PALO ALTO NETWORKS SECURITY OPERATING PLATFORM INTEGRATION WITH SILENTDEFENSE

Resilience for critical infrastructure and data centers against cyberattacks and operational issues

Highlights

- Unprecedented visibility of industrial control system networks allows critical infrastructure organizations to assess, monitor and mitigate potential threats to their core.
- Integration of SecurityMatters and Palo Alto Networks technology provides real-time, automated protection against identified threats.
- Fast deployment, out-of-the-box checks for ICS threats and self-learning of normal network behavior in an integrated, automated security platform bring immediate ROI.

Challenge: IT/OT Convergence

Critical infrastructure operators face constant demand to increase productivity and reduce costs. To achieve these goals and accommodate management demands, operators are shifting toward the use of standard technologies as well as opening links between industrial and enterprise networks to enable real-time sharing of process information across these systems. Despite the clear business advantages, this paradigm shift has considerably reduced the resilience of industrial networks, and several issues have arisen, including the exposure of legacy systems with limited security mechanisms, the integration of technologies originally devised to address different issues, and the increasing complexity and criticality of the managed processes.

Although cases of cyberattacks on ICS networks are increasing, they are not the most imminent threats to the manufacturing industry. Cyber incidents occur daily, including small to major network or process disruptions due to misconfigurations, erroneous commands and operations, software errors, and device failures, which are not intentional but nevertheless affect asset owners' bottom lines.

To effectively protect their networks and avoid downtime, asset owners must be able to detect all these threats in a timely manner.

Security Operating Platform

Palo Alto Networks® is leading a new era in cybersecurity, serving more than 45,000 customers in more than 150 countries by protecting thousands of enterprises, governments, service providers and industrial networks from cyberthreats. Its Security Operating Platform comprises next-generation firewalls, advanced endpoint protection, comprehensive cloud security, and an array of cloud-delivered security products and services. The platform provides an integrated, multi-method approach focused on preventing attacks on the IT/OT environment across the entire attack lifecycle.

Figure 1: Palo Alto Networks Security Operating Platform

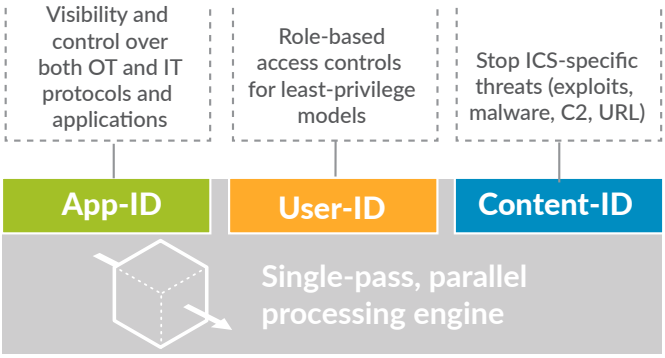

Figure 2: Next-generation firewall Layer 7 classification engine

Security Operating Platform

The next-generation firewall, with its innovative single-pass, parallel processing engine, or SP3, provides granular traffic visibility even to ICS protocols, applications and users. Plus, as the enforcing device, it allows users to segment their networks using intuitive Layer 7 business policies that reduce the attack footprint. App-ID™ technology, a component of the SP3 engine, gives users the ability to enforce policies based on a set of standards-based ICS protocols, such as Modbus, DNP3 and IEC 60870-5-104; and vendor-specific ICS protocols, such as Siemens S7, Honeywell/Matrikon OPC Tunneller and OSIsoft Pi. Through User-ID™ technology, organizations can easily realize role-based access controls where relevant within their OT environments. The Threat Prevention service works with Content-ID™ technology to further secure the allowed traffic by natively blocking known threats to both IT and OT, including ICS-specific exploits, malware, and associated command-and-control, or C2, traffic (see Figure 2). This helps organizations protect their unpatched or unpatchable systems until they can be updated or replaced.

For more sophisticated, unknown threats, WildFire® cloud-based threat analysis service quickly analyzes samples to determine their malicious/benign nature before sending protections back to the next-generation firewall to prevent malware propagation and C2 communications.

The NGFW runs PAN-OS®, which includes a powerful XML-based API that can be used to access and manage the NGFW through a third-party service, application or script. This allows for closed-loop, fully automated OT threat detection and response.

SilentDefense

SilentDefense™ from SecurityMatters is the most advanced and mature network monitoring and situational awareness platform for industrial networks. It employs full deep packet inspection capabilities and the Industrial Threat Library, which includes more than 1,300 ICS-specific threat indicators, to analyze standard and proprietary industrial protocols from all the major SCADA manufacturers and issue real-time alerts on any threats to operational continuity. These threats include network connectivity problems, device malfunction and misconfiguration, dangerous process operations, use of insecure protocols and default credentials, advanced cyberattacks, and exploit attempts.

SilentDefense is fully passive and therefore does not introduce any latency nor affect the monitored network or its devices. It can be deployed in a matter of hours and provides immediate visibility into existing problems and threats. By making use of patented anomaly detection technology that enables users to automatically baseline network communications, it also minimizes configuration effort. SilentDefense's self-learning visibility and detection engines allow:

- Automated graphical asset inventory and contextual vulnerability analysis.
- Continuous detection of port scan, MITM, protocol violations and lateral movements.
- Automatic profiling and monitoring of communication patterns, protocols and commands.
- Automatic profiling and monitoring of normal protocol fields and values.
- Network- and process-specific behavioral checks for time-based events, event correlation, etc.

This guarantees complete, real-time awareness, forensics and hunting capabilities to achieve full protection of the network as well as effectively respond to existing and emerging threats (see Figure 3).

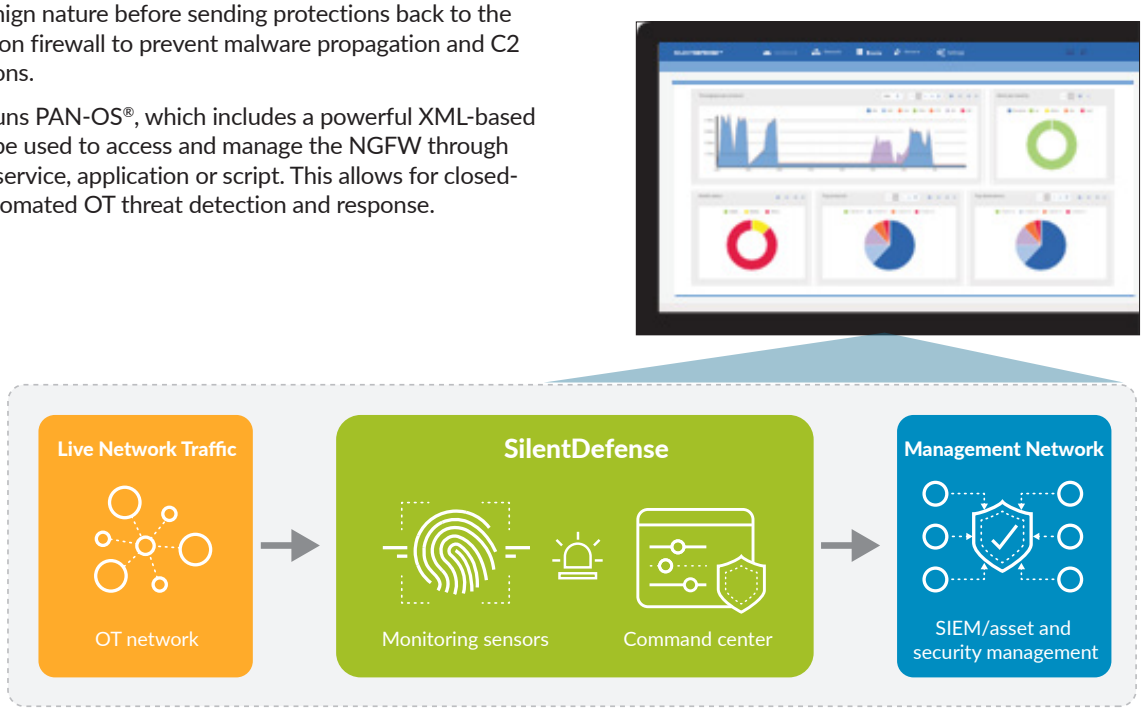

Figure 3: SilentDefense in the network

Security Operating Platform & SilentDefense

The partnership between Palo Alto Networks and SecurityMatters aligns the real-time detection and protection capabilities of the two companies, providing our joint customers with increased visibility and synchronized defenses to effectively combat today's advanced threats against industrial control systems, data centers and critical infrastructure organizations.

Joint customers can integrate Palo Alto Networks with SilentDefense in a matter of minutes by indicating which events SilentDefense should report to the Palo Alto Networks next-generation firewalls to trigger the creation of a new rule to block or limit the source of the threat, effectively preventing disruption of critical operations.

Benefits for our joint customers include unprecedented visibility into assets and data flows in their industrial control systems networks; automated, real-time response against potentially disruptive events; and end-to-end protection for their IT and OT networks.

Figure 4 shows the integration of Palo Alto Networks and SecurityMatters using a layered view of converged IT and OT environments, such as the Purdue and ISA-95 reference models. Users deploy SilentDefense sensors and Palo Alto Networks next-generation firewalls in strategic detection and prevention points. As the SilentDefense sensors discover threats, they can send real-time requests to the NGFWs to block or limit communications for a single node or between nodes.

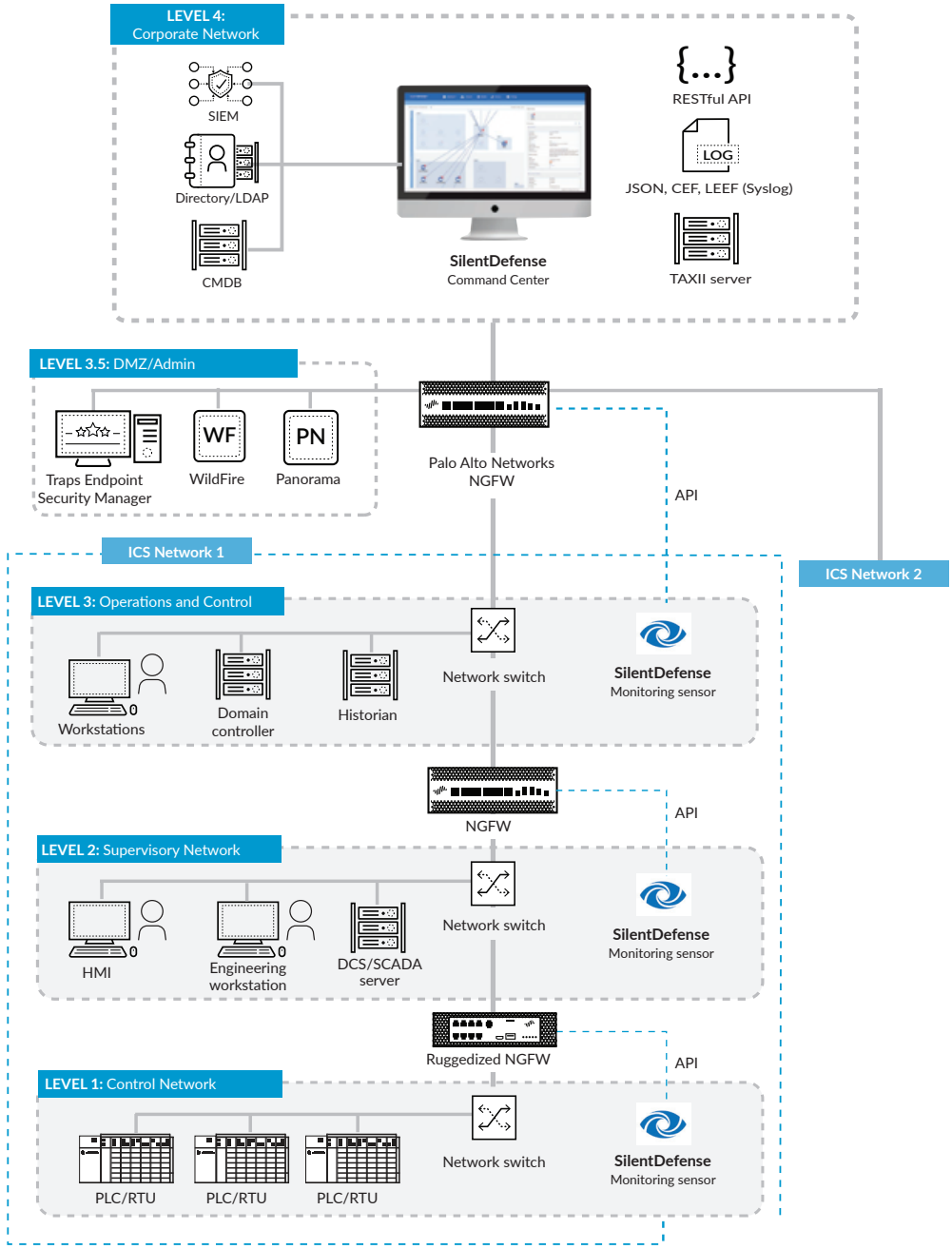

Figure 4: Palo Alto Networks and SecurityMatters integration

USE CASE: ELECTRIC POWER

Detection of Zero-Day Exploitation Against RTUs

Challenge

Grid operators use RTUs to control and collect information from remote substations. Palo Alto Networks firewalls allow asset owners to restrict access to RTUs, such as by allowing only the Energy Management Systems to communicate with them, and to limit the commands that can be issued to them. Despite these restrictions, it is still possible for an attacker or insider to disrupt operations by issuing a legitimate command with anomalous parameters, such as resetting the remote device, or worse, by putting it in a faulty status until a full power-off/power-on cycle is manually executed. SecurityMatters has discovered several similar unknown vulnerabilities over the years.

Approach

SilentDefense automatically generates a network whitelist based on communication patterns, down to the commands being sent, by observing and inspecting network traffic through complete packet dissection. This whitelist, which operators can fully customize, is later used to detect anomalies, such as out-of-range parameters. SilentDefense can be deployed within the main control center, such as the Energy Management System, to monitor all remote connections carried out from a single location, including remote locations such as electrical substations, to monitor incoming connections as well as local traffic from devices behind the RTU.

Response

SilentDefense can reconfigure Palo Alto Networks firewalls on the fly to block further attempts to exploit RTUs. In situations where an incident is suspicious but not clearly malicious, SilentDefense can instruct the NGFW to limit the kinds of commands the suspicious device can initiate over ICS protocols, such as DNP3, IEC 60870-5-104 or Modbus.

USE CASE: OIL & GAS

Detection of Zero-Day Exploitation Against an OPC server

Challenge

Open Platform Communications, or OPC, servers are typically used to share process and/or production data between different production and analysis systems. Organizations deploy firewalls to filter out unwanted and unauthorized communications, and only certain OPC message types are exposed to the corporate domain. In 2012, a previously unknown vulnerability was found in a widely deployed OPC server. The vulnerability allowed a remote attacker to exploit the ubiquitous OPC authentication interface by sending a large amount of data to trigger a buffer overflow and possibly execute arbitrary code on the target.

Approach

The network whitelist automatically generated by SilentDefense detects anomalous commands and parameters, such as out-of-range values that could indicate attempts to exploit a buffer overflow vulnerability, in real time. SilentDefense can be installed at remote sites within Layer 3 networks, where OPC servers are typically deployed. As SilentDefense supports a wide range of industrial protocols, including proprietary ones from ABB, Emerson, Yokogawa, Siemens and more, it can also be deployed within Layer 2 networks to detect anomalies and misuses occurring in process control networks.

Response

SilentDefense can reconfigure Palo Alto Networks firewalls on the fly to block further attempts to exploit other OPC servers. New IPS signatures can be deployed on the NGFW to protect vulnerable systems until patches can be deployed.

USE CASE: BUILDING AUTOMATION

Detection of Exploitation Against BAS Systems' Vulnerabilities

Challenge

Building Automation Systems, or BASs, are becoming ubiquitous in today's infrastructure, including in data centers, hospitals, airports and malls, and are the cornerstone of the Smart Cities vision. The cybersecurity of these systems has been neglected for a long time, and the underlying networks are seldom properly segmented, remaining vulnerable to various attack vectors. For example, it was such a situation that allowed the 2014 Target breach. These vulnerabilities can enable attackers to change temperature set points in climate-controlled environments, such as data centers, hospitals and research labs.

Approach

SilentDefense automatically generates a fine-grained blueprint of the various set points observed within the BAS by thoroughly observing and inspecting network traffic. Network operators can easily review and tweak this blueprint. Further, SilentDefense supports in-depth analysis of BAS protocols, allowing operators to monitor the behavior of devices over IP-based networks as well as inspect the traffic of devices connected over serial links to BAS gateways. During the detection phase, SilentDefense automatically detects and reports any deviations from the automatically learned values.

Response

SilentDefense can reconfigure Palo Alto Networks firewalls on the fly to block malicious devices and communications. In situations where the incident is suspicious, but not clearly malicious, SilentDefense can instruct the NGFW to limit the kinds of commands a suspicious device can initiate over ICS protocols, such as BACnet.

Other Resources That May Interest You

Brief: Visibility, Detection and Control for Industrial Networks

Learn more about the applications, benefits, integration and support of SilentDefense.

SilentDefense Datasheet

Read about the architecture, technical specifications, protocols and configurations of SilentDefense.

Want More Information?

To receive more information about SilentDefense and its benefits, please contact SecurityMatters at **info@secmatters.com** or visit **www.secmatters.com**.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

platform-integration-with-silentdefense-pb-060118