Attack Surface Manager
Technical Overview

Overview

Attack Surface Manager (ASM) is a component of the Illusive Networks Platform designed for the pre-breach stage before an attacker lands within the network. It reduces the attack surface by continuously monitoring for and eliminating conditions that could potentially be used by an attacker to facilitate lateral movement. Specifically, the first release of ASM focuses on minimizing the proliferation of credentials.

On a daily basis, users within any organization leave behind an invisible “access footprint”—credentials and connections to other systems. Once inside the network, advanced attackers use these as keys to get closer to their targets. Depriving attackers of these keys is an essential, preemptive component of preventing high-impact cyber attacks.

By exposing attack vectors that enable lateral movement, and by enabling instant corrective action, Attack Surface Manager provides the visibility and automation security teams need to continuously increase the resistance of the environment to advanced attackers—without inhibiting the business.

What is the “Access Footprint”?

The “access footprint” is the sum of all credentials and connections that exist in a network—intentionally and unintentionally—between endpoint systems. While users sometimes acquire credentials they’re not authorized to have, this access footprint is not mainly malicious—it is an inherent byproduct of the organization’s daily activity. Credentials proliferate through a variety of means. For example:

- User names and passwords can be inadvertently captured in browser history;
- After providing remote support, an IT person’s domain admin credentials can be left in system memory;
- System management and maintenance routines can require that credentials be embedded in applications.

The access footprint has several characteristics:

It is necessary, but larger than it should be. Some of this access footprint can and should be removed, but some of it is essential to the functioning of the business.

It perpetually changes, as systems and users come on and off line, as the user population changes, as access rights change, etc.

It is not easily visible through common security technologies.

It is vast—that is, in all but the smallest organizations, it would be virtually impossible to identify and manage the access footprint manually.

ASM Value and Benefits

To preemptively reduce attack risk, security teams need a scalable means of continuously monitoring the access footprint, identifying risky elements that should be removed, and executing efficient remedial action. Organizations using ASM will be able to:

- **Gain unprecedented visibility on the access footprint** and related policy violations across the enterprise that can facilitate attacker mobility;
- **Continuously minimize the attack surface**, even in rapidly changing human and IT environments;

- **Prioritize and rapidly resolve violations** through a choice of automated and manual methods;
- **Detect advanced attackers faster**. By reducing the number of attack vectors in the environment, particularly ones most appealing to the attacker, ASM decreases the number of real objects that enable lateral movement and increases the odds that attackers will choose false objects.

These benefits are delivered through a solution that is scalable, easy to deploy, low-cost to operate, and integrates easily with other monitoring, threat hunting, visualization and forensics technologies.

Technology Overview

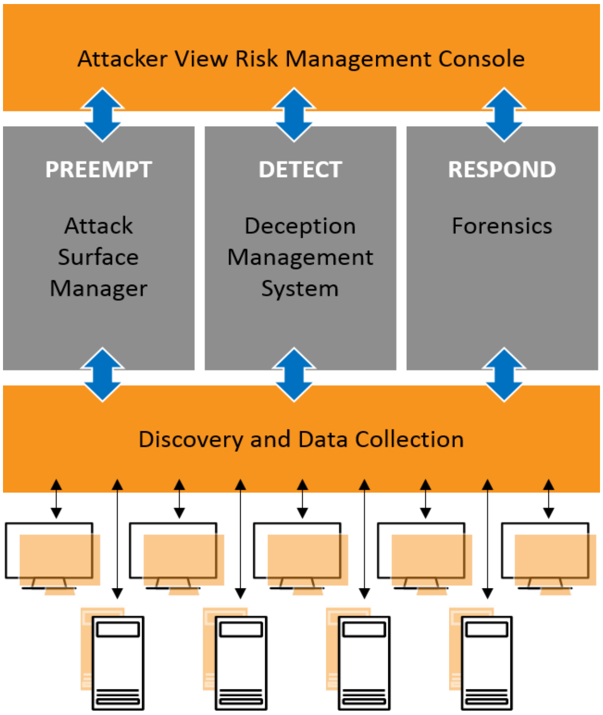
ASM doesn't detect whether an attacker is present; it shows what an attacker *could* do once inside, and enables elimination of the offending attack vectors. ASM is the **preemptive** element of Illusive's deception-based approach to mitigating the business risks posed by targeted attacks.

Illusive's Deception Management System provides core **detection** functions by deploying and managing tailored deceptions on each system to create a web of fake elements which, appearing useful for lateral movement, trigger an alert when activated by an attacker. Once an alert is raised, Illusive enables incident **response** by gathering real-time forensic data from compromised hosts and supplying risk orientation to help responders prioritize and remediate based on relative business impact.

ASM provides the following functions and features:

- **Automated, agentless discovery and mapping** of the access footprint across all endpoints;
- **Easy definition of rules and policies** through both manual and automation-assisted processes;
- **Continuous monitoring** for credential violations;
- **Risk-oriented, contextualized visibility** on the potential impact of policy violations;
- **Hunting and forensic** tools to support investigation;
- **Corrective action** through a choice of manual and automatic methods.

Figure 1: ASM within the Illusive Platform


Attacker View Risk Management Console
PREEMPT
Attack Surface Manager
DETECT
Deception Management System
RESPOND
Forensics
Discovery and Data Collection

The four components of ASM are described below.

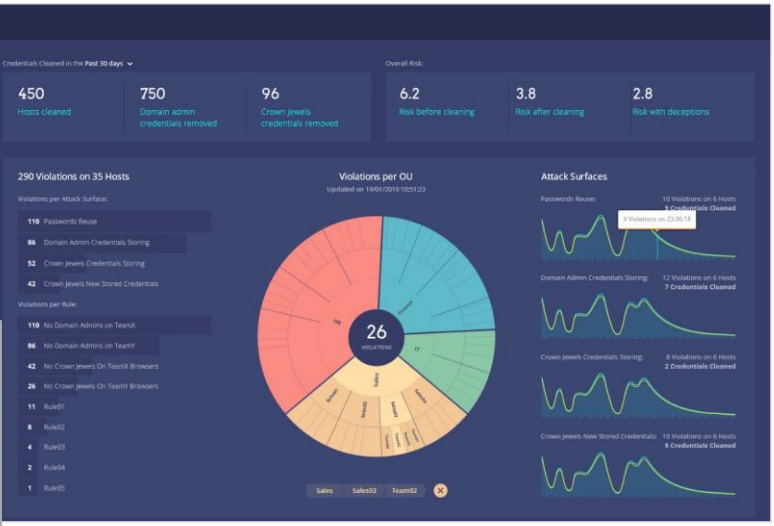
1. Analyst Dashboard

The Analyst Dashboard is the ASM user interface, designed for use in the SOC alongside SIEM and other technology dashboards. It complements other tools by providing a broad picture of the access footprint and related issues and incidents requiring attention, providing both summary and drill-down views of credentials residing on systems across the organization and its various divisions.

The Analyst Dashboard:

- Displays all access activity and violations in the network across the different departments;
- Identifies potential problem areas;
- Directly generates rule suggestions and automatically populates rules on demand for selected ranges of users, OUs or subgroups;

Figure 2: ASM Analyst Dashboard


ASM

ASM Dashboard

Violations

Rules Management

Credentials Cleaned in the **Past 30 days**

450 Hosts cleaned

750 Domain admin credentials removed

96 Crown jewels credentials removed

Overall Risk:

6.2 Risk before cleaning

3.8 Risk after cleaning

2.8 Risk with deceptions

290 Violations on 35 Hosts

Violations per Attack Surface:

110	Passwords Reuse
86	Domain Admin Credentials Storing
52	Crown Jewels Credentials Storing
42	Crown Jewels New Stored Credentials

Violations per Rule:

110	No Domain Admins on TeamX
86	No Domain Admins on TeamY
42	No Crown Jewels On TeamX Browsers
26	No Crown Jewels On TeamY Browsers
11	Rule01
8	Rule02
4	Rule03
2	Rule04
1	Rule05

Violations per OU

Updated on 19/01/2018 10:51:23

Attack Surfaces

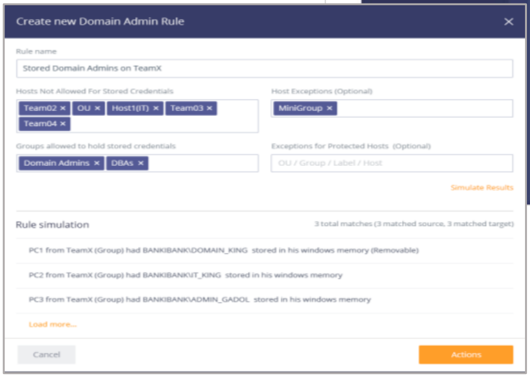
Passwords Reuse: 10 Violations on 6 Hosts **5 Credentials Cleaned**

6 Violations on 23.06.18

Domain Admin Credentials Storing: 12 Violations on 6 Hosts **7 Credentials Cleaned**

Crown Jewels Credentials Storing: 8 Violations on 6 Hosts **2 Credentials Cleaned**

Crown Jewels New Stored Credentials: 10 Violations on 6 Hosts **5 Credentials Cleaned**


Create new Domain Admin Rule

Rule name: Stored Domain Admins on TeamX

Hosts Not Allowed For Stored Credentials: Team02 × OU × Host1(IT) × Team03 × Team04 ×

Host Exceptions (Optional): MiniGroup ×

Groups allowed to hold stored credentials: Domain Admins × DBAs ×

Exceptions for Protected Hosts (Optional): OU / Group / Label / Host

Simulate Results

Rule simulation — 3 total matches (3 matched source, 3 matched target)

PC1 from TeamX (Group) had BANKIBANK\DOMAIN_KING stored in his windows memory (Removable)

PC2 from TeamX (Group) had BANKIBANK\IT_KING stored in his windows memory

PC3 from TeamX (Group) had BANKIBANK\ADMIN_GADOL stored in his windows memory

Load more...

Figure 3: Rule Management
Rules are automatically populated and monitored for effectiveness.

- Provides an interactive "canvas" showing potential attack vectors, violations and clean-up activities;
- Tracks progress made by the security team;
- Automatically populates and adjusts as rules are defined or revised.

2. Rules Engine

The Rules Engine is the heart of ASM. It enables:

- Manual definition of the organization's policies for credentials and access to "crown jewels";
- Inspection and approval of automatic rule suggestions (those proposed by the Rules Engine based on actions taken by the analyst).

The Rules Engine parses and maps data collected from the organization's endpoints to identify violations. Rules can be configured through two primary methods:

- Manually based on organizational knowledge
- Automatically populated, spawned through data provided to the Analyst Dashboard and Attacker View, automatically referencing relevant Crown Jewels, hosts, and OU's.

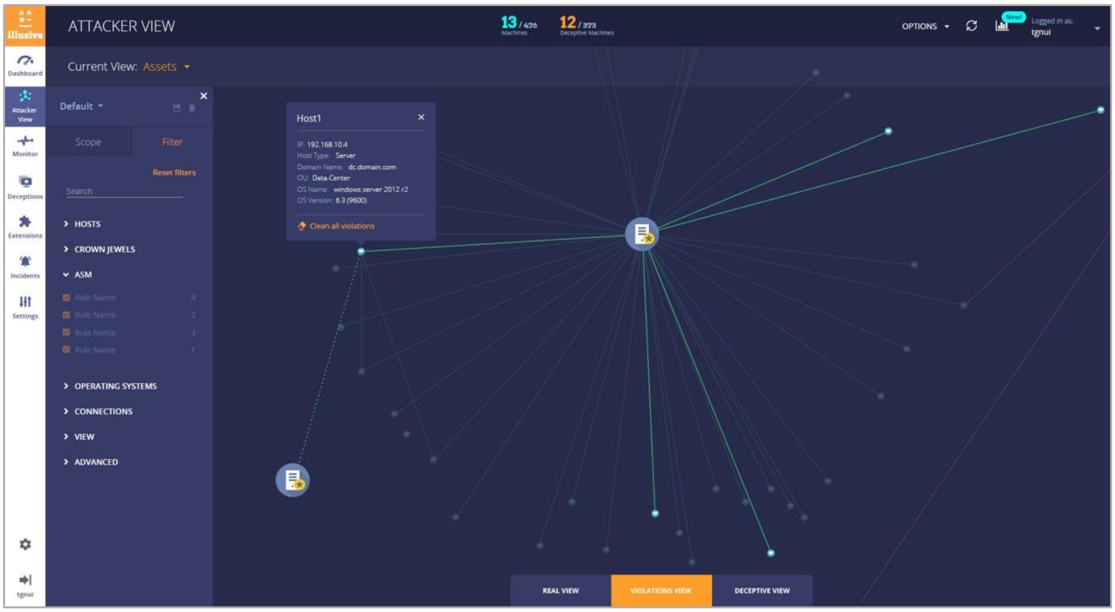
Once rules are defined, the Rules Engine:

- Eliminates conditions that match an ASM Rule;
- Transmits violations to a SIEM or other platform;
- Transmits an email to designated individuals.

The Rules Engine is conscious of human error and is designed to promote transparency. In creating rules, analysts leverage a "simulation mode" in which a new rule, rather than being immediately promoted to production, is run offline on existing data to ascertain the number and type of matches it will yield. This option reflects Illusive's commitment to "noiseless" technology and a near-zero rate of false positives. This validation step helps Illusive users anticipate the impact of rules before they're introduced to ensure high quality—versus high quantity—of alerts.

3. ASM Extension of Attacker View Capabilities

In a detection context, Illusive's Attacker View maps the endpoint environment as the attacker would want to see it—showing system-to-system connections and potential paths to critical assets. Upon detection, security analysts can see the proximity of the attacker to critical assets.



Host1

IP: 192.168.10.4
Host Type: Server
Domain Name: dc.domain.com
OU: Data-Center
OS Name: windows server 2012 r2
OS Version: 6.3 (9600)

Clean all violations

Figure 4: Attacker View in ASM Mode

With ASM, Attacker View can also be a hunting tool, allowing security teams to drill down on specific areas of the organization (OUs, labels, user groups, etc.). This enables them to view actual system-to-system relationships based on credentials in use, see how users are connecting to other systems, and view credential policy violations across the network. From within Attacker View, analysts can also take action to eliminate or remove violations (see "Action Engine").

4. Action Engine

With ASM, Illusive introduces the ability to execute actions to reconfigure or remediate violations or other conditions. The following functionality is provided to reduce the attack surface:

- Remove/Delete credentials from memory;
- Remove/Delete credentials from browsers;
- Remove/Delete credentials from a single host remotely;
- Remove/Delete credentials from a group of hosts remotely;
- Remove/Delete credentials from an OU, a group of OUs, or the entire organization.

The Action Engine will enable efficient resolution of violations through various means and degrees of automation. Credentials can be removed—

- Manually, streamlined by the automatic identification of violations;
- Semi-automatically in Attacker View by executing ad hoc actions, or by selecting groups of objects for removal of single or multiple violations;
- Fully automatic, rules-driven vector elimination.

The Action Engine enables customers to accomplish routine hygiene tasks more efficiently and at scale, helping to reduce risk while also maintaining or lowering OpEx.

For more information

Visit us at www.illusivenetworks.com

Email us at info@illusivenetworks.com

Call us at +1 844.455.8748 (North America)
or +972 73.272.4006 (EMEA and AsiaPac)

Illusive Networks is a leader in deception-based cybersecurity solutions, empowering security teams to take informed action against advanced, targeted cyber attacks. By inhibiting and detecting the lateral movement of adversaries toward critical assets early in the attack process, attacks can be stopped before damage is done.