VECTRA
SECURITY THAT THINKS.®

HACK THE BUILDING BRIEF

DreamPort/MISI Hack the Building to support U.S. Cyber Command

Taking place Nov. 16-19, 2020, CYBERCOM/DreamPort Hack the Building (HTB) is a Department of Defense-inspired exercise, where technologies compete and demonstrate the impact of cyberattacks against critical building automation and mission operations. As the only program of its kind, HTB is a critical initiative to our national security. Vectra was the showcase solution supporting detection capabilities, detecting threats with AI-driven machine learning in real time and enabling rapid responses by the blue teams onsite.

About Hack the Building

Maryland Innovation & Security Institute (MISI) and DreamPort assembled the brightest minds in the intelligence, defense, academia and cybersecurity industry into a four day red team vs. blue team real-world exercise. The HTB event was inspired by a request from U.S. Cyber Command to implement a full array of IT, IoT, and operational technology (OT) environments for a full attack simulation. In the end, roughly 35 offensive red teams and 15 defensive blue teams supported the exercise both onsite and remotely, adapted to accommodate COVID-19 safety measures.

By applying AI-derived machine learning, Vectra categorized 52 critical hosts and 59 high-risk hosts.

Hack the Building is critical to national security, with Vectra being the only solution supporting Network Detection and Response.

The Team: Vectra Federal and Red Alpha

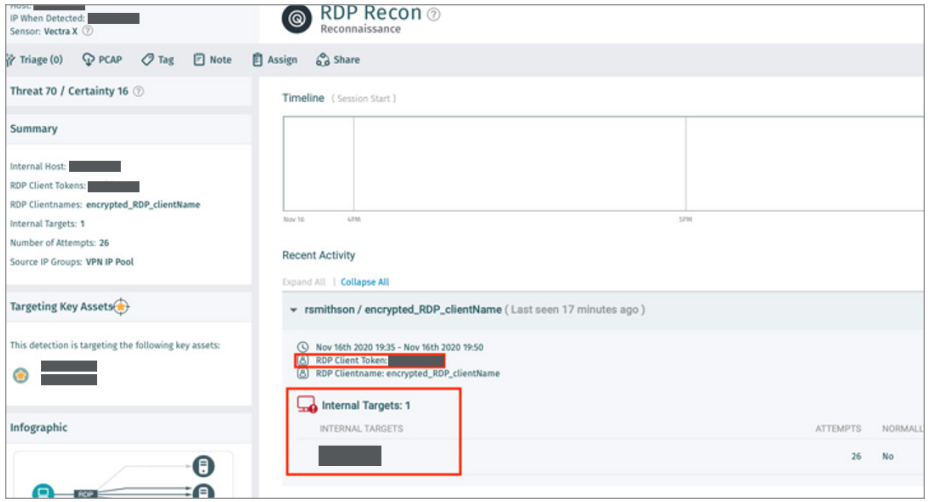
Vectra Federal Security Engineers and Red Alpha's industry-leading threat analysts and security architects combined resources to provide an unparalleled capability. Onsite in Annapolis, the Cognito network detection and response (NDR) platform supported Cognito Detect, which uses AI-derived machine learning to identify and respond in real time to cyberattack behaviors inside the network infrastructure. Cognito Stream from Vectra was also deployed to deliver enterprise-scale network metadata enriched with security insights to empower threat hunting, incident investigations, and the interface to the HTB Elastic and ELK environments. Vectra was provided with a full SPAN from the MISI packet broker to ingest all of the various network segments and remote VPN users. In the spirit of sharing, Vectra provided government teams with access to the Cognito Detect dashboard to leverage for their threat hunting, detection and response activities.

Overall, the Vectra team collected over 400 attacks onto the environment. These consisted of subsets of recon, lateral movements, smash-and-grab, data exfiltration, and command-and-control activities across the IT, control systems, and cloud assets.

As shown in the Cognito Detect dashboard from Vectra, the attack surface was quite large, and Vectra was able to apply AI-derived machine learning into the environment to categorize 52 critical hosts and 59 high-risk hosts, on which the blue teams focused efforts. Vectra then teamed up with two soldiers who quickly took to the user-friendly nature of the Cognito NDR platform; the soldiers began feeding detections to the blue team Discord Channel, while calling out the red teams for their activities in real time.

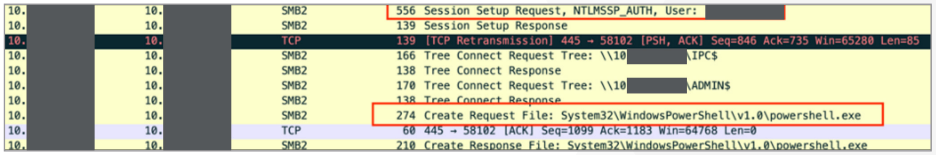
Timeline of an Attacker (attackhost1 10.xx.xx.xx Example)

Cognito Detect from Vectra immediately began to notice RDP-based recon activities from host attackhost1 at 7:35 p.m. on the first evening, targeting Host 10.xx.xx.xx on the BCR Industries mock defense network. The host then began an attack from multiple external clients to gain guest and VPN access into the environment. The Cognito Detect dashboard lit up in real time with the detection. This allowed the Vectra/Red Alpha/Military team to watch the attacker as it attempted threat activities while Vectra anticipated the next targeted move.



The Cognito Detect dashboard lit up in real time with the detection; this allowed the Vectra/Red Alpha/Military team to watch the attacker as it attempted threat activities and Vectra to anticipate the next targeted move.

The micro-PCAP data from Cognito Stream showed remote code execution via Windows PowerShell.exe and led the team to patient zero (remote user on 10.yy.yy.yy).



The micro-PCAP data from Cognito Stream showed remote code execution via Windows PowerShell.exe and led the team to patient zero (remote user on 10.yy.yy.yy).

Vectra security engineers were then able to locate continued suspicious activities by patient zero immediately after the initial compromise. From this point, Vectra and the team monitored the threat activities and continued to make traige notes of the events and notify the active blue teams about the detections.

Attacker Remediation

In a real-world scenario, Vectra works in conjuction with the SOC tools to provide automatic alerts about the access of the users from an account and network perspective. Upon the first indicator of the attackhost1 takeover, Vectra integrations via NAC and SOAR platforms would be utilized to remove user access, enhance ACLs to limit impacts, and automatically deactivate the account with Vectra Active Directory/LDAP integrations. In this exercise, no alterations to the network were permitted. However, detections were moved from automated response/enforcement to a notification/traige activity.

In addition to the use-case above where Vectra observed an entire attack from recon, lateral movement, remote execution and command and control, hundreds of other activities were observed in real time via AI-derived behavioral machine learning methods. Security that thinks is not just a tagline at Vectra, but a promise to government customers and partners that the best protection comes from intelligence and the thoughtful application of advance AI that legacy signature-based and NetFlow solutions cannot address.

Subsequent Activities

Vectra Federal and Red Alpha continue to support the missions impacting our national cybersecurity concerns with an innovative approach. In an ideal situation, Vectra would have also deployed the native Microsoft Office 365 collaboration tool that detects account compromises, lateral movement, and other capabilities as over 40% of organizations with Microsoft Office 365 experienced account compromises in 2019. Malicious cloud-based privilege escalations, credential access, lateral movement, and command and control are top concerns for Federal agencies and defense contractors in these environments. As we see a continued push towards CMMC across the community, ensuring all environments and systems receive proper controls with a singular view for SOC analysts, engineers and leadership will become even more criticical.

About Vectra

Vectra® protects government organizations in the cloud, data center, IoT, and enterprise by stopping data breaches. It was first to apply AI to automatically detect and respond to hidden attacker behaviors across the entire infrastructure, while enabling organizations to perform conclusive incident investigations and AI-assisted threat hunting. Using AI to collect, enrich and store metadata from all traffic, the Cognito® platform lets organizations respond faster to cyberattacks that evade legacy perimeter security controls.

About Red Alpha

Red Alpha is a small family of engineers established in 2010. Red Alpha is built upon five core values: Integrity, Collaboration, Learning, Innovation, and Customer Service. Our core competencies include: cyber security, cloud computing, enterprise web applications, mission critical large-scale systems engineering, and large-scale distributed/virtual systems administration.

For more information please contact a service representative at federal@vectra.ai.

Email federal@vectra.ai vectra.ai/federal