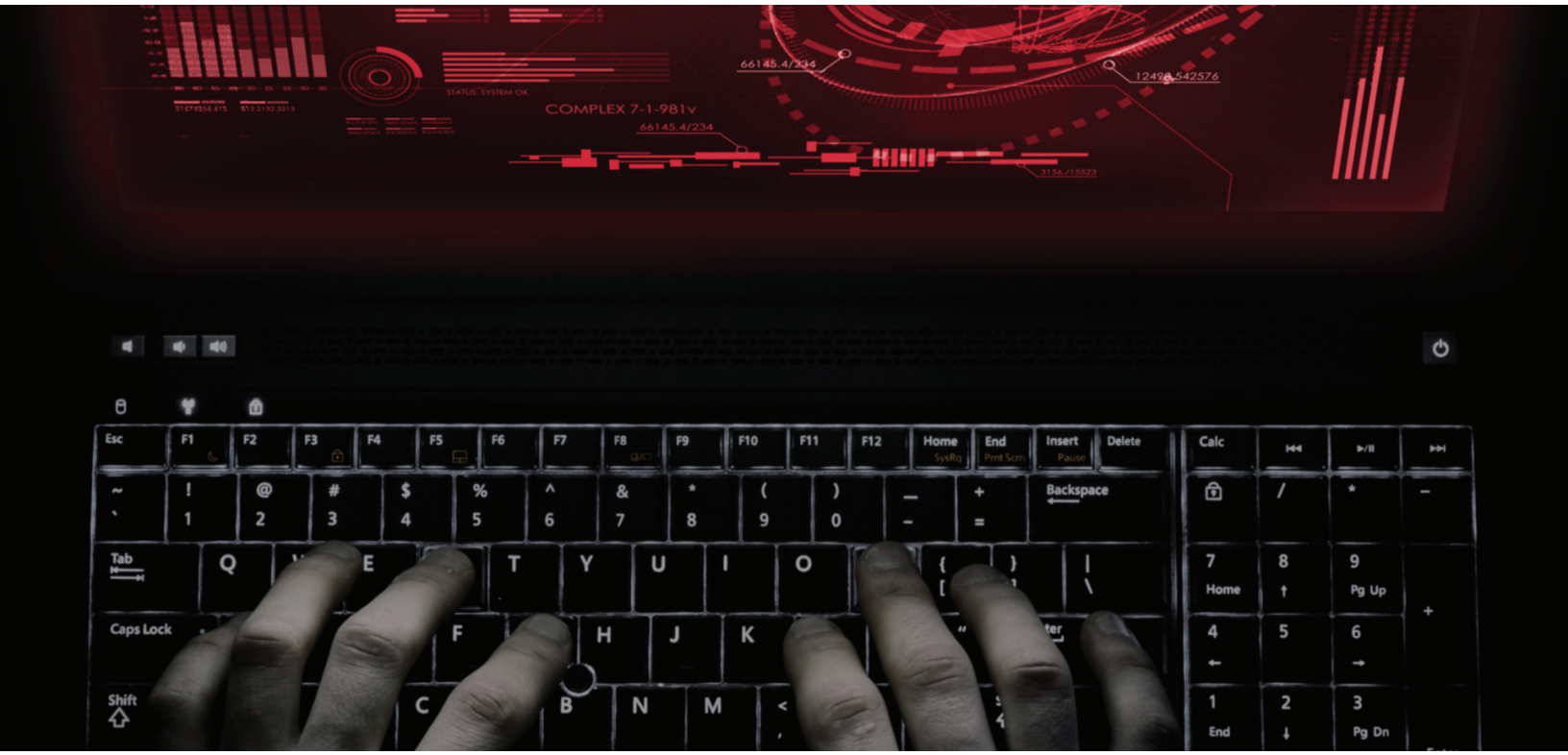
esentire®



Incorporating Hunt Teams To Defend Your Enterprise

How the application of military-grade investigative techniques can defend the network from cyber threats

Produced in partnership with Cognitio

Table of Contents

The Need for a New Approach in Operational Cyber Defense

The U.S. Department of Defense (DoD) operates the largest collection of networks and computers in the globe. Defending them against dynamic adversaries requires constant vigilance and continuous effort. This continuous effort has turned the DoD into a massive laboratory of innovation in cybersecurity, producing new concepts of use to the entire community.

The DoD has produced concepts like Incident Response, Defense In Depth, Malware Reverse Engineering, Red Teams, Penetration Testing, Deep Packet Inspection, Data Loss Prevention, and Cyber Threat Intelligence, to name a few.

One of the latest concepts to come from this laboratory of innovation is the concept of the Hunt Team, also known as an "advanced threat" or "advanced adversary" team. A Hunt Team is a group of operational network defenders skilled in the latest attack techniques, and how to defend against them.

As such, they are able to leverage network investigation skills and offensive counterintelligence, as well as knowledge of an organization's infrastructure, to find and stop adversaries who may be using zero-day exploits, advanced malware, or other covert means to infiltrate an organization's systems, and their mission is to seek out and stop the adversary, even those skilled at remaining covert.

This paper provides an update on the Hunt Team construct. We capture lessons from DoD, including insights from a key champion of DoD's Hunt Teams, retired General Ronnie Hawkins, USAF. We then conclude with actionable information and best practice recommendations any business should consider in their evaluation of Hunt Team options in order to find one that best fits the organization.

"A Hunt Team is a group of operational network defenders skilled in the latest attack techniques, and how to defend against them."

Background

History and current operations both make it very clear: when an adversary has an objective they keep trying. Good defenses can mitigate most risks, but sometimes an adversary or their malicious code will get in. Finding a covert adversary quickly requires a special breed of investigator, a hunter.

"A Hunt Team enables proactive monitoring to detect breaches, and well trained Hunt Teams can also accelerate incident response."

Today Hunt Teams are operating in some large enterprises in both industry and government especially in the intel and military branches. A Hunt Team enables proactive monitoring to detect breaches, and well trained Hunt Teams can also accelerate incident response and rapid implementation of countermeasures. Larger organizations establish their own Hunt Teams as part of their incident response teams. A recent trend has emerged where these best in class practices are now available as a service from what Gartner research has recently termed Managed Detection and Response[1] which are quite distinct from managed security service providers (MSSPs). Any business embracing best cyber security practices can now tap into trusted external experts to find evidence of adversary action.

The Hunt Team Construct

The DoD has long recognized the need for Red Teams, groups of good guy penetration testers and hackers who can test the security of operational networks form the outside. Red Teams help defenders understand weaknesses and contribute greatly to defense. Good Red Teams are like good adversaries in that they will not stop until they get in, except the Red Team will give you feedback on what to fix after they have gotten in.

The professionals who have spent time on Red Teams develop mastery of several offensive skills, including how to remain as covert as possible for as long as possible. The DoD leveraged these talents in their establishment of Hunt Teams. Who better to catch a covert hacker than someone who has been a covert hacker?

The Hunt Team construct has now evolved to an art form, where a high end team of skilled investigators is allowed to take a long view over data to look for signals or indications of adversary action. Internal Hunt Teams work across the existing security and network operations organizations, ensuring that data from the security operations center, forensics teams

1 Gartner Inc., Market Guide for Managed Detection and Response Services (May 2016), available at https://www.gartner.com/doc/3314023/market-guide-managed-detection-response

and network operations teams, as well as endpoint defenses, is shared and analyzed, with the objective of finding sophisticated adversaries and stopping a breach in process. Organizations utilizing Hunt Teams as a service generally have less sophisticated data collection capabilities and therefore rely on their service providers' advanced tools for creating the vast data sets necessary for effective hunting.

Hunt Teams can be expected to master highly specialized tools, such as full packet capture and network forensics which have proven to be invaluable at detecting embedded executables, behavior anomalies and full traffic replay much like a black box recorder. Additional capabilities also may include highly instrumented servers to detect filter access and movement, and honey pots or honey nets which are specifically set up to tempt and capture adversaries.

More importantly, the talents of very experienced professionals are used, and the brainpower of these sharp thinkers is employed to create and test methods to find and mitigate adversary action. The adversary always has first mover advantage and one of the characteristics of successful Hunters is get into this mindset. The best Hunt Team is made up of creative, quick-thinking professionals who have the persistence to find the adversary and to do what it takes to push them out.

"The adversary always has first mover advantage and one of the characteristics of successful Hunters is get into this mind-set."

The Mark of a Good Hunt Team

One of the pioneers of the Hunt Team construct is General Ronnie Hawkins, USAF retired, former Director of the DoD's Defense Information Systems Agency (DISA). We asked General Hawkins for his views on the Hunt Team, specifically what makes a good hunt team:

> ***"In my experience the Hunt Team requires something above and beyond. As you can imagine this must be a team that knows the technology and has experience in offense, defense and forensics investigations. I call this the science of the hunt. This is a professional team provided with continuous training following professional methods."***

Hawkins went on to say...

> ***"The operative word in Hunt Team is team! Hunt teams operate 24/7 in pursuit of enterprise objectives. Professional operations require teams that maintain and persist knowledge no matter who is on watch. The entire team is focused all the time on what it takes***

to win and this requires professional methods of turnover and persistently share situational awareness. Successful Hunt Teams are teams."

Hunt Teams and the Business World

Few organizations will have the means to establish their own Hunt Teams. The primary driver for this is an acute shortage of advanced cyber threat analysts (and there is no sign that this shortage will ever end). The clear trend is towards leveraging the kind of talent and tools that can only be provided by a highly trained and well-led cadre of cyber defenders who have chosen a career in operational cyber defense. More than likely, the Hunt Team an organization turns to for defense will be one provided by a service partner that has the ability to contextually enrich its data collection and can rapidly transfer the knowledge of the organization's infrastructure, applications, policies, trading partners and data.

"The Hunt Team becomes an extension of your organization and makes contextually informed decisions as though it were your organization making the decision."

One of the main differences between a Hunt Team from a service provider and an MSSP is that the Hunt Team becomes an extension of your organization and makes contextually informed decisions as though it were your organization making the decision. Whereas MSSPs are much more in the vein of business process outsourcers who generally deliver to contracted SLAs for daily report delivery, device management response time and security software patching – all of which are necessary. All too often Hunt Team service partner relationships form while your organization is under attack and they have been called in for an investigation and mitigation. In all cases, it's vital to think through selection criteria in advance, to save valuable time when a breach is actually in process.

Criteria for Team Selection

Any business seeking to leverage a Hunt Team whether creating in house or via a service provider should consider the following criteria:

- The team you select should be capable of operating 24/7 in your interest.
- Skills must include event detection, incident response including mitigation and incident investigation.
- The Hunt Team selected should have deep experience in the face of a wide variety of adversaries. They must know the cyber threat in detail.

This cyber threat knowledge will inform Hunt Team strategies.

- The team must have people with Red Team experience. This is critical to having the ability to think like an adversary.
- Hunt Teams must also have experience in defense, especially in the specific defensive tools leveraged by the organization being defended, including IDS, IPS, SIEM tools, proxy servers for decryption and packet capture tools.
- The Hunt Team should have their own tools as well. The most agile and responsive Hunt Teams will have solutions that integrate the best of signature, behavioral and anomaly detection and forensic replay abilities which are proving to be very useful when dealing with zero day exploits, but more importantly, they will have people skilled at working them.
- When leveraging a Managed Detection and Response Service Hunt Team, consider the architecture. Look for a hybrid architecture that enables the best use of highly qualified experts while keeping the most sensitive data inside your network.
- The Hunt Team should have the attitudes and approaches required for victory—they must have a mix of both creativity and persistence. As proof that they have what it takes, they will almost certainly have a long list of past performance to cite.
- The Hunt Team should have a formalized continuous learning process for mission debriefing and knowledge sharing especially when there are multiple locations and overlapping shifts
- There is really only one way to tell if the team is the right fit for the organization, and that is to talk to current clients of the team. Ask lots of questions, and focus on the most significant characteristic of a good Hunt Team: its ability to really perform against tenacious adversaries.

"The Hunt Team selected should have deep experience in the face of a wide variety of adversaries. They must know the cyber threat in detail. This cyber threat knowledge will inform Hunt Team strategies."

Conclusion

For many companies, it makes sense to use a Hunt Team provided by a third party. The time to evaluate potential partners for Hunt Teams is before the breach occurs, to shorten the time it takes to resolve a breach in process.

We recommend entering into discussions with potential providers now, in order to have the right team selected, mobilized and monitoring your traffic before a breach occurs. During the interview of potential providers, keep the list of criteria above in mind, and ask questions to ensure that the team selected is the best fit for the specific environment and needs of the organization.

"We recommend entering into discussions with potential providers now, in order to have the right team selected, mobilized and monitoring your traffic before a breach occurs."

About the Authors

Cognitio is a strategic consulting and cybersecurity firm established and managed by a team of senior technology executives from the U.S. Intelligence Community and the financial sector. Our accomplished team has a track record of safeguarding some of the nation's greatest secrets. We operate across multiple sectors of the economy an internationally to help firms assess gaps in cyber defense and build action plans to enhance their security and reduce the digital risk to business. We publish the highly read strategic cyber threat product The Daily Threat Brief, available at ThreatBrief.com

Contributors to this paper include:

Bob Gourley
Partner, Cognitio
Former CTO of DIA
DoD and Intel Community background. Cyber Intelligence assessments across multiple industries.

Roger Hockenberry
CEO, Cognitio
Former CTO of National Clandestine Service
Background in cyber Intelligence assessments and technology in and out of government.

Chris Ward
Senior Analyst, Cognitio
DoD and consulting background. Strong in enterprise IT including applying right tech to mission needs.

Bob Flores
Partner, Cognitio
Former CTO of CIA
Background in enterprise technology and cyber Intelligence assessments.

Chuck Hall
COO, Cognitio
Background in enterprise grade information technology and business leadership, especially in the financial and healthcare sectors.

David Highnote
Partner, Cognitio
Background in strategic consulting and cyber assessments across multiple industries.

About eSentire

eSentire® is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Protecting more than $5 trillion in corporate assets, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements.