the cyberwire

The CyberWire
621 East Pratt Street, suite 300
Baltimore MD 21202–3140
editor@thecyberwire.com
www.thecyberwire.com
@thecyberwire

SINET 16

December 3-4, 2014 Washington, DC

December 3

The Security Innovation Network (SINET) opens its 2014 Showcase 2014 at noon today. We'll be live tweeting from the conference, which is made possible by a partnership between SINET and the Department of Homeland Security Science and Technology Directorate.

The showcase highlights the SINET 16, "'best-of-class' security companies that are addressing industry and government's most pressing needs and requirements." This year's class includes (in alphabetical order) Click Security (advanced threat detection), Contrast Security (continuous application security), CrowdStrike (technologies and services focused on identifying advanced threats and targeted attacks), Cylance, Inc. (artificial intelligence, algorithmic science and machine learning), Cyphort, Inc. (advanced threat protection), GuruCul (security risk intelligence), Interset (insider and targeted outsider threat detection), Norse Corporation (live attack intelligence), PFP Cybersecurity (threat detection), PhishMe, Inc. (threat management for advanced targeted attacks), Pwnie Express (asset discovery, vulnerability scanning and penetration testing), SecureRF Corporation (cryptographic security for wireless sensors, embedded systems and other devices), Shape Security (advanced dynamic defense against malware, botnets and scripts), Skyhigh Networks (cloud visibility and enablement), vArmour (data center security) and ZeroFOX (social risk management).

The Showcase will also be accompanied by workshops covering topics of particular interest to security entrepreneurs: perspectives on research and development, cyber threat trends, and emerging tactics, techniques, and procedures for defending the enterprise. We expect today's session to close with a presentation from Cylance on "Operation Cleaver," the extensive Iranian cyber campaign that the company says it has uncovered. Operation Cleaver appears to be currently in its preparatory phase, with reconnaissance and compromise being the immediate goals.

Today's sessions covered much interesting ground. We'll summarize two of the longer presentations here: Martin Brown's advice for security startups, and Stuart McClure's presentation on Operation Cleaver.

Martin Brown, Chief Security Architect, BT Security Enterprise, advised startups on how to approach large enterprise customers. His title – "But, my security product is AWESOME! Why don't you want it!?") – suggests the challenges involved in breaking into the managed security service provider market. Brown's role at BT requires him to scout emerging opportunities and technologies, and he offered his insider's perspective on what a large company looks for in innovative security products.

Entrepreneurs should understand that they're effectively selling into a company's ecosystem. Consider a company like BT. It's in one hundred and seventy countries, operates a significant number of SOCs, has some thirty thousand devices, etc. Security touches every aspect of BT's organization, and it has to work — it must be reliable. Brown suggested that security may usefully be thought of as having three aspects: 1) core, transactional security products, 2) proactive security, and 3) people and processes. A large but finite amount of data comes from core and proactive security technology. Those data must be looked at for content, context, and costs.

Selling to a large enterprise involves understanding this context (and, he noted, when you develop a product, develop it with the assumption that it will find its way into the managed service market). Pose, and answer, well-formed questions framed in such context. Don't just tell the customer that something on the network is bad – tell them why it's bad, and where it's bad.

Context is essential not only to developing a product, but also to deploying it. Managing a large enterprise can be very difficult. Make your system easy to manage within the customer's ecosystem, and be sure to explain the value of your product clearly. The customer can take you for granted if you don't show them your metrics of success, so do so in financial terms.

Brown observed that many companies fear losing their IP. He recommended that, on the contrary, the best use of your IP involves giving customers some insight into how you reach your decisions, and how your technology works. Without such information, the customer will be very nervous about automating their use of your product – and automation is inevitable, because it is the proactive layer of security, not the transactional layer, that makes decisions.

He concluded with a number of pieces of specific advice. Multi-tenancy is essential. Clients like BT need data separation and access control. You can't expect a customer to run a dedicated UI or server for each of their customers. Let your customers run scripts. Don't force them to install easily exploitable software. They don't want exploitable products in SOCs — no Flash, no Java, etc. Use easily authenticated RESTful APIs; your big customers will love RESTful APIs. Make your application easy to deploy. Try not to put it onto an appliance. You will need secure uploads for updating — no CDs for updates, please. Your customers test products before they buy them, so be prepared to submit your product for testing.

Brown concluded by emphasizing, again, that however innovative your technology is, it must fit the customer's ecosystem.

Stuart McClure, CEO of Cylance, presented his company's discovery of an extensive Iranian cyber campaign, "Operation Cleaver."

Cylance named the campaign because of the frequent use of the word "Cleaver" in the attackers' custom-built tools. Cylance noticed that similar — in some cases, identical — techniques and tools were appearing in disparate attacks targeting critical infrastructure globally. The list of victims reads like a list of the world's important infrastructure. The attackers were achieving shocking levels of access, and their intrusions were serious – even potentially lethal. In many cases, they'd achieved complete access to their targets' networks, as well as access to many ancillary accounts (like PayPal and GoDaddy).

Cleaver began in 2012. It appears that after Stuxnet, Duqu, and Flame, Iran realized its cyber operations needed to go beyond counting coup for the sake of the national ego — website defacements and the like, designed to show the world that the Islamic Republic was there, and capable — and move on to a genuine offensive capability. Shamoon was an early exercise of that capability; Cleaver is far more advanced. It revealed its Iranian origins through its involvement with particular subnets, in particular source and target pairs, and the extensive use of Farsi in its coding. Attribution rarely comes with a smoking gun, but Cylance is morally certain that the circumstantial evidence is compelling.

The Iranians don't attempt anything particularly exotic, but they're clever, capable, and have advanced a great deal. They use SQL injection, anonymous FTP for exfiltration (among other techniques), and some well-conceived spearphishing tactics. A big tranche of the data Cylance investigated came from airports and airlines in at least two different countries, and those data showed not only considerable information sharing among attack teams but also a disturbing interest in the physical environment surrounding air travel as well as the reconnaissance of particular individuals. (One target compromised, for example, was an airport security badging system.)

Cleaver, McClure concluded, is an active and actively tasked effort. It involves three-to-four teams with common direction, all sharing the information they develop.

December 4

The SINET Showcase wrapped up today, and so we wrap our coverage up with this issue.

Rick Geritz, CEO of LifeJourney, and SINET Chairman and Founder Robert Rodriguez opened the day's proceedings with an overview of cyber startups — their geographical location, their VC support, etc. — with particular attention to the United Kingdom's contributions to cyber security as they introduced the morning's keynote speaker, Richard Paniguian, who heads the UK's Trade and Investment Defence and Security Organization. Paniguian described the contribution of small enterprises and universities to a sound cyber security capability. He praised Anglo-American friendship as not only founded on common values, but as vital to global peace and prosperity. He singled out the onerous burden of compliance as a challenge (commending it to the attention of the companies and agencies in attendance) and closed with a call to more effectively communicate the value of security.

The keynote having been delivered, Doug Maughan of the Department of Homeland Security Science and Technology Directorate introduced the SINET 16. He emphasized the entrepreneurial nature of the cyber industry, pointing out that most of the companies who competed for the SINET 16 were not only small but very young as well. Each of the winning firms described their products, services, or solutions and the challenges they address. Their presentations were brief — held to just six minutes each — but unusually clear and informative:

Click Security said that traditional security isn't working — it's too slow. $70B is spent on infosec, but criminals take $250B, which creates an unworkable mismatch. Click Security wants to empower the human in the loop, turning analysts into decision-makers with Click Commander. Click Security's Click Commander's cycle is click, see, and prevail. The goal is to make it easy on the analyst.

Contrast Security notes that software is both pervasive and "stunningly vulnerable." Manual code reviews find some 22.4 serious vulnerabilities per 1000 applications. Software has outrun the ability of both experts and legacy tools used to vet it. Contrast Agent instruments sensors in applications for security visibility, enabling rapid, and accurate evaluation. This goes beyond both static and dynamic security evaluation, yielding a real-time security-scoring dashboard.

Crowdstrike described itself as "redefining next-generation endpoint security." Advanced threats bypass current solutions, overwhelming organizations and rendering them unable to address silent failure. CrowdStrike Falcon addresses detection, prevention, attribution, recording, and monitoring. It quickly deploys lightweight sensors on endpoint systems, detecting the unknown through Stateful Execution Inspection. It observes and tracks nations and criminal groups. The solution is cloud-scale, with no on-premises equipment required.

Cylance argued that, contrary to emerging conventional wisdom, enterprises don't need to give up on prevention. Algorithmic science is the key to restoring preventive defenses, and while that science is nothing new, it renders other approaches obsolete. Cylance's algorithmic approach incorporates context, and therein lies its innovation. Application of Cylance's approach yields next-generation endpoint protection.

Cyphort, whose slogan is "Target the threats that target you," described changes to the threat landscape and the rapid expansion of attack surfaces. First-generation solutions overload enterprises with data. Cyphort's platform deploys sensors and detects evasive malware. Its machine learning enables containment, its virtualized systems enable scaling, and a RESTful API fits existing ecosystems. In sum, Cyphort offers a heterogeneous detection platform.

GuruCul began by pointing out that, because defenses generate too many alerts to handle, enterprises are turning to log aggregators. This is problematic, however, because log aggregators don't capture the unknowns. GuruCul focuses on either the compromise or misuse of an identity — the root causes of many threats. GuruCul calls its approach "contextual identity." It deploys machine-learning algorithms to develop risk scores for identities within peer groups.

Interset focuses on surfacing threats before data loss occurs. It offers a self-learning, big-data platform that scores activity risk and identity risk mathematically. Their solution has obvious implications for, and use cases in, recognizing insider threats. Interset seeks to eliminate the noise in which such risk often hides; if you can identify highly risky behavior before data exfiltration, you can keep the data secure.

Norse presented actionable fusion intelligence. Norse is a global telecom that doesn't provide telecom services. With some 8M sensors deployed, they invite and analyze attacks, preparing enterprises for the cyber killchain by closing the intelligence fusion gap.

PFP Cybersecurity offers anomaly-based cybersecurity threat detection. They baseline systems, compare their state against that baseline, and thereby detect anomalies. PFP Cybersecurity's solution is scalable from endpoint to SOC, and is designed to cope with the fact that the bad guys are now inside the firewall.

PhishMe presented an approach to security that focused on managing human intelligence. 91% of cyber attacks start with spearphishing. We need to cultivate human attack sensors — human sources – the same way that the police do. Employees can act as attack sensors provided they're educated and equipped to be a source of intelligence. Through user training and tools ("a button on the email") PhishMe has shrunk detection time to seconds. The number of people who report are an order of magnitude larger than those who bite on phishbait. Mitigation is necessary (but not sufficient), and people can be conditioned not to click on dodgy links.

Pwnie Express was founded to solve the problem of remote security testing — thus the Pwn Plug. They've now built a network of Pwn Plugs. The next big problem lies in the Internet-of-Things (IoT), in particular "the Internet-of-Evil-Things." They want to help protect you against rogue actors with rogue weaponized devices, and Pwnie Express is actively looking for partners.

SecureRF focuses on securing the burgeoning Internet-of-Things. 28,638 new devices joined the Internet-of-Things in the six minutes that their presentation lasted. SecureRF designs sensors that can extend security to those computationally poor but data hungry IoT devices, with linear crypto technology that fits them. Use cases for their product include brand protection, secure chain of custody, secure supply chain management, authentication, and data protection.

Shape Security delivers a "botwall" that defends web applications against unwanted automation. Bots, which automate your web applications, are the modern threat and exact a high cost. Web applications are vulnerable because their source code is public. Shape Security uses polymorphism to change the attack surface. Real-time polymorphism takes a page from the attackers' book, using an evasion technique to disable the biggest threats.

Skyhigh Networks facilitates safe cloud adoption. They deliver visibility into shadow IT, and enable customers to understand the risks shadow IT poses. Users fall into shadow IT largely because they don't know better, and visibility into shadow IT facilitates breach identification. (In one case, Skyhigh found a Chinese APT using YouTube for steganographic infection of networks.) Skyhigh also provides data loss prevention and identifies compromised accounts. (And they offer free assessments.)

vARMOUR is a distributed data center security solution — data security for the data-defined network. They offer a single logical system for distributed security, a completely independent

layer to detect and remediate threats. Their use cases include internal segmentation, third-party separation, and East-West threat management.

ZeroFOX is a social-risk mitigation company. Social media have introduced a new security paradigm: users, not systems, are in the attackers' crosshairs. Three-fourths of Internet users actively use and routinely trust social media. Yet social media tend to be invisible to IT teams. ZeroFOX combats targeted phishing, social engineering, fraud, and impersonation. They provide live social threat intelligence, with real-time alerts and automated remedial actions customizable to an enterprise. ZeroFOX offers a way of not only reporting but also quantifying risk.

Wiliam Evanina, National Counterintelligence Executive spoke on integrating counterintelligence, security, and information technology. He highlighted three current areas of emphasis: security clearance reform (the government wants to tighten reinvestigation, and is looking for solutions), insider threat mitigation (with the goal of deploying a robust program across the government) and damage assessment. This last area, he noted, is a non-trivial problem. What damage, for example, did Snowden do? This remains unclear.

Richard Baich (EVP and CISO, Wells Fargo) framed the concept of network vulnerabilities in terms of a home-security metaphor. Much security is basic, not advanced. It's tempting to chase the innovative and advanced, but we must do this with caution — don't do so at the expense of basic security hygiene. To decide which risks to address, consider what's valuable to your enterprise. Security vendors should consider the skills gaps in customers, and design products that don't demand scarce expertise. In answering a question, Baich noted that large enterprises need help understanding what indicators were significant and developing intelligence that would let them know where to concentrate security resources.

An afternoon panel took up the characteristics of "minimal product viability." To find a place in the market, security products must be open. A clean, appealing, and functional user experience is vital. Viable products are easily installed and tested. They must clearly solve a customer's problem. And finally, startups selling a product need to ensure an early adopter that they'll still be around in twelve months.

Jerry Archer, Senior Vice President and Chief Security Officer at SallieMae, and also a founding board member of the Cloud Security Alliance, spoke about "securing the Internet-of-Everything." The cloud, he argued, will dissolve, and is already dissolving, into a pervasive mist. We're seeing transducers collecting 90 zetabytes of information, and transducers take action. Data will be collected, and things will happen for you, to you, and about you.

He illustrated this with a long (and, in truth, rather spooky) discussion of smart toilets, and the healthcare information they'll collect on their users. This he followed with a meditation on the legal implications of data collection, with smart cars providing the example. If your car is going to testify against you, does it have legal rights? Can your car serve you up to the state troopers if it determines that you're impaired? And airliners, of course, are also increasingly connected. What happens when a terrorist gets into this data stream? Or consider power plants, which, including nuclear power plants, are both connected and complex. Nuclear plants rely on commercial software that is not tested as rigorously as nuclear systems historically have been. Their very complexity can cause errors to cascade into disasters. The Internet-of-Things could also, potentially, drive human evolution. You could create something that would propagate at an astonishing speed, changing all aspects of human life. This has been the stuff of sci-fi horror, but it's no longer so farfetched. There's also an enormous economic opportunity in the Internet-of-Things — $19 trillion by 2020, says John Chambers — and this opportunity will impose a tremendous pressure to expand.

So, Archer concluded, we must reconceive security for the mist. Devices and applications must self-defend. New coding and testing techniques must be found. We must look at containment,

and so should think organically. All of us live with some degree of infection in our body; so, too, must our devices. Security professionals have to be involved with the mist – lack of involvement would be negligence. Mist systems will significantly influence who we are, what we are, and what we think. And there will be no opt-out.

Rick Geritz (LifeJourney CEO) led, with NIST's Bill Newhouse (head of NICE), a discussion of building the cyber workforce. NICE is particularly interested in helping define the cyber profession. Geritz discussed the importance of understanding that cyber security is cross-disciplinary, not merely an IT field. Students fail to conceive of careers in cyber security largely through a failure of imagination, and this can be redressed through proper ideation.

The SINET Showcase was an occasion for many productive conversations among those in attendance. We'll close by mentioning one the CyberWire had with Cylance CEO Stuart McClure, following up on his Wednesday presentation on Operation Cleaver. He had observed that, while interesting, attribution tended to be a mug's game. Why? Well, if you're an enterprise – particularly a commercial one – what exactly would you do with attribution? Is it likely to help you with prevention or mitigation? Perhaps in a few circumstances, and to a degree. But, unless you're a government worker — "someone with a badge or a gun," as McClure described them — what exactly are you going to do to the threat actor you've found in your network?

In any case, an interesting story of attribution is presenting itself this week — see the links below. Those of you with badges and guns, please discuss.

the cyberwire

editor@thecyberwire.com
www.thecyberwire.com

@thecyberwire
+TheCyberWire

About The CyberWire

The CyberWire is supported by CyberPoint International and its community partners. We invite the support of other organizations with a shared commitment to keeping this informative service free and available to organizations and individuals across the globe.

Revised 8.4.15