Benefits of an Organized Cyber Defense

Juha Haaga
Solutions Architect

We operate in a world where cybercrime is typically well organized. The stereotype of an individual super hacker who is able to achieve everything by themselves to perform spectacular feats of crime and run away with the loot is a rare exception. The vast majority of cybercrime is actually performed by specialized groups. The groups buy and sell their specialized services to each other, from turnkey exploit kits to large botnets to money mules. They build up extensive criminal supply chains that are necessary for performing the large-scale cybercrime where the money is. Their time is valuable, so they optimize and spend it where they get the best return on investment.

As defenders, we are at a considerable disadvantage when we try to defend alone against the organized adversaries. One reason for this asymmetry is simply the availability of resources. For a small security team of an organization it is hard to match with the breadth of the capabilities that the organized adversaries have. The adversaries also have the advantage of attempting the same approach in parallel to multiple victims to find the one who has a weakness for the particular vulnerability that they can exploit. That unfortunate victim may well be you. How can the defenders also organize in a way that removes the advantages that the organized adversaries can pile up against them?

Defense cells help get organized

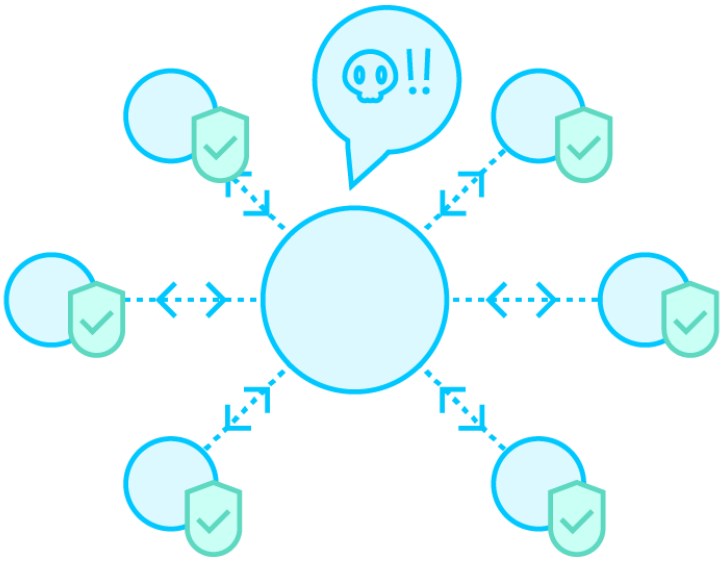
In this article, I will introduce the concept of cyber defense cells. Defense cells are organized groups consisting of actors that identify either as threat intel providers (Hub) or consumers (Node). Defense cell members share a common interest and engage in automated and targeted bidirectional threat information sharing. The goal of a defense cell is to help large amounts of organizations to organize in cyber defense and to share information and resources in an automated way that helps to scale up the efforts.

It is important to note that none of the activities of a defense cell mentioned in this article are new to the domain. Individually these activities are all currently being practiced in many different ways and in many different contexts, either by using existing tools and platforms or just talking and sharing information manually. What is new is to define this abstraction that lets us see the activities from a different perspective. Looking at organizing cyber defense at this higher level helps us to identify the driving motivations of the organizations who identify themselves with these roles. This is important because understanding their motivations further helps us to develop better strategies, processes, and tools to support the necessary activities for such defense cells.

Defense cells can be formed organically around existing Hubs that have a motivation to improve the cyber security of their stakeholders, or Hubs that seek to further improve their cyber security through the efforts of others around them. National CSIRT teams, domain-specific CSIRTs, and

ISAC/ISAO organizations are typical examples of Hubs, while critical infrastructure enterprises, government, and academia are typical examples of nodes. The primary motivation of the Nodes is to use the already existing resources for their own purposes and to extract maximum benefit from their existing investments into cyber security.

These Hub and Node roles are not strict, and some organizations may well be a blend of both archetypes. An example of this could be an enterprise that understands the value of the shared defense and sees themselves taking a leading role in their industry to achieve that. In this scenario they are both Nodes that consume threat intelligence to protect their own organization. At the same time they both act as a Hub that relays information between other members of the defense cell.



Key task of defense cell is to share threat intelligence

One of the core concepts of a defense cell is automated, targeted and low latency information sharing. Some national CSIRTs have actively shared automated threat and victim information in one direction for more than a decade. That kind of threat intelligence sharing is now becoming a standard practice and is a key capability for a Hub in a defense cell, but a lack of feedback in the sharing ecosystem is a limiting factor for realizing all of the benefits. When there are people in the equation, delays and latency become major issues in information sharing. and that also makes feedback less valuable. The automation perspective makes it clear that the defense cell members will need to start from sharing the information that is easy to work with without human intervention.

In a defense cell, this kind of information sharing needs to be targeted in a way that removes as

much as possible the amount of extraneous information for the recipient, and the information should always be actionable for the recipient in some practical way. Highly automatable information is plentiful, so getting started with this kind of sharing is not a problem. Avoiding inundating the recipients with unnecessary information is a much bigger challenge.

Information management is one of the main tasks of the Hubs. First, outside of the defense cell there is highly useful information that the members need to have access to. Thus, they first need to identify which information is useful to share to the members and then arrange access to that information. The purpose of a Hub here is to aggregate information from large amount of sources, and spare that work from the Nodes whose main interest is to consume it. The second task is to assist the other Nodes of the defense cell in understanding what kind of information the members have that would be useful to share. Consequently, Hubs help the members make that information available in a way that makes it easy for the others to consume. Here we should also look at how to make that information available through automation.

In a defense cell, this kind of information sharing needs to be targeted in a way that reduces the amount of useless information for the recipients, and the information that is delivered should always be actionable for the recipient in some practical way. The motivation to consume and use the received information is easily frustrated by providing information that requires a verdict or analysis whether it can be used in the Nodes environment. There is plenty of highly automatable information available for the Hubs, so getting started with this kind of sharing is not a problem. Avoiding to drown the recipients with unnecessary information is a much bigger challenge.

Information sharing can be arranged at human-to-human and machine-to-machine level, or it could be mixed. Because automation is a defining characteristic of a defense cell and the whole purpose is to scale this up to larger numbers Nodes, in a defense cell we first focus on the machine-to-machine level sharing, even though sharing between people may well already exist in parallel for some organizations. Creating a defense cell requires identifying the intelligence packages that can be shared without human intervention and then forming the links between the organizations to do so. Since our aim is large scale adoption, setting up the sharing between Hubs and Nodes needs to have as little friction as possible to be successful. The shared information needs to be simple enough so that it can be shared with different types of stakeholders without the need for the recipient organization to have trained cyber security experts to make use of it. Those experts don’t exist in most organizations, so we need to bring this information to the network and systems administrators who are already there.

Hubs and Nodes get situational awareness

Both Hubs and Nodes in a defense cell have a need for situational awareness of what is happening, with the difference that Hubs care more about the wider context while the Nodes care more about their internal situation. Information gathering is one of the primary functions in a defense cell. When normalized that collected information can be it also provides rich material for generating practical awareness of what is happening. By combining this collected information with feedback from the other members of the defense cell in an automated way it leads to a powerful capability to observe what is happening within the defense cell. The feedback between

Hubs and Nodes can be sightings in the most basic form, but also new intel that is related to the received indicators and valuable to other members of the defense cell.

In summary, thinking about cyber defense in terms of the defense cells helps us see how the members can organize, and how they can communicate with other cells through the Hubs. Once an organization understands their role in the defense cell, it becomes clearer which activities contribute to the collective defense and what they can expect from their peers. When we look at the motivations from the scaling and automation perspective it helps us see the important points for implementing this in practice. We identify the key benefits: up-to-date threat information that reaches to larger group of defenders and to make use of the existing resources that are already there to make those organizations more robust. We can minimize the use of the precious human resources and reap the benefits of a network effect in situational awareness through the feedback.