the

House Committee on Oversight and Government Reform
Subcommittee on Information Technology

Chairman Hurd, Ranking Member Kelly, and members of the Subcommittee, thank you for the opportunity to appear before the Committee today.

My name is Richard Barger, and I am the Chief Intelligence Officer and co-founder of ThreatConnect, a Virginia-based cybersecurity company. I lead a research team dedicated to understanding existing and emerging cyber threats to ensure our software platform equips organizations to conduct intelligence-driven security operations. Prior to ThreatConnect, I served as a U.S. Army Military Intelligence Analyst and supported customers within the Department of Defense and Intelligence Community as a civilian.

ThreatConnect, Inc. was founded in 2011, and our platform launched in 2013. Since then, we have seen 40% of the Fortune 100 use our software, as well as more than 9,000 global users. We have amassed details for more than 55,000 security incidents and 3,500 threats which consist of more than 3.5 million indicators. From our inception, we have committed to and offered a free cloud-based edition of our ThreatConnect software platform so everyone has the opportunity to collaborate and simplify the challenges of cybersecurity.

Today my testimony will focus on the concept of fragmentation as the root cause behind our continuing struggle to detect and respond to cyber threats in both the public and private sector. The four key areas I will discuss are **people, processes, technologies, and community.**

Fragmentation

ThreatConnect customers within both the public and private sectors often express the same problem in different ways: fragmentation across their security operations is both their biggest frustration and their biggest risk. Whether they are a global financial services firm, a North American oil and natural gas company, or a federal agency, the fissures that exist across people, processes, and technologies create footholds into our networks that allow malicious actors access to our finances, sensitive personal data, and corporate intellectual property.

Security is difficult work. There is no "easy button" or "silver bullet" solution. Today's defenders face the gargantuan task of protecting networks that were not designed with security in mind. Our defensive posture tends to be a reaction to the last threat or breach, which briefly focuses attention and resources on "doing more". As a result, we add another device or build another team. But this additive response exacerbates fragmentation.

The 2015 Verizon Data Breach Investigation Report[1] (DBIR) highlights that 60 to 90% of the time adversaries are breaching enterprises in days or less, but are only being detected in days or less 10 to 20% of the time. There is a huge gap of time between initial breach and response. Our own research validates the DBIR's findings, from sophisticated state actors who targeted the Office of Personnel Management[2] as well as entities with strategic diplomatic and strategic interests in the South China Sea.[3]

Our efforts over the past decade - new authorities, laws, advancements in technology, increased security investments - are not making much of a difference against this detection deficit. This is where I believe we are coming up short: our innate inability to evolve our respective security resources into an organism that can intelligently orchestrate its own defense. Focusing on a constantly evolving threat landscape distracts us from the realization that we are our own worst enemy.

Fragmented Security Teams

As we increase the number of individuals and teams required to work together, organizational agility, transparency and situational awareness often suffer, making us our own worst enemy. More people may be necessary, but it is no longer possible to play "man-to-man" defense in information security. Effective zone defense requires investments that allow people to efficiently prioritize, triage, memorialize, and share their findings. Too often an organization's expertise and institutional memory is scattered across diverse teams, shared drives, and emails, often rendering it functionally inaccessible. Reducing the fragmentation of security teams is just one of the hurdles that we at ThreatConnect are helping the industry clear by giving

---

[1]http://www.verizonenterprise.com/DBIR/2015/
[2]https://www.threatconnect.com/opm-breach-analysis-update
[3]https://www.threatconnect.com/camerashy/

the experts a secure place to work together, so that everyone benefits from their collective knowledge and talents.

Fragmentation also exists across executive staff, C-suites and Boards. There is a communication deficit, which negatively impacts leadership's ability to interpret and prioritize core organizational challenges and subsequently leads to ineffective decision making. Effective communication, increased transparency, and shared situational awareness across a variety of stakeholders is a key center of gravity that we recognize and where we are investing to help organizations achieve greater efficiencies in the face of increased risk.

Fragmented Processes

In terms of security processes, there is no one-size-fits-all approach. Enterprises are like snowflakes: made of the same elements, but uniquely configured. Different business objectives drive different business processes, and multidisciplinary security operations reflect a company's overarching sector, vertical, legal and regulatory requirements. Combined with the growth of security teams described earlier, this is a recipe for fragmentation. Examples abound such as a vulnerability management team failing to coordinate a list of unpatched assets with the Security Operations Center (SOC) or the SOC escalating a series of suspicious events to those assets without including required information for the incident response team.

Intelligence-driven security needs to become the focus as practitioners grapple with a tangle of these siloed processes built around different teams and technologies. It is much easier to define, measure, and advocate for the resources required for a new tool or new headcount; optimizing processes seems mundane and intangible by comparison. But this is the dirty little secret: developing coordinated intelligence-driven processes is the linchpin to identify, protect and respond to threats in an efficient, measurable way. This is one of the most powerful value propositions for our customers, but also one of the most difficult to explain. At ThreatConnect, we are helping global organizations master their own processes and in-house data and complement it with external threat data to proactively identify threats before damage occurs. As these organizations build confidence and gain comfort, they begin to adjust some of those other siloed processes - incorporating them into this newfound knowledge base and fine tuning so they can put their energy where it matters most.

Fragmented Solutions

We have engaged with security teams worldwide, and they often highlight that they spend an inordinate amount of time struggling with their various security solutions, such as perimeter or endpoint controls. Today's practitioners expect these solutions to deliver "breathing room" to the organization and create measurable efficiencies, not consume additional organizational resources. Unfortunately many of these solutions are created in a vacuum and simply are not designed to be interoperable. This is where the industry feels the pain of fragmentation the most. Practitioners feel they are in the business of wrangling these solutions, rather than actually securing their organizations. This is why we place so much emphasis on the need to bring the power struggle between man and machine back into balance.

By replacing fragmentation across security teams, security processes and security solutions with orchestration, we begin to align the disparate parts of security operations. This concept of orchestration is

not a new notion for those in the public sector familiar with Command & Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR). But this is a significant doctrinal shift for private sector enterprises very much rooted in traditional fragmented security practices. Today we see a growing hunger in industry for solutions to these fragmented practices. Even if an organization is only starting to recognize foundational C4ISR principles such as centralization and coordination are key, they still instinctively understand how reducing fragmentation will have an impact. From our work with organizations around the globe, we understand that to be effective agents of change we need to enable security operations to be integrated, orchestrated, and supported by intelligence and interoperable defensive solutions. This is the combined arms approach that allows the sum of the parts to yield mutually supporting effects against threats.

Fragmented Community

At ThreatConnect we see information sharing as a key tenet to overcoming the challenges of fragmentation between today's siloed security organizations. At the core, information sharing is less a technical issue and more of a cultural issue. As practitioners, we have either participated in or maintained a multitude of private researcher-sharing communities, all of which have their own unique focus areas, memberships, and respective value proposition. Within the 2015 Verizon DBIR, ThreatConnect contributed metrics associated with various types and levels of sharing that occurs within our platform, reinforcing that individual sharing communities are often unique. They vary in topical focus areas, member experience and size; some individual participants share more frequently than others; and some share content that is arguably of more value than others.

Ironically, we encounter many organizations that lack effective information sharing practices within their own organization, where privacy and trust should be more abundant. It is then not surprising that some will try to put the cart before the horse and navigate the complexities of institutionalized external sharing. Organization to organization information sharing continues to remain an "*advanced move*" for many as an official corporate practice. Today, sharing is fragmented and often occurs under the radar of executive or legal staff, primarily happening informally at the individual practitioner level. Sharing in this manner has its advantages: it is often quicker, more frequent, and the information shared is often of higher quality than what is found in bulk via the more formal information industry sharing programs. However, that approach is not scaleable.

The passing of S.754, the Cybersecurity Information Sharing Act of 2015, has renewed focus on information sharing. S.754 is a step forward for our industry, but remains very much focused on enabling technical, atomic indicator-based sharing with the Department of Homeland Security (DHS). ThreatConnect remains committed to supporting initiatives such as DHS's Automated Indicator Sharing (AIS), but we also look forward to working with DHS and others to evolve today's baseline sharing practices toward a broader goal of cross-sector coordination and collaboration.

In our view, atomic indicator sharing is a useful first step in fostering a sharing culture, but those indicators are highly perishable. Unless sharing happens in near real-time, the value of those indicators deprecate quickly. Indicators of compromise are the tactical bits of our business, but we have to evolve collaboration to include sharing the "recipes" or the process by which the indicators were created in the first place. This

requires a foundation of trust across the stakeholders, which is largely established through day-to-day operations and social interactions. There is no better way to establish trust than rolling up one's sleeves, planning, and working through a problem together. It is here that we foster lasting trust and democratize domain knowledge and expertise for the long term - the type of information sharing that lasts decades.

Final Conclusion

It is said that "*necessity is the mother of invention.*" ThreatConnect was created with a desire to fill such a necessity that I and my co-founders witnessed first-hand supporting the Department of Defense and various intelligence agencies. The "detection deficit" I mentioned earlier highlights that despite a decade of best efforts, we are not improving. The gap between compromise and detection is clearly not closing, which is why we are working to reduce the thorny reality of organizational fragmentation across public and private sector security operations. Without closing that gap, we continue to be our own worst enemy, and we cannot expect to be effective in detection, response and mitigation

Across a spectrum of threat actors driven by ideological, criminal, or espionage motives, the internet knows no borders. Yet everyday the global market expects security and privacy to be easy, ever present, and to simply work. Irrespective of sector, security continues to be an achilles heel for many organizations due to the types of fragmentation issues we've highlighted here. The disconnect between expectation and reality is elevating enterprise security to become a more prominent and central fixture within the corporate structure. This rise in priority must continue and organizations must be incentivised to look at enterprise security as a critical business function. Information sharing initiatives must transcend cross-sector coordination and collaboration. The security professionals of tomorrow must be educated and enabled to scale to the current demand for talent.[4] The market must drive the need for interoperable security technologies.

By solving the challenges that we find at the seams, we can begin to reduce the effects of fragmentation between our organization's people, processes, technologies.

Thank you again for the opportunity to testify before you today. I look forward to your questions.

[4] https://www.threatconnect.com/sending-aspiring-jedi-knights-to-the-dagobah-system/

THREATCONNECT™

Committee on Oversight and Government Reform
Witness Disclosure Requirement – "Truth in Testimony"
Required by House Rule XI, Clause 2(g)(5)

Name:

Richard M. Barger

1. Please list any federal grants or contracts (including subgrants or subcontracts) you have received since October 1, 2012. Include the source and amount of each grant or contract.

None

2. Please list any entity you are testifying on behalf of and briefly describe your relationship with these entities.

I am testifying on behalf of ThreatConnect, Inc. I am the Chief Intelligence Officer and co-founder at ThreatConnect.

3. Please list any federal grants or contracts (including subgrants or subcontracts) received since October 1, 2012, by the entity(ies) you listed above. Include the source and amount of each grant or contract.

See the attached supplement.

I certify that the above information is true and correct.

Signature: Richard M Barger

Date: 4/17/2016

Richard Barger
Chief Intelligence Officer
ThreatConnect, Inc.

Rich is a pioneer in threat intelligence analysis and is the Chief Intelligence Officer and co-founder of ThreatConnect. In 2011, Rich sought like-minded security experts, and together they founded ThreatConnect. Rich has more than 15 years supporting DC's most elite cyber defense and intelligence organizations from within both public and private sector as a former U.S. Army Intelligence Analyst and security consultant. Rich is an analyst at heart, and his technical and operational vision is truly what makes ThreatConnect a disruptive new technology for organizations worldwide. Rich leads the globally recognized ThreatConnect research team. Rich maintains a variety of professional industry certifications and holds a B.S. in Information System Security.

Supplement: Federal grants or contracts (including subgrants or subcontracts) received since October 1, 2012 by ThreatConnect, Inc.

Type	Prime Contractor	Contract	Client	Period of Performance	Funded Amount	Ceiling Value
Subcontract	Booz Allen Hamiliton	SIGINT Development Support (SDS) II	National Security Agency	1/1/2016 - 12/31/2016	Cumulative as Ordered	$3,715,000
Subcontract	Booz Allen Hamiliton	IT Supplies and Support Services: STOR22	Federal Bureau of Investigation	4/1/2013 - 9/29/2016	823636.16	$975,000
Subcontract	CGI Federal	ITA Enterprise Information & Mission Assurance	Department of the Army	9/30/2012 - 9/29/2014	351297.65	$351,298
Subcontract	DRS Technical Services	SITEC Tower VI (SOCEUR)	U.S. Special Operations Command	7/15/2012 - 7/15/2016	373400.66	$500,000
Subcontract	General Dynamics	SITE Information Assurance/Computer Network Defense	Defense Intelligence Agency	9/16/2011 - 9/15/2016	636114.38	$3,656,112
Subcontract	Northrop Grumman	Air Operations Center Weapn Systems Modernization (AOC)	Air and Space Operations Center, USAF	1/16/2012 - 9/30/2013	620400	
Subcontract	Northrop Grumman	U.S. Computer Emergency Readiness (USCERT)	Department of Homeland Security	4/1/2015 - 3/31/2020	210608.12	$1,000,000
Subcontract	Network Security Systems Plus	SPAWAR Computer Network Defense & Information Assurance Support	Department of the Navy	8/2/2012 - 12/4/2015	Incrementally funded	
Subcontract	Leidos	National Security Agency Threat Operations Center Analyst (NANA)	National Security Agency	10/1/2010 - 9/30/2019	4337063.83	$4,337,064
Subcontract	SRA International, Inc.	CITS	U.S. European Command	3/1/2011 - 1/31/2013	864479.75	$1,601,264
Subcontract	SRA International, Inc.	J36	U.S. European Command	9/13/2013 - 7/22/2014	673599	$1,000,000
Subcontract	SRA International, Inc.	CITS II	U.S. European Command	7/23/2014 - 5/31/2016	2062846.24	$4,715,210