SOLUTION BRIEF

A Strong Cyber Defense Wherever the Mission Takes You

SOCS OF THE FUTURE: PROJECT MEDICI MOONS

Detecting Advanced Adversary Activity Across Your Entire Enterprise

Better Integration. Deeper Insight. Quicker Response.

Deploy the full SOC capability of the naval base to the tactical edge of your network. By improving how you collect, analyze, and disseminate information, you can deliver aggregate and corelate data for deeper insight to improve your incident response, because when your team knows better, they do better.

The enterprise is made up of tens to hundreds of disparate networks that do not, or cannot, leverage each other's indications and intelligence. SOC defenders at regional and global levels struggle to rapidly tie indications of an event to a specific host at the tactical level and can be blind to lateral movement in these networks. The varying levels of defense throughout the enterprise, coupled with potential delays in identification, analysis, and remediation provides access points that make it easier for the adversary to potentially exploit unnoticed. As a result, the adversary may be able to cross from cyber threats to inflicting real world consequences in a kinetic conflict, providing an upper hand in the global arena.

Project MEDICI MOONS is the SOCs of the Future Architecture that addresses the need for greater threat awareness, validation, rapid response, and remediation. Medici Moons is a next-generation, distributed SOC design that improves the collection, curation, and analysis of information to arm security teams with actionable intelligence for better preparation for today -and tomorrow's- cybersecurity risks. With its multiple SOCs, advanced sensors, and numerous potential technical innovations, the Medici Moons design shows that new technologies and updated tactics, techniques, and procedures are required to protect our nation against all our adversaries.

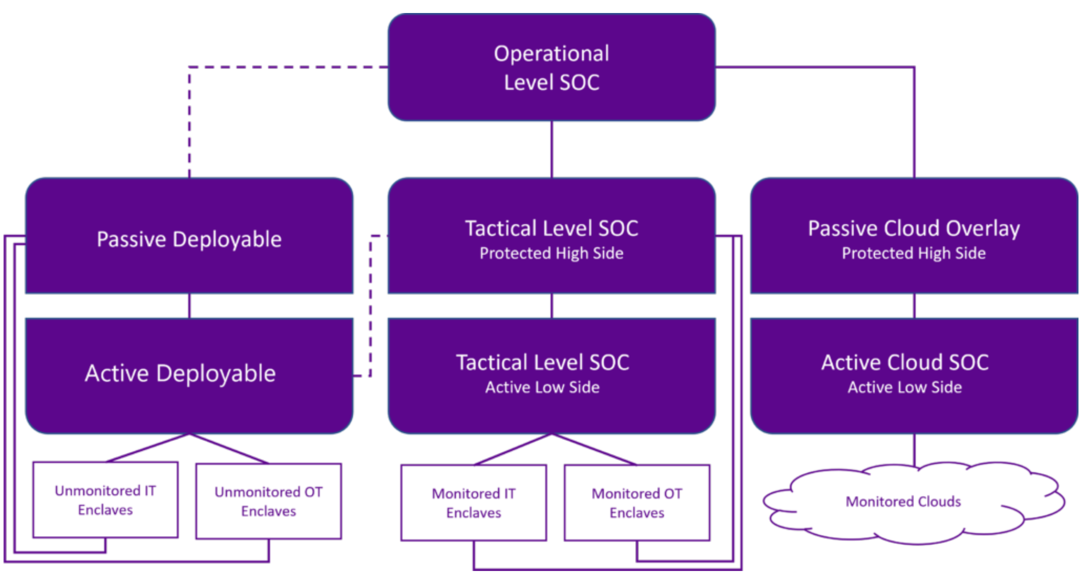


Figure 1. SOCs of the Future: Project Medici Moons Simplified Architecture

The MEDICI MOONS Architecture

SOC of the Future (SoTF)

The MEDICI MOONS design includes a distributed, operational-level cybersecurity operations center (CSOC) which manages and receives data from the tactical-level CSOC. The tactical CSOC is made up of an active, low-side enclave that provides initial collection and automated response and a secondary passive,

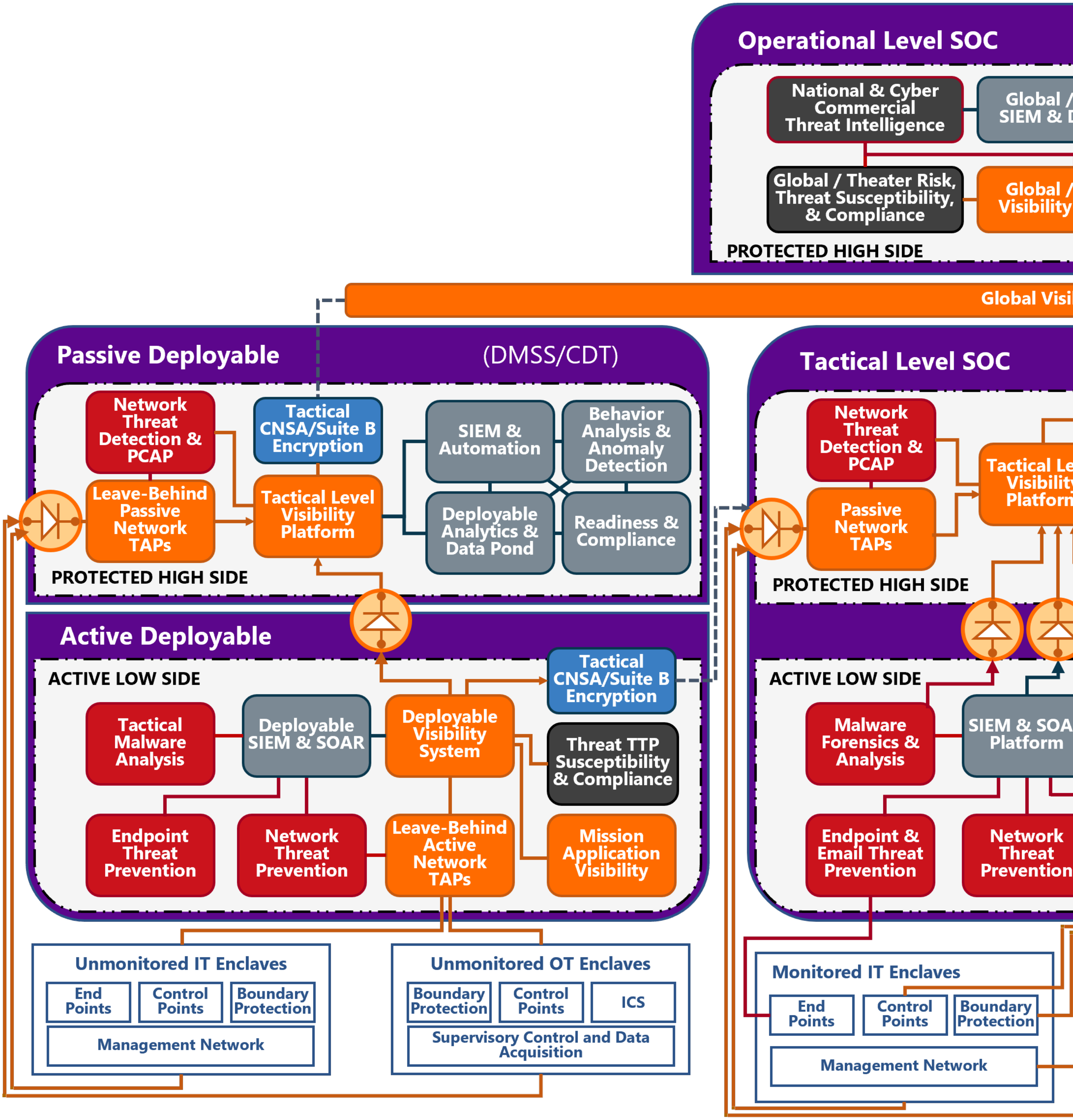
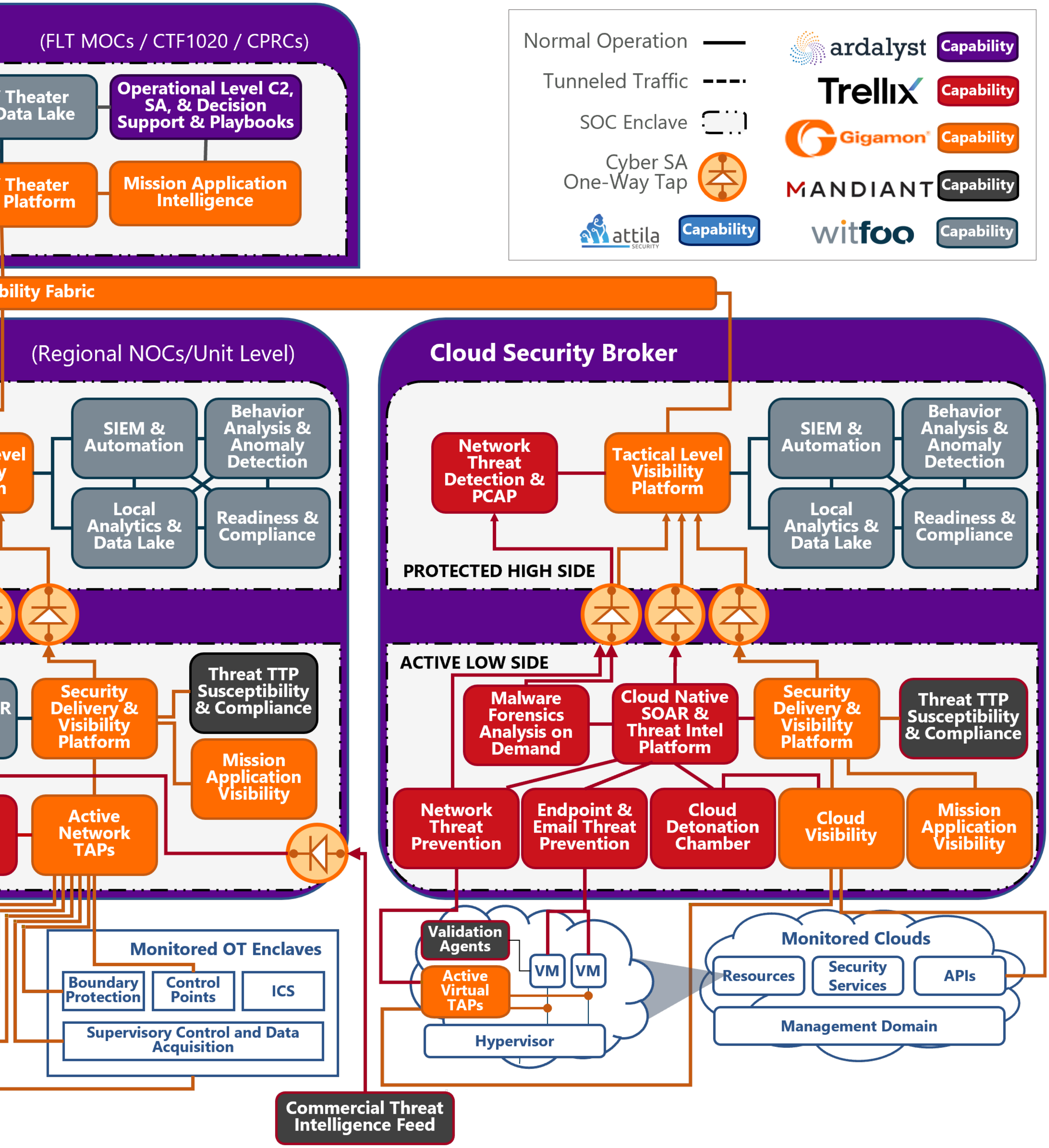


Figure 2. SOCs of the Future:



MEDICI MOONS Architecture

high-side enclave that provides out-of-band collection activities. The design leverages capabilities for use in a deployable support system and cloud-based environments to enable active and passive capabilities from sea to cloud.

The MEDICI MOONS Project Team leverages best-of-breed, commercial-off-the-shelf (COTS) products to provide a common platform that meets the SoTF requirements, integrating the following platforms:

The most capable rugged server system on the market. - Hewlett Packard Enterprise's Edgeline servers are unmatched. Plug and play blades allow reconfiguration on the fly without having to power down the chassis. With the travel case it is a data center on wheels.

Threat Visibility – The Mandiant Advantage Platform provides unparalleled visibility and expertise into threats to provide insight into what the adversary is doing right now.

Trellix Security Operations Platform – provides next generation security orchestration with the integration of machine learning, detonation chambers, and the leading commercial Threat and Victim Intelligence-based Analytics and Signatures provider into a single platform.

Security Delivery & Visibility Platforms – provides visibility from physical, virtual and on- and off-premises cloud environments to FireEye and other security appliances for inspection, collection, or blocking at a global scale.

Network Visibility – Gigamon GigaVUE® V Series and Cloud Suite enable security and monitoring tools to gain full network visibility, providing a holistic visibility and analytics fabric solution that eliminates network blind spots. Load balance and send relevant traffic to analytic tools, reducing compute and transport cost.

Automated Threat Management - WitFoo Precinct leverages crowdsourced cybersecurity expertise to combine and consolidate massive amounts of disparate data into meaningful, investigable incidents, the object-oriented SOAR can deliver higher fidelity confidence to perform automatic or manual remediation actions.

Secure over any connection – with Attila GoSilent even the least secure connections become incredibly secure. Built to adhere to even National Security standards, GoSilent protects data to the highest levels.