Securing Industrial Control Systems

Check Point AAD (Anomaly and Asset Detection) Mapped to NISTIR 8219 Behavioral Anomaly Detection Document

GOALS & OBJECTIVE

The US National Institute of Standards and Technology (NIST), National Cybersecurity Center of Excellence (NCCoE), in conjunction with NIST's Engineering Laboratory (EL) recently released a draft paper, Interagency Report 8219 - named: "Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection (BAD)", putting forth the idea that anomaly detection is an essential tool for owners of Industrial Control Systems (ICS) to identify, mitigate and remediate Cyber threats to Operational Technology (OT) environments. The goal of this document is to raise awareness of a Check Point tool, Asset and Anomaly Detection (AAD), available to ICS owners, both government and commercial and to compare the Check Point solution to the ideas put forth in the NIST paper.

The objective of both BAD and AAD is to combat the ever growing threat to ICS worldwide. Traditional detection systems and tools that ICS owners may have in place today may be geared towards finding parameters and conditions that are either outside of normal operating specifications or are for predefined threat signatures that are known indicators of compromise. Anomalous detection tools such as Check Point AAD and the concepts outlined in NISTIR 8219 all seek to expand the existing ICS tool set and are not meant to be a replacement or substitute for traditional tools.

> *"Cybersecurity is essential to the safe and reliable operation of modern industrial processes. Threats to ICS can come from numerous sources, including hostile governments, criminal groups, disgruntled employees, other malicious individuals, unanticipated consequences of component interactions, accidents, and natural disasters. The Cybersecurity Framework [1] addresses identifying threats and potential vulnerabilities; preventing and detecting events; and responding to, and recovering from, incidents. It is not possible to prevent all cyber events. It may not even be possible to identify all threats for which ICS need to be prepared. It is certainly necessary to detect incidents before the response to, or recovery from, the incidents can be undertaken. Therefore, the detection of cyber incidents is an essential element for cybersecurity."*
> --NISTIR 8219

To that end, Check Point Software Technologies has expanded our existing ICS tool set by integrating AAD capabilities to our already extensive ICS protocol support in our Application Control and ICS specific signatures in our Intrusion Prevention System (IPS).

SCOPE

The NISTIR 8219 paper includes a "Demonstration Scenarios and Findings" section in which NIST created two example ICS environments to simulate real-world operations within which NIST introduced several different commercial anomaly detection products representing different deployment models for anomaly detection. The deployment models are at the network level, endpoint level and Historian/Sensor level. The general ideas put forth by NIST may be implemented in multiple ways. The Check Point AAD solution is covered under the network based model.

It is not the intent of this paper to replicate the tests or to even conduct a similar test but rather to compare the features and capabilities of our network-based detection method to the features and benefits presented in the NISTIR 8219 draft to those provided by Check Point AAD.

METHODS AND IMPLEMENTATION

The NISTIR document lists 3 BAD detection methods and implementations: Network, Agent and Historian/Sensor. The NISTIR paper makes no effort to conclude which method is better. Check Point AAD is a Network-based solution.

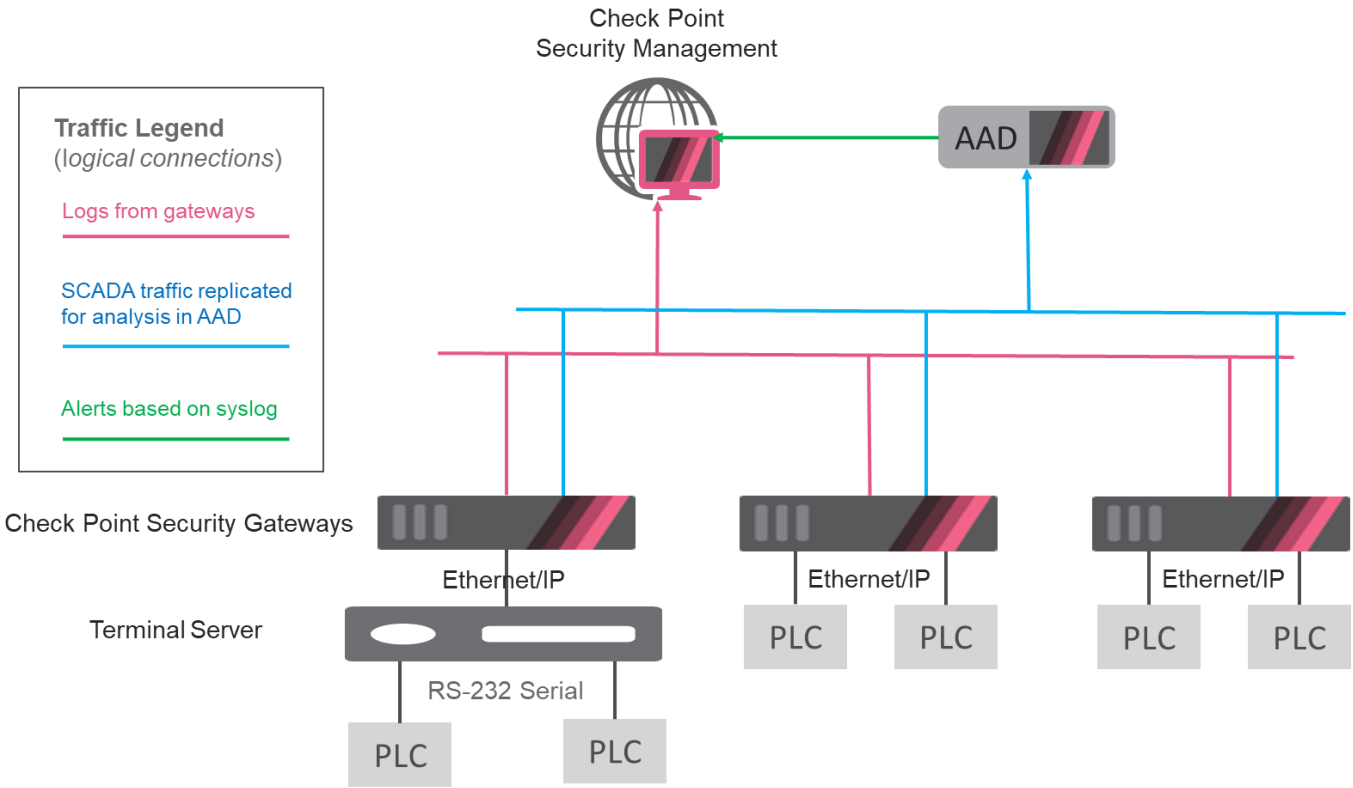

Figure 1: Single Site Basic Configuration

CAPABILITIES

Section 1.4 of NISTIR 8219 lists the following example BAD Capabilities that manufacturers can adopt to achieve their cybersecurity goals. The following aligns the Capabilities identified by NISTIR 8219 with corresponding references from the Check Point AAD datasheet. Check Point AAD meets or exceeds the Capability specified in NISTIR 8219.

Capability: Models of BAD capabilities that manufacturers can adopt to achieve their security goals for mitigating the risks posed by threats to cybersecurity

Check Point AAD Page 5: Following a brief learning period, AAD 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.

Capability: Nonintrusive techniques to analyze industrial network communications, allowing the existing ICS infrastructure to flow through the network without interruption or a performance impact

Check Point AAD Page 5: AAD is a completely passive monitoring system and imposes zero impact on the OT network. There is no need to install software on endpoint devices. However, AAD provides additional levels of discovery methods, to cover cases where the passive method isn't efficient enough: Active and App DB options.

Field Note

Q: What is the best way to collect information and provide ICS visibility?
A: We call it Multispectral Data Acquisition and it supports the following passive and active collection methods.

Passive: continuous, real-time monitoring of OT Networks
Rapidly discover network communications and asset details down to the I/O level
Field proven and 100% safe for OT networks.

Active: precise, periodic queries of OT and IT Assets
Safely query ICS and non-ICS assets for enhanced visibility into asset configurations
Enhances context for alerts and vulnerabilities

App DB: offline enrichment of OT asset data
Ingest and parse PLC/RTU project and other configuration files and binaries
Gain nearly 100% asset coverage and enhanced configuration details

Q: Why do we need Active collection?
A: There is important data that passive collection does not have access to and some use cases where approaches other than passive are simply necessary.

Q: Is it safe to use Active collection?
A: There are two primary ways in which traditional active collection can cause harm in OT networks. First, queries can end up saturating the small pipes that make up many industrial networks. Further, it can impact the legitimate OT traffic.
We offer "Safe Active", a solution which takes into account those factors.
To avoid the saturation issue, the system has the ability to rate limit the number of concurrent queries. For the incorrect protocol issue, we employ a combined passive and active approach.

Q: Why do you need Active and other modes of data collection?
A: Passive capability provides a rather impressive, and often startling, array of data about the assets on an ICS network, and for many environments, this level of detail is adequate. But some use cases need more lower-level detail, and this type of passive scanning cannot discover everything. Passive techniques are not able to yield some endpoint configuration data, e.g. which patch level a Windows or Linux machine is running, which software packages are installed on these nodes, or the version of virus definition files.

There are also instances where devices do not communicate on the network, or communicate very infrequently, so passive is not able to capture data about these nodes. And in a few situations, we simply don't have access to devices, e.g. because they are on a different network segment or because the customer has an unmanaged switch without SPAN or mirror capabilities. In these cases, the use of multispectral data collection can serve to enrich our already robust data set and better inform these important use cases.

Lastly, and very importantly, some plants or operational environments simply cannot easily or cost effectively deploy passive Deep Packet Inspection. For instance, some plants do not yet have modern switching infrastructures that support SPAN/Mirror ports. And even in plants that do, internal change management processes add substantial time constraints. In these cases Active and App DB may prove to be more cost effective or substantially reduce the time to deploy.

Capability: Establishment of one or more baselines, and notification when specific changes or anomalies occur in the environment over time
Check Point AAD Page 5: In addition to the AAD capabilities outlined for the first capability, above, 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.

Capability: Identification of new devices on the ICS network and of assets that have disappeared from the network
Check Point AAD Page 9 - AAD Malicious Activity Alert example New Asset: new asset initiates communications in the network. The Malicious Activity module can also identify missing assets as compared to the baseline.

Capability: Detection of unauthorized configuration changes and of the transfer of files in the network
Check Point AAD Page 9 - AAD's Malicious Activity alerts listed below exemplify this capability:
- Configuration Download: engineering station downloads code to controller.
- Configuration Upload: engineering station retrieves controller's code.
- Firmware Upgrade: change in controller firmware. Mode Change: controller mode transition (Program, Run, Monitor)

Capability: Increased visibility into network operation and real-time alerting
Check Point AAD Page 5: 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.

BENEFITS

Section 1.5 of NISTIR 8219 lists the following Benefits intended to help organizations accomplish their goals by using anomaly detection tools for the following purposes. The following aligns the Benefits identified by NISTIR 8219 with corresponding references from the Check Point AAD datasheet. Check Point AAD meets or exceeds the Benefit specified in NISTIR 8219.

Benefit: Detect cyber incidents in time to permit effective response and recovery
Check Point AAD Page 5: 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.

Benefit: Expand visibility and monitoring capabilities within manufacturing control systems, networks, and devices
Check Point AAD Page 11: AAD 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.

Benefit: Reduce opportunities for disruptive cyber incidents by providing real-time monitoring and anomaly-detection alerts
Check Point AAD Page 10 - Analyze specific scenarios simulating possible attack vectors that have the potential of compromising critical OT assets: By leveraging AAD 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.

Benefit: Support the oversight of resources (e.g., IT, personnel, and data)
Check Point AAD Page 9 - 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. 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.

Benefit: Enable faster incident-response times, fewer incidents, and shorter downtimes
Check Point AAD Page 9: - 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.

ADDITIONAL CHECK POINT VALUE IN ICS NETWORKS

The following benefits, included here for informational purposes, may be applicable to many ICS owners and are over and above those put forth in NISTIR 8219.

Provisioning

- Check Point Security Gateways provide the ability to limit traffic among assets groups based on different characteristics: Type, Vendor, Zone and more
- BAD alerts can be used for Incident response and enforcement by alerting/blocking traffic from malicious assets

Central Management and Integration

- AAD is an integrated component in the Check Point ICS solution.
- The AAD communicates with Check Point Security Gateways in the OT network that forward 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 the Check Point Security Management server where it is displayed to the user in SmartConsole.
- Firewall hosts are identified by assets names and details, e.g. 9PLC, HMI, etc. detected by the AAD

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.

CONCLUSION

The Check Point AAD ICS solution meets or exceeds all of the capabilities and benefits outlined in NISTIR 8219 and can better arm ICS and OT owners to combat cyber-attacks.

REFERENCES

[1] "Framework for improving critical infrastructure cybersecurity," NIST, Gaithersburg, MD, Apr. 16, 2018 [Online]. Available: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11
[2] Check Point Software Technologies. "AAD Asset and Anomaly Detection Data Sheet" Available: https://www.checkpoint.com/downloads/products/datasheets/ics-scada-asset-and-anomaly-detection-datasheet.pdf
[3] "Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection" NIST, Gaithersburg, MD, Nov., 2018 [Online]. Available: https://csrc.nist.gov/publications/detail/nistir/8219/draft