Check Point
SOFTWARE TECHNOLOGIES LTD.

21 October 2018

AAD - ASSET AND ANOMALY DETECTION DATASHEET

Meaningful Insights with Zero System Impact

STEP UP TO
5TH GENERATION
CYBER SECURITY

Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page https://www.checkpoint.com/products-solutions/certified-check-point-solutions/.

More Information

Visit the Check Point Support Center https://supportcenter.checkpoint.com.

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on AAD - Asset and Anomaly Detection Datasheet .

Revision History

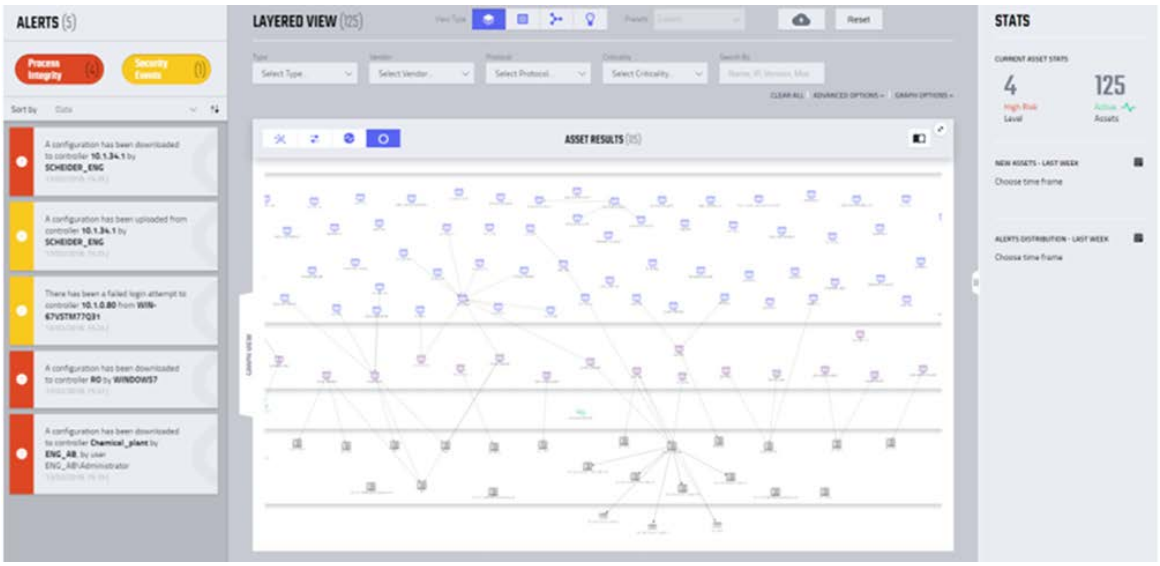
Date	Description
21 October 2018	First release of this document

Contents

Introduction

AAD is a completely passive monitoring system and imposes zero impact on the OT network. No active scanning is required and there is no need to install software on endpoint devices.

- **Behavioral Analysis** - Leveraging these fine-grain network details, AAD employs advanced, behavior-based anomaly detection and sophisticated pattern matching for early identification of malicious activity.
- **Visualization** - Correlate data and visually depict the complexity of communications pathways down to the lowest levels of the network, down to the serial and fieldbus networks that control physical processes.
- **Dissectors** - Proprietary dissectors for all major IT and industrial network protocols, leveraging deep packet inspection to safely extract information from both serial and IP-based networks. These dissectors extract precise details about each asset on the network, capture exactly how assets are communicating across the network.



Asset and Anomaly Detection (AAD) is the asset management and anomaly detection product for ICS networks that provides rapid and concrete situational awareness through real-time alerting. **AAD** constantly monitors industrial control system (ICS/SCADA) network traffic and generates alerts for anomalous network behavior that indicates a malicious presence and for changes that have the potential to disrupt the industrial processes.

AAD software is installed on a server or runs as a VM. The system connects to Check Point GW's and managed switches. Employing deep packet inspection (DPI) on a real-time copy of network traffic, the system uses a safe, fully passive approach that never impacts industrial control systems or the safety and reliability of the process.

When connected to an industrial network, AAD automatically discovers assets, learns network topology, models the networks unique communication patterns and creates a fine-grain behavioral baseline that characterizes legitimate traffic. The system provides important insights about network hygiene, configuration issues, and vulnerable assets.

Following the learning period, the system shifts to operational mode where alerts are triggered for any violation of the baseline. AAD generates actionable alerts that are clear, consolidated, and context rich. This provides security and control teams rapid situational awareness of potential and actual process disruptions and enables teams to quickly and efficiently respond to events as well as maintain the safety and reliability of industrial processes.

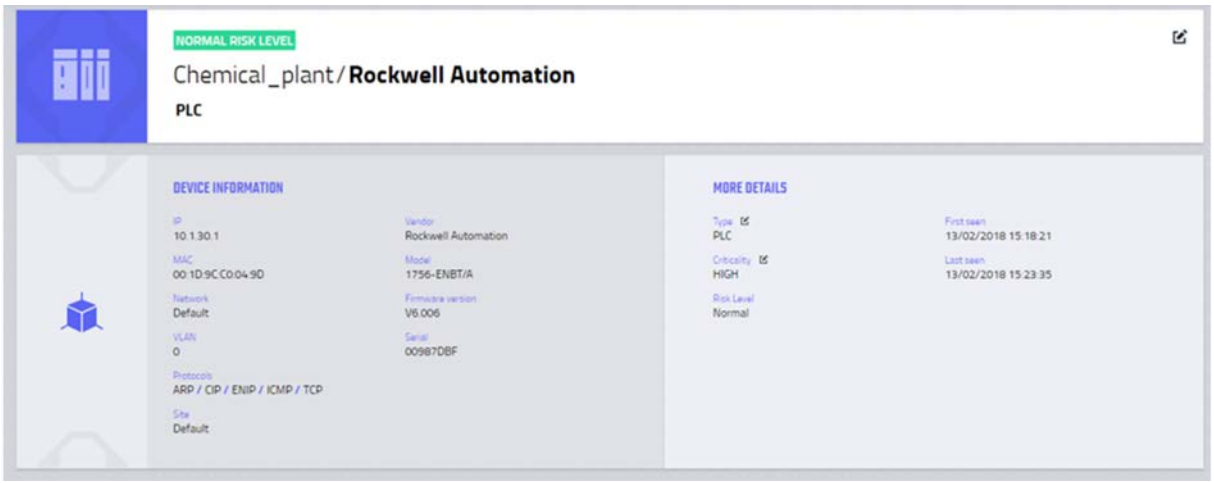
Benefits

In This Section:

Asset Discovery

The system discovers assets across the entire industrial network – IP assigned, nested assets and assets that communicate over serial connections.

This real-time visibility can be utilized for asset inventory and management tasks, and for addressing various regulatory and internal audit requirements.



Examples of various data displays:

- Network graphic representation (asset map).
- Various graph filters: Protocols, Asset Types, Criticalities, Risk Levels, Firmware Version, Address, MAC, and Name.
- Table page, containing all the assets with the following identifiers: Name, Address, MAC Address, OS, Protocol, Vendor, Type, Criticality Risk Level, Network.
- Single asset page, containing additional unique identifiers: Zone, First Seen, Vendor, Serial, Model, Firmware Version, asset network graph, and physical slots data (in a PLC that supports such architecture).
- Report generation by applying **Export** on a chosen filtered search.

While there are generic identifiers that apply to all assets (IPv4, MAC, Protocols), there are others that are unique to specific products\product groups.

Examples of the latter include:

- PLC Rockwell 1756-L71/B-LOGIX5571: Vendor, Serial, Number, Firmware Version, Rack Slots physical data.
- Stratic_8000 Switch: Host Names, Vendor, Model, Firmware Version.
- Schneider Electric M430: Vendor, Model, Firmware Version, Project.
- Any Windows Endpoint: OS Version, Host Name.

Proactive Network Resilience

The system provides deep visibility into the network's assets, networking infrastructure, and discovers:

- Networking hygiene issues and misconfigurations
- Weak passwords
- Insecure connections (outbound, or between seemingly segmented zones)
- Software vulnerabilities
- Active sites and remote connections

Security and Operational Alerts

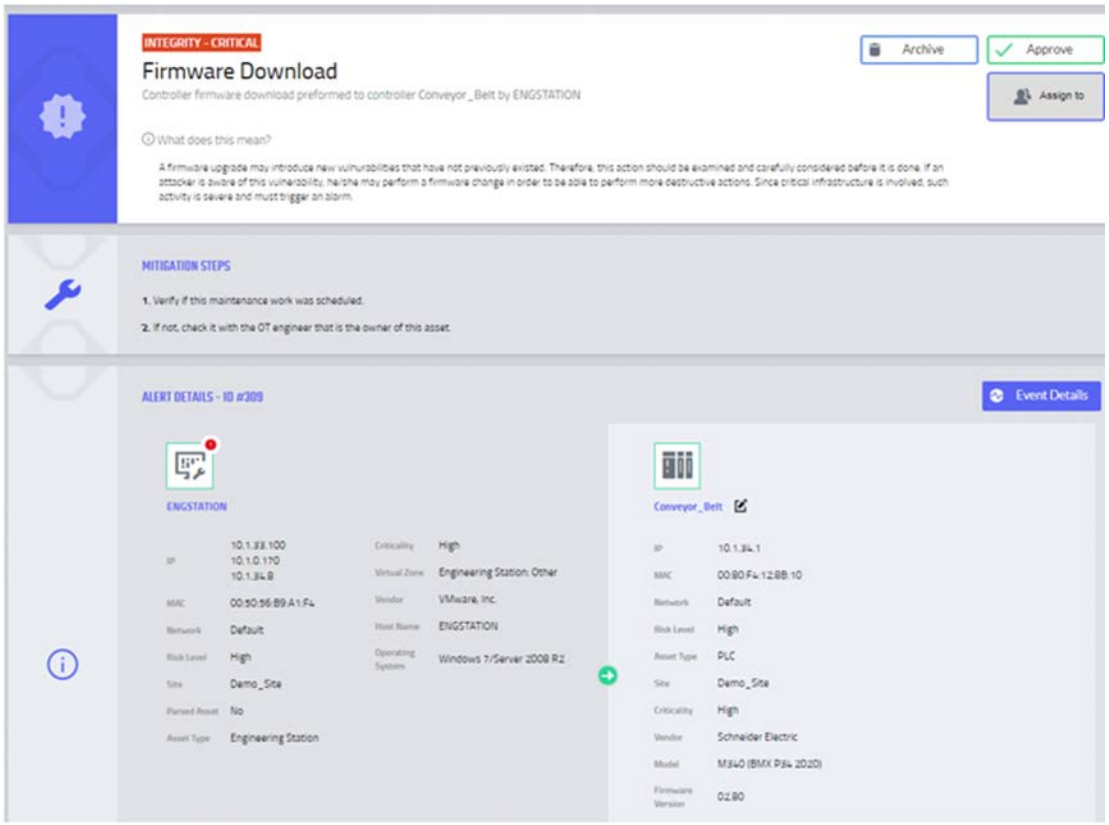
AAD generates an alert upon occurrence of anomalous and critical events. An event might be a single deviation from an assets' baseline, such as a Windows endpoint issuing a Write command to a controller it has never communicated with before, or more complex, comprising multitudes of such deviations. In this case, the system would apply its analysis engine and conclude the event stream to a single, human readable alert.

Alerts fall into the following groups:

- Critical change
- Malicious activity

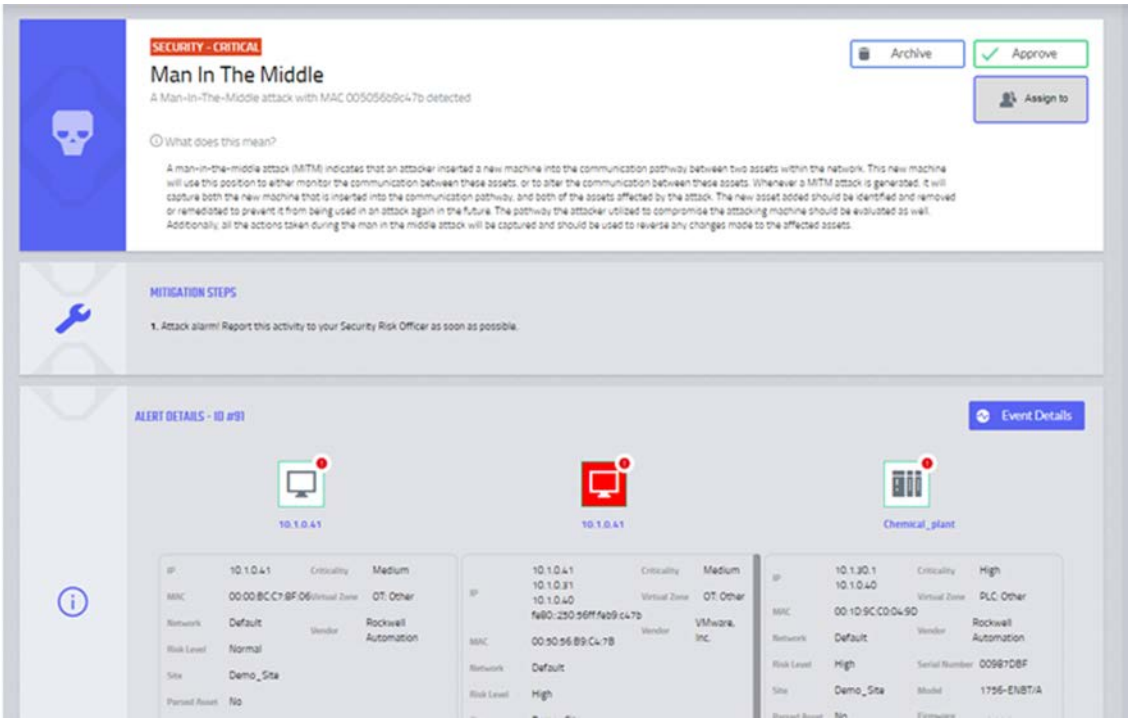
Critical Change

A critical change is any asset communication that imposes direct potential or actual impact on an OT process. The risk of such an event is determined by its context. For example, a configuration download to controller is benign when performed by a control engineer as part of an operational routine, but poses a significant operational risk when executed by an attacker.



Malicious Activity

A malicious activity is an asset communication that clearly indicates malicious presence or activity in the network. This might be an early reconnaissance activity such as port scanning, or a more mature attempt to establish a Man in the Middle communication.



Alert Examples

- Configuration Download: engineering station downloads code to controller.
- Configuration Upload: engineering station retrieves controller's code.
- Mode Change: controller mode transition (Program, Run, Monitor)
- Firmware Upgrade: change in controller firmware.
- Info Change: change in an asset's unique identifiers (IP, Name etc.)
- Online Edit: change in the code while controller is running.
- New Asset: new asset initiates communications in the network.
- Failed Login: any connection attempt that
- Man-in-the-Middle: compromised device initiates assigns to itself two asset's IP addresses to intercept their exchanged traffic
- Network Scan: asset scans open ports of multiple other assets.
- Port Scan: asset scans ports of single asset.

Baseline deviations, critical change or malicious activity alerts provide the security and control team with all the data and context to gain immediate understanding regarding what happened, and which assets were involved.

In the case of a direct process disruption, such as configuration download or online edit, the alerts even show the exact change to the controller's code, enabling the control team to rapidly reverse the change and restore previous settings.

Central Management and Integration

AAD is an integrated component in the Check Point ICS solution.

The AAD communicates with Check Point GW's in the OT network that forwards the raw data for analysis and processing.

In a single or multisite installation (either physically remote sites or isolated production islands), each individual AAD system sends its alerts to Check Point Smart Console management.

Precise CVE Matching

Identify assets with known vulnerabilities (CVEs) – all the way down to firmware versions for industrial devices.

Specific Configuration Insights

Uncover network configuration "hygiene" issues to reduce the attack surface and improve operational reliability.

Attack Vector Analysis

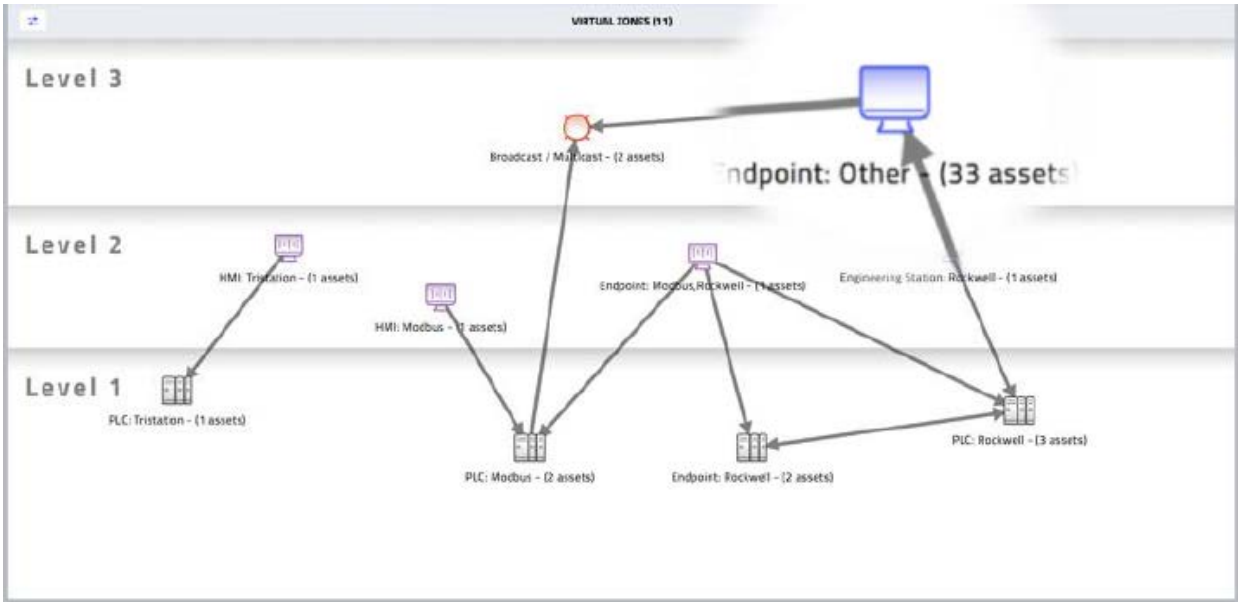
Analyze specific scenarios simulating possible attack vectors that have the potential of compromising critical OT assets.

Leveraging the Attack Vector Analysis, OT security teams can proactively mitigate risks and prioritize activities based on the most likely attack scenarios.

Attack Vector Analysis allows security teams to quickly simulate what-if mitigation actions to continuously adjust their security posture and reduce the overall attack surface. Consequently, they can further expedite the creation or update of a network segmentation leveraging a contextual-based analysis of all identified network and endpoint vulnerabilities.

Network Visualization and Virtual Zones

AAD's Network Visualization and Virtual Zones provides the needed capabilities to expedite the process of a new imitative network segmentation as well as fine tuning an existing schema. By applying smart grouping algorithms, security teams can quickly and easily minimize access to sensitive information and assets to people who don't need it, while allowing access to those who do. Additionally, and to further tighten access to network assets, the system maps out the exact communication patterns that helps to quickly and easily define firewall rules on the basis on the deep analysis.



The above figure shows the result of an automatically generated virtual zones mapping.

Clicking on one of the virtual zones provides a deeper dive into the specific communication patterns between 2 (or more) virtual zones. This unique capability provides security teams detailed information on which protocols are used (including specific ports) between the zones (including source and destination IPs) along with communication frequency. This detailed information can be leveraged to create firewall specific rules – by allowing you to whitelist all traffic between two (or more) assets and blacklist all other traffic. This further tightens security around specific assets and consequently assists in reducing the overall attack surface.

Reference Architecture