Recent events have redefined the meaning of “normal user activity,” and cybersecurity approaches must follow suit. With the massive shift to working from home, and its subsequent uptick in alert volume, organizations need tools that will help them quickly determine which alerts should be prioritized for mitigation. The Illusive Platform integration with Microsoft Azure Sentinel provides high-fidelity notification and full intelligence about attack surface risk and the most dangerous in-network threats so they can be stopped early before damage can be done.

**Stop the Lateral Movement that Enables Attacks**
Illusive attack surface management identifies and removes leftover credentials and connections that attackers leverage to move from machine to machine as they laterally move towards the critical assets they seek to steal. Then, Illusive replaces those credentials and connections with deceptive versions that attackers would expect to encounter and exploit. Once attackers engage with this deceptive data, organizations receive full forensics on attacker activity and can take any necessary steps to remediate the threat.

Through the Illusive Attack Management System data connector, organizations can share Illusive’s attack surface analysis data and incident logs with Azure Sentinel. This information can be viewed from dedicated dashboards especially designed for Azure Sentinel that provide actionable insight into attack surface risk and that provide high-fidelity notification of unauthorized lateral movement in your organization’s network.

The Benefits of Integrating Illusive with Azure Sentinel:
- Incorporate Illusive attack surface management and high-fidelity threat detection within Azure Sentinel
- Detect malicious lateral movement from anywhere to anywhere in hybrid cloud environments
- Find imminent threats that behavioral-based detection often misses
- Map and secure network pathways to critical assets
- Reduce false positives to make threat investigations quicker
- Get enriched Illusive forensic intelligence for any alert Azure Sentinel aggregates
- Custom playbooks and APIs for Sentinel that automate additional attack intelligence and forensics
- Leverage detailed threat analytics to make incident triage more efficient

**Detailed east-west lateral movement risk and attack intelligence from within Azure Sentinel**

```
<table>
<thead>
<tr>
<th>Domain User Credentials</th>
<th>Domain User Credentials - Top Violating Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>458</td>
<td>224, 159, 75 (prec.proprietarion.com)</td>
</tr>
</tbody>
</table>
```

![Incidents over time](chart)

- Number of incidents in which Trigger Type is found
  - 21 incidents
  - Type 1
  - Type 2

- Number of incidents in which Event Type is found
  - 24 incidents
  - Average 11
Illusive Networks for Azure Sentinel: Key Features

**CEF Connector and Dashboards:** ingest Illusive attack surface management and threat detection data into Azure Sentinel. A series of dashboards with full analytics about potential attack risks and current threats provides intelligence about the most dangerous threats, their distance from critical assets, attacker behavior, and much more.

**End-to-end Microsoft Cloud Tools Support:** Out-of-the-box integrations with Azure AD, Intune and Microsoft Managed Desktop (MMD) allow for a full Illusive deployment in Microsoft-enabled cloud environments.

**Illusive Playbooks Designed for Sentinel:** Enhance Security Operations Center (SOC) efficiency for any event detected by Sentinel. Get full Illusive forensics for all incidents, including a chronological timeline of all events on a specific host, and automate attack surface reduction as new potentially risky attacker pathways appear.

**Enhanced Threat Visibility through Attack Surface Manager:** Illusive’s Attack Surface Manager, a part of the Illusive Platform, provides increased visibility into the potential ways that attackers can move laterally towards critical data on your network. Get crucial intelligence about your crown jewel assets, how many hops it would take to reach them, which machines have admin credentials stored on them, and much more.

**Launch Automated Deception Campaigns When Risk Is Detected:** The Illusive Platform boasts a full array of data-based network deceptions, device emulations and full decoy environments. Network deceptions and emulations can be triggered to launch when threats are detected to instantly block malicious lateral movement.

**Comprehensive Forensics that Increase SOC Efficiency:** With Illusive’s detailed forensics about attack surface risks, impending threats and attacker behavior, organizations are able to empower lower tier analysts and improve the quality of their escalations, freeing upper-tier analysts to focus on the most urgent threats and waste less time on false positives.

The Illusive Platform provides centralized management across even the largest and most distributed environments. Three modular components can work together or be operated separately to preempt, detect, and respond to cyberattacks.

Attacks come from all directions - from phishing emails to cloud account takeovers. The key to foiling attackers is stopping the attacker’s ability to move anywhere they might be.

Stopping attack movement means stopping lateral movement in the data center environment, vertical movement to and from cloud, and movement across and within clouds. Illusive does all three, providing a comprehensive platform for stopping attacker movement no matter where they start or end up.

© 2020 Illusive Networks. All rights reserved.