exabeam

WHITE PAPER

SECURING OPERATIONAL TECHNOLOGY FOR RAPID THREAT DETECTION AND RESPONSE

SUMMARY

A new generation of Industrial IoT devices leverage the internet for smarter Operational Technology (OT). These OT solutions serving a multitude of industry verticals are as vulnerable to global cyber threats as standard IT devices. OT solutions are often less secure because they focus on productivity; security was less important when they operated in a closed network system. As OT integrates with IT, lacking the right security tools makes it impossible to detect attacks on devices that operate automatically – especially legacy OT. Organizations using OT need to evaluate exposure and step up their ability to quickly detect and investigate OT anomalies, respond to and mitigate attacks. Providing OT device security can be challenging as many of these devices aren't designed to integrate with security management tools. The integration of security management for OT and IT is especially important because of IP connectivity: threats can easily move laterally from the enterprise into OT and vice versa. This white paper describes how to understand and address OT device risks with a cohesive security strategy. While OT security entails many controls for protecting devices from attack, the white paper focuses on an integrated approach for simultaneously monitoring OT and IT security and responding to incidents.

THE PROMISE AND THREAT OF OPERATIONAL TECHNOLOGY

Operational Technology (OT) devices and systems are the backbone of modern commercial automation solutions and Industrial Control Systems (ICS) for critical infrastructure. Many OT scenarios are mature with decades of experience and effectively-running systems that use "ancient" technology. Legacy examples include programmable logic controllers (PLCs) that run industrial electromechanical processes for manufacturing and robotics; open and close valves

for water, oil and gas; and turn circuits on and off to regulate flow of electricity. Newer scenarios include sensors on truck fleets, trains and drones enabling driverless operation, and Smart City sensors on public infrastructure informing automated systems when to turn streetlights on or off, change stoplight flow patterns, or empty a garbage can. OT enables unlimited possibilities for more cost efficient and reliable operations.

OT devices and systems are enabled with and managed by information technology – typically IP-based networks and back-end compute and storage resources on premises and in the cloud. Due to the similarity of IP connectivity, some OT devices are also called Internet-of-Things (IoT) devices – and while the idea is true, many IoT devices are purpose-built for consumer use. This white paper focuses on IoT devices used for commercial solutions and critical infrastructure so all are referred to here as "OT."

From a security perspective, networks controlling OT devices and their functions used to be separated from the enterprise network to ensure safety and prevent unauthorized access. Many legacy OT devices and solutions, however, are increasingly being connected to IP networks and the internet to enable centralized command-and-control and remote access. Other purpose-built OT devices (also called Industrial Internet of Things or IIoT) provide native integration with IP networks.

Whether OT devices are dumb or smart, simple or complex, the shared characteristic of IP connectivity over the global internet has established their nearly universal exposure to the same cyberthreats associated with enterprise IT. For with IP, everything connected is vulnerable.

OT DEVICES AND SYSTEMS REQUIRING SECURITY

- Supervisory control and data acquisition (SCADA)
- Process control networks (PCN)
- Distributed control systems (DCS)
- Manufacturing execution systems (MES)
- Telematics
- Robotics
- Facilities management / building automation systems

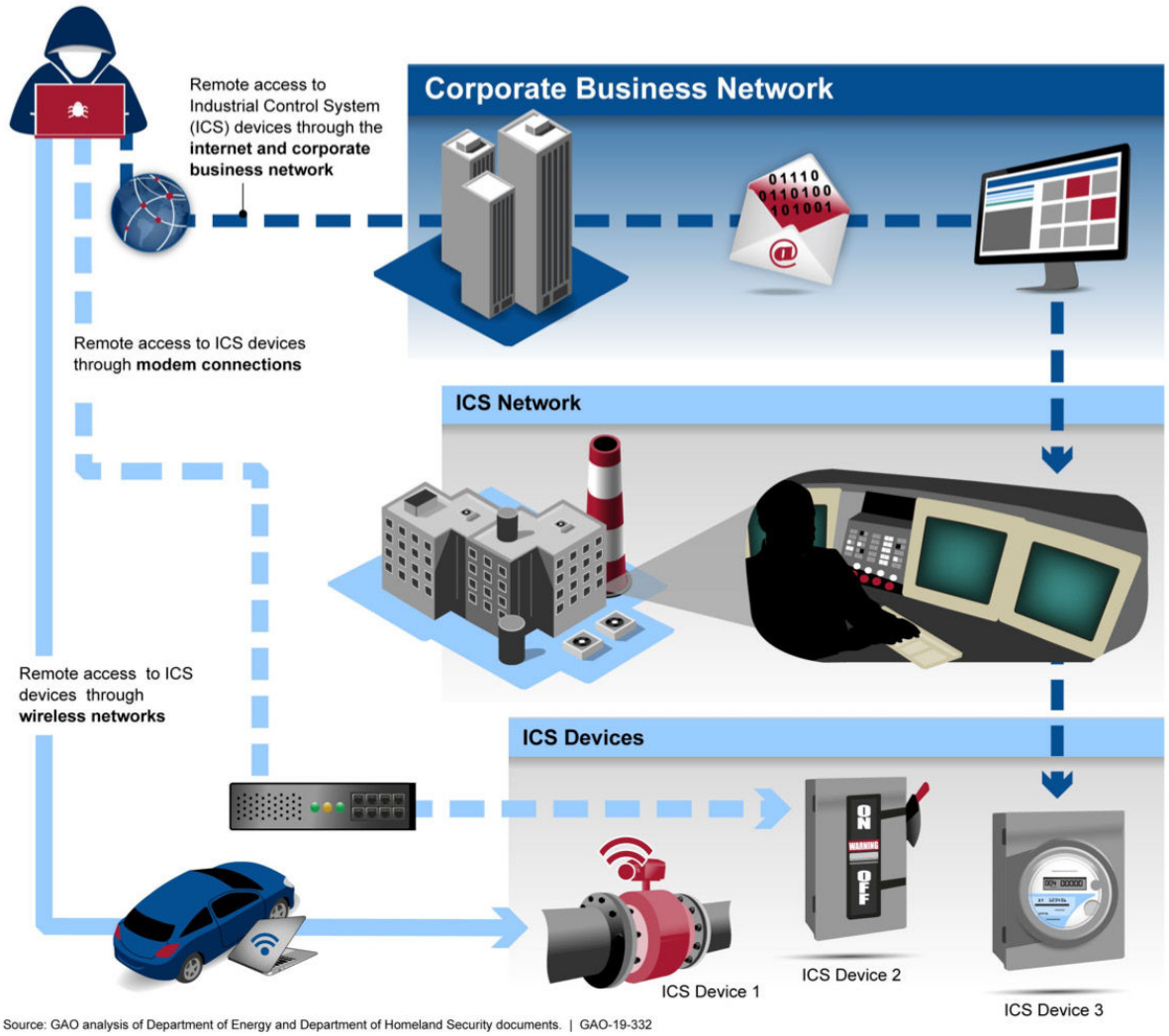
Source: Gartner Market Guide for Operational Technology Security (30 July 2018)

The requirement for securing OT devices is vital to continuity of critical services, protecting the nation, and ensuring the safety of people. For this reason, U.S. Federal Policy Directive 21 ("Critical Infrastructure and Resilience") and the National Infrastructure Protection Plan (NIPP) call for a "unified national effort to strengthen and maintain secure, functioning, and resilient critical infrastructure."[1]

The adjacent diagram by the Government Accountability Office shows multiple vectors threatening OT. Organizations wishing to step up security for IP-connected OT devices are often challenged by a siloed process. The big obstacle is systemic: people managing OT are frequently different from enterprise security professionals who manage IT security via a security operations center (SOC). Moreover, OT-focused teams may not have deep experience with IP security tools for threat detection and response. The lack of expertise is serious because vulnerabilities in one organization's OT can easily affect its IT, and vice versa.

[1] See https://www.dhs.gov/cisa/supporting-policy-and-doctrine

POTENTIAL WAYS AN ATTACKER COULD COMPROMISE INDUSTRIAL CONTROL SYSTEM DEVICES



Source: GAO analysis of Department of Energy and Department of Homeland Security documents. | GAO-19-332

For example, a smattering of reported breaches to critical infrastructure such as the electric power grid may be the tip of the iceberg due to reluctance of announcing vulnerabilities and exploits. In March 2019, a power grid attack occurred in the western U.S., according to the North American Electric Reliability Corporation (NERC). A vulnerability in firewall firmware caused several to reboot and go offline for nearly 10 hours.[2] Operators at a power control center repeatedly lost communication with "multiple power generation sites" for several minutes at repeated intervals. Other incidents caused by a variety of vulnerabilities are documented by NERC.[3]

[2] See https://www.nerc.com/news/newsletters/Newsletters/NERCNews-2019-09.pdf, https://www.secureworldexpo.com/industry-news/first-u.s.-power-grid-attack-details, and "Lessons Learned" for this incident in https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/20190901_Risks_Posed_by_Firewall_Firmware_Vulnerabilities.pdf

[3] https://www.nerc.com/pa/rrm/ea/Pages/Lessons-Learned.aspx

Incidents like these show why security for an organization's OT and IT needs an integrated approach to quickly identify and respond to related incidents. SOC managers who are being pulled into the erstwhile separate orbit of OT may be unfamiliar with security-related idiosyncrasies of OT devices or how to bring them into coverage by enterprise security tools. The next section describes a model for integrating OT device security with enterprise IT security to provide a centralized, organization-wide view that enables rapid detection, investigation, response and mitigation of internet-borne threats.

FRAMING THE CHALLENGE OF OT SECURITY

Siloing security management for OT and IT security is not the only challenge. Some legacy OT was or continues to be air gapped to ensure operational integrity and control. But as various architectures allow connecting legacy OT to the internet for modern operational command-and-control, IP connectivity also brings exposure to internet-borne exploits.

Siloed efforts for security of OT and IT mean there is no enterprise view of risks, nor is there an integrated enterprise capability for rapid threat detection and response across all types of connected technology.

OT devices carry intrinsic security challenges. They are deployed over a wide attack surface with numerous threat vectors such as authentication and authorization, software, device threats, network threats, and OS-level vulnerabilities. Many OT devices do not provide a rigorous patch or upgrade routine, which pretty much ensures they will forever be exposed to persistent vulnerabilities on the internet.

OT DEVICES BRING RISKS TO CRITICAL INFRASTRUCTURE

Chemical
Commercial Facilities
Communications
Critical Manufacturing
Dams
Defense Industrial Base
Emergency Services
Energy
Financial Services
Food and Agriculture
Government Facilities
Healthcare and Public Health
Information Technology
Nuclear Reactors, Materials, and Waste
Transportation Systems
Water and Wastewater Systems

Source: https://www.dhs.gov/cisa/critical-infrastructure-sectors

It's almost guaranteed that legacy OT devices will have no integrated capability for security management. Surprisingly, this is often true even for new "IIoT" devices.

Eventually chip and OT device manufacturers will achieve greater success in addressing this state of general insecurity. Meanwhile, organizations that use old and new OT alike must deal with what they've got and determine an immediate path for stronger OT security. As a starting point, let's consider requirements for monitoring OT devices.

UNDERSTANDING HOW TO MONITOR OT DEVICES

Detecting an attack on OT requires baseline security monitoring of all devices in the OT system. Monitoring OT devices is a specialized task for solutions from several companies focused on SCADA, ICS, PLCs, and servos. Examples of these OT-focused security monitoring vendors include Armis, Claroty, Corelight, DarkTrace, ExtraHop, Indegy, Nozomi, Stealthwatch, Vectra and others. All have special expertise in OT protocols such as DNP3, Modbus, Profibus, and of course IP-standard network protocols. Organizations without OT protocol expertise will need to use a third-party solution for monitoring OT devices. Frequently, OT monitoring solutions integrate with external sources for analytics and response automation, such as Exabeam SIEM Management Platform.

Native security monitoring capability is often baked into newer IoT and IIoT devices. Native security allows these devices to automatically transceive security data with the central OT monitoring solution. While this is an ideal scenario, the possibility of native security is slim-to-none with legacy OT devices due to their limited memory or processing capability.

If an OT device has adequate on-board resources, you may be able to install a security agent to implement monitoring. The agent facilitates automatic transmission of event logs to the monitoring server. Currently, about half of OT devices can send logs via the Syslog protocol. Other scenarios require operational data to be retrieved from the OT device via a polling mechanism. In some cases, the device may support an "agentless" solution that communicates directly with a monitoring server.

In scenarios where OT devices have no extra available memory or processing capability, gathering event data is more challenging. One approach is to automate periodic device polling with scripts to get around lack of security software on legacy OT devices. Another is to monitor the devices by their network activity.

Network traffic analysis is interesting because OT devices typically operate without human action. They are pure machines, which means understanding their "behavior" in an attack chain requires a different approach from traditional security tools that monitor IT activity based on direct human actions. To accomplish this, we turn to Entity Analytics as applied to OT device activity.

HOW ENTITY ANALYTICS ADDRESSES OT DEVICE RISKS

OT devices are automated machines, which excludes them from typical IT security awareness programs such as warning users to use strong passwords or avoid unusual contacts phishing for access credentials or other information helpful for defeating controls. Despite the automated use of OT devices, they do share a trait with human users in that OT devices also use the internet for connectivity and execution of their individual tasks. By classifying OT devices as eligible for behavior processing with a technology called User and Entity Behavior Analytics, or UEBA.[4]

User and Entity Behavior Analytics is one of the fastest-growing areas within enterprise security, growing at a compound annual growth rate of 48% per year, according to Gartner.[5] Modern enterprise IT security solutions use this technology to detect and remediate advanced threats that are unable to be addressed by legacy solutions.

[4] For more background, see Exabeam, "Top 10 UEBA Security Use Cases"

UEBA solutions ingest operational data from many sources, and use analytics such as machine learning and behavior analysis to determine what is "normal" behavior by users and entities on an enterprise network. Entities may include IT assets such as hosts, applications, network traffic and data repositories – and virtually any IIoT or OT device. Our focus here is on Entity Analytics fueled by event data from OT devices and systems.

The solution builds standard profiles of OT device behavior across peer groups and over time in order to create a baseline. For example, if OT devices for an oil and gas valve controller system are usually accessed from specific designated operators using specific computers at a specific location, an Entity Analytics system can instantly detect an abnormal attempt to access those OT devices.

As anomalous activity is identified, it is assigned a risk score. The score rises with increasing amounts of anomalous behavior until it crosses a predefined threshold. Upon this escalation, Entity Analytics sends an alert to Security Operations Center analysts who use the data for investigation and appropriate remediation of threats.

Entity Analytics is important for OT security because legacy tools are often unable to detect abnormal behavior of OT devices. Typical attempts to monitor this activity result in swamping analysts with alerts that are difficult to understand and are often useless for rapid detection and remediation. As part of a UEBA solution, Entity Analytics employs a different approach by using variations of artificial intelligence and machine learning, advanced analytics, data enrichment, and data science to effectively detect and thwart OT threats. The Entity Analytics solution combines all the data sources together for analysis and automatically

[5] See https://www.gartner.com/reviews/market/user-and-entity-behavior-analytics

CASE STUDY: SECURING OT FOR NATURAL GAS & ELECTRICITY

Customer: A regional natural gas and electric utilities company serving 1.2 million customers in the United States.

Challenge: Enable compliance with the North American Electric Reliability Corporation Critical Infrastructure Plan NERC CIP-007-6, Requirement 4 to summarize or sample logged events on OT at intervals no greater than 15 calendar days to identify undetected cyber security incidents. The OT includes specialized devices that control critical processes for the delivery of natural gas and electricity. Centralized monitoring required by NERC CIP also helps identify and prevent the spread of attacks from OT to interconnected IT throughout the enterprise. Some of the OT devices used are more than 30 years old but are perfectly functional. However, due to limited memory or on-board processing capacity, it was impossible to simply "plug in" many OT devices to the company's legacy rules-based Security and Information Event Management (SIEM) tool.

Solution: Customer was at the time modernizing its SIEM by migrating to Exabeam Advanced Analytics to model behavior of its enterprise users for IT security detection and response. The company decided to also apply this approach for its OT with Exabeam Entity Analytics (EA). This solution uses machine learning to monitor the behavior of OT devices – especially of devices that do not automatically send log data for security monitoring. With experience gained by various techniques used to normalize OT data input for the legacy SIEM, the SOC team easily ported those processes for automatically sending data to Exabeam EA. "Exabeam is very flexible in allowing us to use many options for getting the data – even if it requires using an upstream device to interpolate downstream activity." The company also has integrated its physical access control system into some use cases, such as badging in prior to logging onto critical OT devices and systems.

Result: With Exabeam EA, they centrally integrated security for OT and IT across the enterprise. The solution has simplified NERC CIP compliance and enabled a deeper degree of visibility and insight on potential issues threatening operations and the safety of its natural gas and electricity delivery systems. "Our shift in security monitoring from a legacy rule-based system to behavior modeling is a huge win for the SOC team. Exabeam reduces the number of things we are chasing every day. Before we chased everything; now we don't have to. Exabeam also lets us address security for more devices without having to add extra people."

synthesizes results. Analysts get a lower volume but higher fidelity feed instead of drowning in alerts. The result is faster, more effective detection and response to active threats.

The use of Entity Analytics with a modern Security Information and Event Management (SIEM) system helps accelerate detection and response by providing organizations with a multitude of typical use case models. In conjunction with use case models, a modern SIEM will also provide auto-generated timelines for each event to help SOC analysts automate detection, response and mitigation of threats to OT devices.

OT SECURITY INTEGRATED WITH A MODERN SIEM

Rather than treat OT as a distinct silo for protection, Exabeam integrates Entity Analytics capability with a modern SIEM platform. Using a modern SIEM as the foundation for security provides an organization with an enterprise-wide view of all IT, OT and network security. It doesn't matter which architectures are used to connect OT or IT devices. Exabeam SIEM is device and network agnostic; it can ingest and analyze all the data from all of an organization's sources, allowing one SOC team to keep a real-time view on all security.

Whether monitoring a local network or assets from a power grid, SOC analysts view data from many security solutions that, when viewed in isolation might appear benign. Exabeam ingests and analyzes logs from VPNs, cloud applications, email services, firewalls, Netflow, and of course OT device sensors and systems. Machine learning and behavioral modeling analyze the input from all these sources, detecting complex threats on OT that would otherwise go undetected.

EXABEAM SIEM REDUCES THE IMPACT OF ATTACKS ON OT ASSETS AND SYSTEMS

Extends visibility into OT environments by providing a centralized event data repository for IT and OT security

Detects anomalous behavior and complex threats like lateral movement – which can spread between corporate and OT networks – with user and entity behavior analytics

Reduces response times and improves productivity with machine-built incident timelines for OT assets

Automates remediation and response for OT assets displaying unusual activity with response playbooks

For every incident under investigation, Exabeam SIEM automatically creates Smart Timelines. These are behavior-aware timelines where events and associated risk reasons are correlated with contextual data. Using behavioral analysis, Smart Timelines provide analysts with normal and abnormal behaviors for users and OT devices. This includes lateral movements, abnormal file/data uploads to external assets, abnormal account switching and anomalous asset logins. Smart Timelines make it easy for SOC analysts to pinpoint anomalies and quickly mitigate incidents by seamlessly pivoting from user to assets.

The single pane of glass view on enterprise-wide security helps the SOC to ensure that security event detection and response is applied exactly as needed, wherever it is required.

SUMMARY

Organizations are seeing a growing number of attacks to OT environments that can shut down or disrupt production lines and critical infrastructure. Many major OT attacks originate in exploited vulnerabilities within IT systems before pivoting to OT systems. Unfortunately, many organizations treat OT security differently than IT security, and in doing so fail to build a cohesive security strategy. This approach leaves OT vulnerable to attacks.

Instead, organizations should merge their OT and IT security operations and extend their IT security practices to their OT environments. This approach will help organizations to continuously improve security against attacks that exploit vulnerabilities in IT systems and then move laterally to attack OT systems.

Your organization can strengthen OT and IT security with a modern SIEM using User Behavior and Entity Analytics. Exabeam integrates these advanced analytics capabilities to help unify security monitoring and response across all IT and OT used by your organization.

We invite you to learn more by requesting a demonstration of the Exabeam Security Management Platform at https://www.exabeam.com/product/exabeam-entity-analytics/.

exabeam

ABOUT EXABEAM

Exabeam is the Smarter SIEM™ company. We help security operations and insider threat teams work smarter, allowing them to detect, investigate and respond to cyberattacks in 51 percent less time. Security organizations no longer have to live with excessive logging fees, missed distributed attacks and unknown threats, or manual investigations and remediation. With the modular Exabeam Security Management Platform, analysts can collect unlimited log data, use behavioral analytics to detect attacks, and automate incident response, both on-premises or in the cloud. Exabeam Smart Timelines, sequences of user and device behavior created using machine learning, further reduce the time and specialization required to detect attacker tactics, techniques and procedures. For more information, visit https://www.exabeam.com.

TO LEARN MORE ABOUT HOW EXABEAM CAN HELP YOU, VISIT **EXABEAM.COM** TODAY.