Defending your business from cyber threats

Platinum Business Partner IBM

Cyber-attacks on organisations are now inevitable. Security is no longer about preventing attacks, it is about preparing for them. This means finding them and dealing with them in real time.

The longer a cyber attack goes undetected (on average 154 days), the more damage it does to the business and the more money it will cost for the business to recover.

A significant shortfall in skilled security resource is slowing down time to detection of security breaches, as organisations simply don't have the bandwidth to manually trace all alerts across their security fabric. Organisations are therefore adopting SIEM (Security Information and Event Management) solutions to provide a single pane of glass view in real time of all external and internal threats, allowing them to be proactive in stopping the attack before it has time to exploit.

Today, customers can choose from a wide range of SIEM software and other security technologies, however, many organisations have realised that software alone will not bring the full level of security required.

Continued investment in experienced personnel and detailed operational processes place a heavy burden on finances and time. By leveraging SCC's SOC (Security Operations Centre) service, our customer can remove these constraints whilst ensuring full visibility, allowing them to focus on their business.

Challenges

1. **Too much data but not enough actionable information**
   Client X have a small IT team, with no dedicated security consultants. With around 1000+ devices, which in turn generate thousands of log entries and alerts per day, data is not being transformed into actionable information of potential cyber threats, posing the risk of multiple unidentified attacks infiltrating the network. Organisations the size of Client X are expected to be targeted with around 1000 cyber-attack attempts within any 24 hour period! Without a dedicated team to focus on this, it is inevitable some threats will be missed, causing both financial and reputational damage.
2. **Only the most obvious attacks are investigated**
   With so much unmanageable data, Client X can currently only investigate what are perceived as easily recognisable cyber-attacks. This however results in too many false positives and does not allow the IT team to drill-down to find and react to REAL attacks that would have significant business impact.
3. **Inability to isolate the root cause of an attack**
   The lack of visibility means intrusions cannot be analysed without consolidating data from multiple point systems. In a decentralised, non-SIEM environment, Client X are currently having to view and understand the nature of issues and alerts on several systems, in order to confirm an attack. This is a highly ineffective means of determining the root cause of an attack, as well as how to respond. Time to remediation will be dramatically increased, leading to potentially greater financial loss and brand reputational damage in the event of an attack.
4. **Lack of visibility to employee activity**
   Insider threats are a bigger risk to cyber security than external hackers, with 74% of cyber incidents happening from within companies. Employees are inadvertently causing corporate data breaches and leaks daily and these are very costly to remediate against. Loss of credentials due to phishing, theft, or even carelessness invites malware into the system when an employee clicks

▶

on a link in a spam email or unknowingly brings an infected device to work. In addition, protection of your IP is at risk in the event of a disgruntled employee or even a leaver wishing to remove data that could potentially provide a competitor with important insight into your business.

RESULT – Client X had a cyber breach which resulted in significant financial loss...

Solution

SCC worked in partnership with Client X to provide the SCC SOC service enabling real time, rapid and thorough analysis of security events originating from both internal and external sources to Client X's network.

The CSS service is designed to detect anomalies, uncover advanced threats and remove false positives. It consolidates log events and network flow data from devices, endpoints and applications distributed throughout a network.

This service is located in SCC's Cyber Security Centre in the UK, where a team of Security Analysts monitor incoming alerts and events. The SOC service remains continually up to date with the latest threats and vulnerabilities provided. It then uses an advanced Sense Analytics engine to normalise and correlate this data and identifies security offences requiring investigation. By IBM X-Force Threat Intelligence which supplies a list of potentially malicious IP addresses including malware hosts and spam sources.

Outcome

- Continuous improvement - the methods that determine what is being attacked and how to stop an attack, are constantly being monitored; as the hackers evolve, we evolve with them, providing Client X real time detection
- Increased efficiencies to address the constant growth of IT environments, as well as the dramatic increase in the number of threats and attacks. The goals are to streamline security solutions while reducing operational costs and staffing requirements. SCC consolidate this data from multiple sources, including networks, servers, databases, applications, and so forth; this enables our SOC analysts to monitor everything from everywhere, in one central location
- Single view of vulnerabilities - Single centralised view of all vulnerabilities with their status and their context. Prioritise by threat and impact - Analyses threat intelligence, vulnerability status and network communications to assess true vulnerability risk.
- Identify at-risk users - account takeover, disgruntled employees, malware actions.
- Streamlined incident investigations - Immediate insights into risky user behaviours, action and activity history.
- 360 Analysis - Perform analysis of activities at the end point, insights from network data, and cloud activities.
- Identify Insider Threats
- Single view of vulnerabilities - Single centralised view of all vulnerabilities with their status and their context.
- Prioritise by threat and impact - Analyse threat intelligence, vulnerability status and network communications to assess true vulnerability risk.