BLUVECTOR®
A COMCAST COMPANY

Conducting a Network Threat Assessment

Companies commonly call in external threat assessment teams to evaluate their systems as part of incident response, compliance audits, and similar activities. These external evaluators do not own or operate these systems or have any knowledge of the environment.

This relationship to the organization can create challenges for the assessment team. Here, we discuss common barriers, their sources, and best practices for overcoming them.

Common Barriers to a Successful Threat Assessment

External threat hunters are outsiders brought in, often by higher management and at short notice, to assess an organization's security. Many of the common barriers to a successful assessment arise from this relationship to an organization, its security team, and its IT systems. Understanding what these barriers are and why they exist is essential to developing an effective strategy for performing threat hunting.

Short Lead Times

Organizations' IT environments are diverse and dynamic, and different events require different responses. A "one size fits all" approach to solutions is not possible, making it necessary to develop a unique approach to each situation.

Often, these assessments are triggered by external events, such as a security incident. Organizations often have tight deadlines to provide the results of the assessment, leaving little time to prepare. As a result, it can be difficult to develop and implement a tailored strategy in the time allotted.

Lack of Internal Support

Evaluations commonly occur when something has gone wrong, such as a security incident or failed audit. Regardless of fault, the need for an evaluation can be seen as reflecting poorly on the internal security team, and the external evaluation may be seen as being forced on them from outside.

Security leadership forced to undergo an external evaluation may create pushback or roadblocks where they can. Additionally, security administrators who see the need for an evaluation as a criticism of their work may be unwilling to provide the necessary access or expose security issues within their systems.

The Environment is a "Black Box"

The goal of an external evaluation is to have the security of an environment assessed by third parties from outside of the organization. This approach provides significant benefits in terms of bringing a fresh and unbiased perspective to the problem.

While external evaluators have a fresh perspective, they also have little or no knowledge or experience with the systems that they will be inspecting. This lack of previous experience can create delays as evaluators gain the required access and familiarity to perform the assessment. With tight evaluation windows, this can reduce the time and resources available for the actual evaluation.

Services Provided at a Higher Echelon

Increased adoption of service-based solutions means that some of an organization's assets and security functions may be hosted externally. If a service that needs to be reviewed is supported and administered at a higher level, accessing the service in a meaningful way can be very difficult. If not planned carefully in advance, this is often a very time-consuming event.

For services hosted externally or in a different part of the organization, interacting with the administrators of these services may be difficult. Like local administrators, remote administrators are often hesitant to share information or access to the systems under their care. However, for remote administrators, the same mandate to provide these resources and cooperate with the assessment may not exist. As a result, it may be difficult or impossible for evaluators to achieve the level of visibility and access that they require to complete the activities listed in the statement of work.

Restricted Access to Systems

Certain systems within an organization's IT environment may have restricted access. This includes:

- "Mission-critical" systems
- Systems requiring government clearances to access (TS/SCI, full polygraph, etc.)
- Systems in areas with potential security hazards that require extensive specialized training (nuclear, chemical, biological, etc.).

If a security evaluation has a tight timeline, then it may be infeasible to gain access to these systems for the evaluation. This creates a problem if these systems are within the scope of the assessment.

Unscannable Systems

Active scanning is a common part of the reconnaissance process. By sending specially crafted traffic to the various ports on a computer, it is possible to quickly determine what services are running on it and their potential vulnerabilities.

Within a target environment, some systems may be unstable if subjected to active scanning. Examples include:

- Older systems
- Supervisory control and data acquisition (SCADA) systems
- Specialized systems

If these systems received malformed or otherwise unexpected packets, they might crash. As a result, they cannot be included in active scans. This makes the evaluation more difficult and time-consuming because these unstable systems must be explicitly excluded from active scans, and it may be necessary to develop alternative methods for performing reconnaissance of these systems if they are included within the scope of work.

Policy-Exempt Systems

Certain systems within an organization's network may be officially exempt from security policies. Often, these are mission-critical or specialized systems, such as those in industrial control system (ICS) and/or supervisory control and data acquisition (SCADA) environments, with high availability requirements. The downtime required for updates and the potential for an update to break critical functionality makes it unsafe to apply necessary updates, resulting in an "exempt" status.

Policy-exempt systems create challenges for threat analysis because these exemptions can allow multiple vulnerabilities or infections to exist on systems within the scope of the assessment. Even if these exempt systems are not within scope, the potential for infections to spread to or impact other systems complicates the assessment.

Overcoming Common Barriers to External Threat Assessments

External evaluators face a variety of challenges due to their lack of access to the environment and the potential for an adversarial relationship between them and internal teams. However, addressing these common barriers can mean the difference between a successful systems evaluation and a failed one. Evaluators should take these steps to mitigate the impacts of these potential challenges on the success of this and potential future cyber threat analysis exercises.

Short Lead Times

If an evaluation has a short lead time, it's essential to take advantage of what lead time is available. Some core actions can be undertaken very early on, which can provide greater visibility later.

For example, if you ask the local network to identify the point of highest network concentration and put a network traffic telemetry/visibility system there, you can evaluate the logs at right away when the engagement begins. This provides the evaluation team with a good starting point for their assessment and eliminates wasted time waiting for a recently-placed collector to start generating useful data.

Lack of Internal Support

Evaluations are often forced on security teams from outside. While this can cause pushback and create roadblocks to the process, threat evaluators can take steps to ease the process, including:

- Highlighting the Benefits: An external security evaluation gives an organization's security team a fresh perspective on their network and access to external expertise. Highlighting the fact that the assessment will only improve the environment can help to alleviate the concerns of senior personnel.
- Engaging Stakeholders: Members of the security team will be involved in the assessment, and trying to "hide"

activities or results will only create bad feelings and might cause deliberate instruction. Engaging team members and including them in discussions from the start makes the process feel more like a collaboration and less like the evaluation is being imposed upon them.

- Walking Through the Process: Often, senior personnel, and security administrators will be anxious about what will happen during and after the evaluation. Describing the complete process from end to end can help with allaying these concerns.
- Laying Out Potential Impacts: Security personnel may also worry about the impacts of tests on their systems. Discussing each test to be performed and the expected impacts (or lack thereof) can help to alleviate these concerns. For example, if only passive scanning is being used for reconnaissance, point out that this has no impact on an organization's systems.
- Report Early and Often: If a security gap is identified, identify them to the appropriate administrator promptly rather than waiting for the report. This enables you to work together to fix the issue and eliminates surprises in the report.

By engaging senior personnel and security administrators in the process and addressing their concerns, the evaluators reduce the feeling that the assessment is imposed upon them and decrease the potential for pushback and resistance.

The Environment is a "Black Box"

Lack of knowledge about the target environment makes it difficult to plan and carry out an assessment effectively. To help address this issue, get network diagrams and make arrangements to speak with the local administrators as early as possible.

Based on this information, plan the engagement and set boundaries on what needs to be evaluated. After doing so, be sure to stick to these boundaries and don't allow scope creep.

Services Provided at a Higher Echelon

When dealing with external services, preparation is key. If possible, identify the external services before visiting and beginning the assessment. Based on this information, determine whether or not that service is within the scope of the assessment as soon as possible.

Often, the same external service providers support multiple organizations or locations that threat evaluators might be visited during an assessment. If this is the case, it is helpful to develop contacts and relationships with these service providers and leverage these contacts when needed. Familiarity and an understanding of the information and access commonly needed for these assessments can help to smooth and expedite the process in the future.

Restricted Access to Systems

Some systems within an organization may have access restrictions that make it difficult for evaluations to perform necessary testing. It is important to identify these systems and determine if they are within scope early in the planning process.

If they are, the next step is to determine and contact the owners of these systems. If the owners can perform the actions required for the assessment, this may be an effective way to bypass the potential issues caused by the access restrictions. If not, it may be necessary to request additional assets, permissions, or exceptions from the assessment scope to compensate for this issue.

Unscannable Systems

For those systems that are unstable or vulnerable to active scanning, the first step is to determine if active scanning is required as part of the assessment. If the assessment scope only includes passive scanning, then these systems will not be an issue.

If active scanning is required, it will be necessary to exclude these systems from the scan. To do so, work with local administrators to segregate vulnerable internet protocol (IP) addresses and/or subnets to ensure that they are not impacted by the scan.

Policy-Exempt Systems

Some systems within an organization's IT environment may have policy exemptions. After identifying these systems, determine the precise policies that they are exempt from and the reason for the exemption.

For each exemption, assess the risks associated with keeping the exemption in place. This should be based upon the longevity of the system, its interconnectivity with other networked devices, the sensitivity of the data stored and processed on the device, and the current patch level of the device.

Based on this risk assessment, make recommendations to the organization on how to manage the risk created by this system such as steps to further isolate the system from the network. Also, talk to users of the system to determine if any alternative systems exist that could perform the same functions while creating less risk for the organization.

Preparing for a Successful Network Threat Assessment

Without proper preparation, an external threat hunting exercise can be challenging and stressful, but these assessments are essential to mitigating and preventing cyber attacks. Taking the right steps to lay the groundwork, clearly define requirements, and build relationships is critical. Throughout the evaluation process, collaborate with stakeholders and communicate findings often to keep everyone and informed boost the probability of a successful evaluation.