SEALINGTECH
a PARSONS Company

GARLAND TECHNOLOGY
See every bit, byte, and packet®

RESPOND QUICKLY AND RECOVER WITH CONFIDENCE

OT INCIDENT RESPONSE WITH SEALINGTECH & GARLAND TECHNOLOGY

THE CHALLENGE

OT incident response is inherently different from IT incident response due to the different devices, communication protocols, and attack techniques used by threat actors to penetrate critical infrastructure environments. With regard to industrial control systems, any sort of disruption due to cyber attacks can be more than just lost revenue and system downtime. In these types of environments, human life and environmental safety can be at risk, which is why it is important to ensure that mission-critical infrastructure is secure and running properly.

It is typical to come across legacy equipment in industrial environments due to strict restrictions on the installation of software and hardware in OEM-supported systems that operate critical processes. This means that incident response teams must be prepared with the ability to collect traffic when Layer 2 switches are unmanaged, unavailable, or potentially need to utilize media that would otherwise be considered outdated.

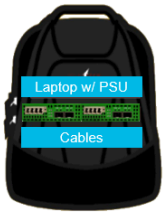
THE SOLUTION

For Assessment and Incident Response (IR) teams to have the equipment needed to perform a variety of detection, forensics response, and recovery activities, they turn to Fly-Away Kits stocked with Garland Technology Network TAPs and Aggregators, Sealing Technologies (SealingTech) servers, Intrusion Detection Software, and other best of breed tools to ensure the team can respond to any scenario they face.

When an IR team enters an ICS environment, they can use a Fly-Away Kit to not only detect and mitigate the effects of a cyber attack but also act as a temporary SEIM solution. The hardware is designed to provide the infrastructure and computing power needed to establish a basic level of cybersecurity that can last for months rather than just a few days or weeks. This allows organizations to analyze their environments and build and deploy a comprehensive cybersecurity solution across their enterprise. In addition, the kit brings additional value as IR teams can utilize it for future IR deployments, enhance a growing network, and add extra layers of protection when required.

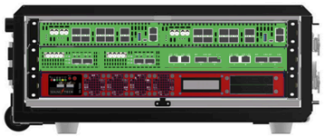
Case #1

- 1x 1U Half-width SFP drawer
- 3x SN3120: 20 Cores, 128GB RAM, 15TB NVMe
- 1x Palo Alto Firewall
- 1x SW2050 Network Switch



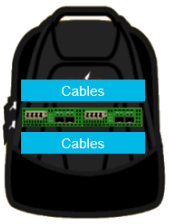
Backpack #1

- 1x Provisioning Laptop w/ PSU
- 2x Garland Taps
- Cables/SFPs



Case #2

- 1x Garland Packet Broker
- 4x Garland Taps
- 1x SN5064: 64 Cores, 512GB RAM, 90TB NVMe



Backpack #2

- Cables
- 2x Garland Taps
- Cables

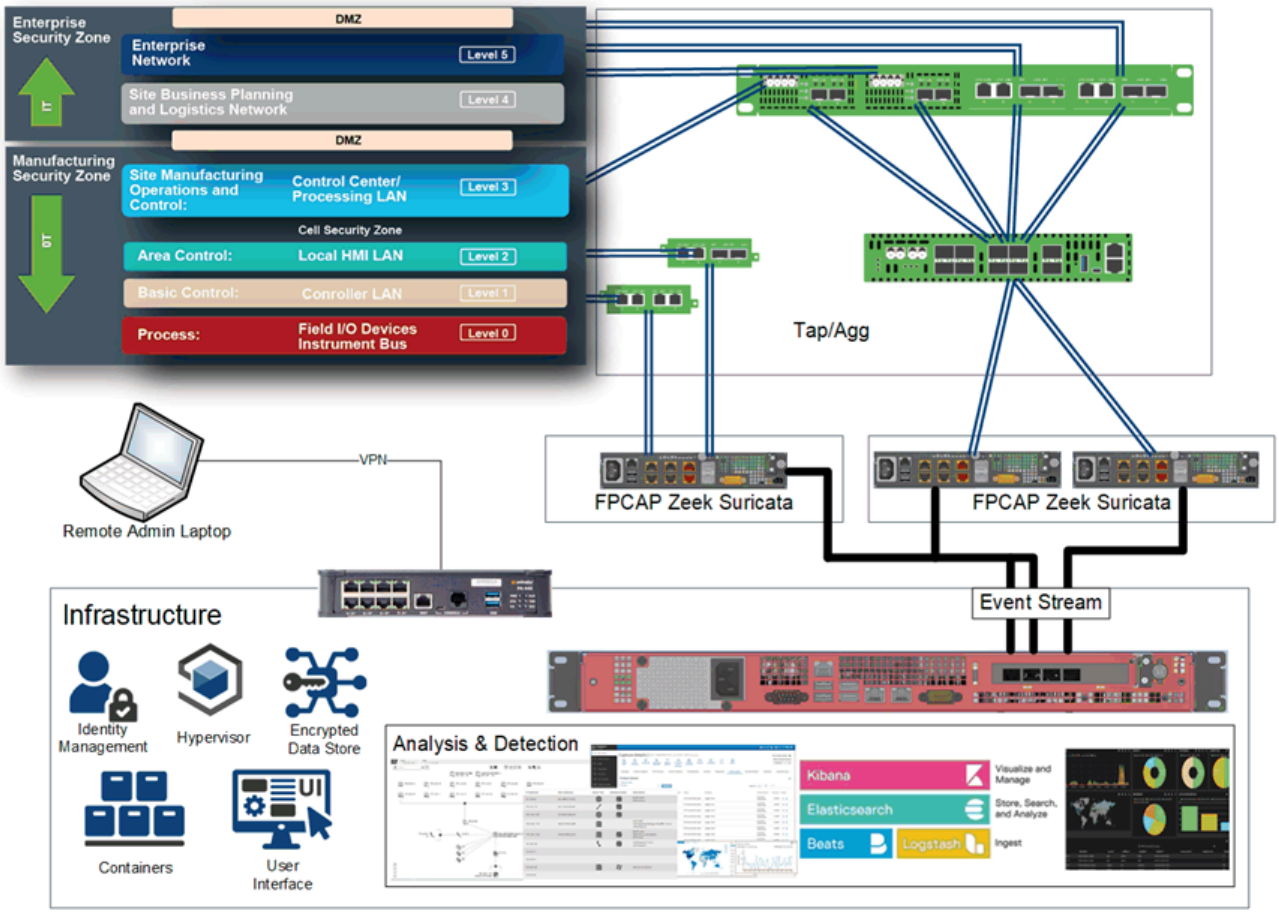
Potential Tool Integrations*

elastic · Elastic Stack · Elasticsearch · Rocky Linux · SURICATA · SOS Security Onion SOLUTIONS
Kibana · paloalto · Elastic Security · zeek · KVM

AGGREGATE SPECS PER KIT		
CORES	MEMORY	BULK STORAGE
124	896GB	135TB

*Not all-inclusive; Enquire about different integration opportunities.

Our passive first approach to data collection ensures that the networks remain protected without introducing additional risk and workload to assets within the environment. Our approach also leverages technologies designed for use in and compatibility with OT / ICS network environments. Utilizing Garland Technology Network TAPs provides access to 100% of the network traffic, which is then aggregated using a Network Packet Broker before being sent to the sensors for passive deep packet collection and inspection. The sensors can preprocess data to perform real-time threat analysis and offload pertinent data to an analytic node(s) for further in-depth analysis. The collection techniques are used to make a direct copy of packets from the ICS environment to allow for passive inventory of assets and the identification of events and incidents occurring within the environment. Full packet capture ensures the incident responder has access to important metadata like header information, protocol, etc., but also ensures that they have access to the full payload in the event that a confirmed incident warrants full in-depth forensic analysis.



WHY SEALINGTECH & GARLAND TECHNOLOGY

By partnering with SealingTech and Garland Technology you can arm your teams with innovative edge-computing solutions tailored to their unique assessment, compliance and incident response needs. Our technology has been proven in the field in some of the most demanding cybersecurity missions, and we have leveraged our expertise to develop a range of industry-leading edge computing and purpose-built network devices, ready to handle the toughest tasks and ready to be deployed anywhere a cyber operation is needed.

- Enable rapid response by IR teams with pre-configured Fly-Away Kits
- Reduce travel costs by leveraging commercial travel options
- Reduce setup time and tear down time
- Guarantee 100% network traffic with no dropped packets
- Small form factor TAPs and Aggregators allow for complete solutions
- Purpose-built technology, Made in the USA

Sealing Technologies, a Parsons Company (NYSE: PSN), rapidly delivers innovative cybersecurity solutions that modernize, protect, and defend the networks and systems of the Federal Government and private industries. Proudly veteran-founded, SealingTech uses vast cyberspace experience and knowledge to provide cutting-edge research, engineering, and integration services that support the United States and its allies. For additional information, visit sealingtech.com.

Garland Technology is an industry leader delivering network products and solutions for enterprises, service providers, and government agencies worldwide. Since 2011, Garland Technology has developed the industry's most reliable test access points (TAPs), enabling data centers to address IT challenges and gain complete network visibility. For more information or to learn more about the inventor of the first bypass TAP, visit GarlandTechnology.com.