Network Threat Monitoring & Detection

Staying on top of sophisticated threat actors is now a full-time responsibility for all organisations.

Advanced network monitoring and threat detection is now a necessity in order to keep organisations defended against the security risk posed by today’s adversaries.

The various technologies offering advanced intrusion detection have become increasingly complex and it can be difficult to upskill your team to interpret the output of these systems.

Breaches can often go undetected for up to two hundred days, and once they are discovered it can take over forty working days to resolve the issues. It is therefore essential that breaches be detected as soon as they happen – or better yet, avoided altogether. Having resources on hand to deal with an attack is virtually impossible for many organisations.

With a 24/7 Security Operations Centre (SOC) and expert Cyber Defence Operations (CDO) team, NCC Group can offer the technologies and personnel to deal with every aspect of an organisation’s threat detection requirements. Whether that is understanding if a compromise has occurred, with our network threat assessment, or a full 24/7 advanced monitoring and detection managed service.

How it works

Using our bespoke network threat sensor appliance we will monitor your infrastructure for any signs of targeted attacks, active malware or policy violations. All alerts are triaged by trained analysts to provide valuable context and ensure your staff only deal with verified incidents.

• Our Threat Sensor is deployed at a key location in your network, with no effect on normal network operation.
• The Threat Sensor looks for indicators of compromise (IoCs) and signatures both from best-of-breed commercial feeds and our own research, resulting a in high signal-to-noise ratio.

• This custom advanced detection and full packet-capture appliance provides visibility of your network activity. Our SOC monitors this activity at all times, day and night, and responds to alerts generated.
• Any alert that is deemed critical or high-risk will be reported immediately to the client. Lower-risk alerts are typically delivered as part of the monthly summary report.
• Depending on the level of service undertaken, our CDO team will also analyse your network for any additional signs of malicious activity.

The need to stay up-to-date

Many traditional intrusion detection technologies can be slow to respond to the changing threat landscape, often relying on signatures that are outdated or deployed too late to offer any real defence against attackers.

Our Threat Sensor feeds on intelligence and information from a network of over 200 threat sensors deployed in 4 continents across a variety of sectors. Once we see a new threat we push this intelligence to all of our monitored estate. This ensures that all of our threat sensors benefit from this unique shared technical threat intelligence.

• Through our automated machine correlation and false positive feedback loops from the analysts, this is reduced to thirty thousand events of interest per year.
• Every event of interest is then analysed by a consultant, resulting in 4,500 confirmed incidents each year. These are then reported back to our customers for further incident management or through to our dedicated incident response team.
• Each of these 4,500 confirmed incidents produces additional threat intelligence which can be accessed by the Threat Sensor.
• Additionally, technical threat intelligence is gathered on a daily basis from the hundreds of incident response investigations that are conducted by our CDO incident response team.
Our monitoring and defence solutions

We understand that no one solution is appropriate for every organisation; that is why we have built a tiered solution. As we are not a software vendor, we can tailor our services to your specific requirements, in order to fit the level of threat to which you are exposed or the budget constraints under which you operate.

<table>
<thead>
<tr>
<th>Service</th>
<th>Duration</th>
<th>Ongoing Monitoring</th>
<th>Proactive Hunting for Sophisticated Threat Actors</th>
<th>Examples of Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Threat Assessment (NTA)</td>
<td>Periodic</td>
<td></td>
<td>•</td>
<td>Designed for organisations who wish to identify if they have been subject to a compromise. Either used as a standalone assessment or in conjunction with our NTM service.</td>
</tr>
<tr>
<td>Network Threat Monitoring (NTM)</td>
<td>Annual</td>
<td>•</td>
<td></td>
<td>Designed for organisations who require 24/7 monitoring for threats coupled with expert analysts where sophisticated or usual traffic behaviour is identified.</td>
</tr>
<tr>
<td>Advanced Monitoring &amp; Detection</td>
<td>Annual</td>
<td>•</td>
<td>•</td>
<td>Designed for organisations who require a bespoke 24/7 threat monitoring service, together with ongoing network analysis for unusual or sophisticated adversaries.</td>
</tr>
</tbody>
</table>

We don’t just rely on our technology; we hunt for the threat actors

In order to provide full coverage, we recommend a combination of technology and highly trained and experience analysts to ensure a viable defence against the most sophisticated threat actors. Our team come from backgrounds such as government and military, with skills including reverse engineering, malware analysis, and product and software security research. They have the experience and capability to deal with threats, from the most sophisticated state-sponsored attack through to less-sophisticated attacks that still bypass traditional network defences.

Our CDO analysts will actively hunt your network for signs or indications of any unauthorised access or compromise. Should we find anything that looks suspicious we will ensure that it is investigated and alert you immediately of anything that needs attention.

About NCC Group

NCC Group is a global expert in cyber security and risk mitigation, working with businesses to protect their brand, value and reputation against the ever-evolving threat landscape.

With our knowledge, experience and global footprint, we are best placed to help businesses identify, assess, mitigate & respond to the risks they face.

We are passionate about making the Internet safer and revolutionising the way in which organisations think about cyber security.

For more information from NCC Group, please contact:

+44 (0) 161 209 5200  response@nccgroup.trust  www.nccgroup.trust