FORTINET

NSE Training Institute

BROCHURE

Fast Track Program

Experience the Fortinet Security Fabric in Action!

Experience the Fortinet Security Fabric in Action

FAST TRACK PROGRAM

Get a head start and stay at the cutting edge of network security by experiencing the Fortinet accelerator program, the Fast Track Program. The program consists of a series of short, comprehensive workshops that cover important topics in cybersecurity.

Fortinet created the Fast Track Program to support your pursuit of the technical expertise and knowledge required to take full advantage of the Fortinet Security Fabric and protect your network against all current and future security threats.

WHO CAN ATTEND?

Any interested Fortinet user can attend the Fast Track Program: new or proficient. Regardless of experience level, all attendees will walk away with a better understanding of how Fortinet can benefit their organization.

WHAT DOES IT COST?

The Fast Track Program is delivered as a complimentary service to our customers and partners.

WHERE AND WHEN CAN YOU ATTEND?

Fast Track is a global program, so to meet the needs of participants around the world, Fast Track sessions are scheduled regularly through your local Fortinet sales and partner teams.

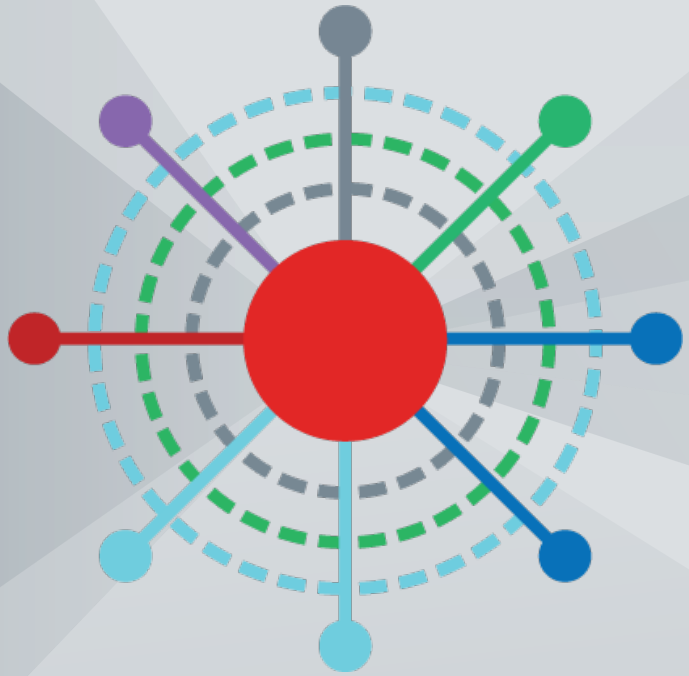
WHAT DO I NEED TO PARTICIPATE IN A FAST TRACK PROGRAM?

A laptop with a current browser.

For more information, or if you would like to register for an upcoming Fast Track workshop, contact your local Fortinet representative.

Creating a Comprehensive Fortinet Security Fabric

Networks today are expanding rapidly. At the same time, the threat landscape is growing faster than ever. Having security that solves the challenges of today's highly adaptive threat landscape, while protecting the entire dynamic environment, is more critical than ever.



How can you manage this high risk and complex issue?

Today's new world of networking requires a new approach to security that can do the following: simply, yet intelligently, secure the entire infrastructure; deliver full visibility into every viable network segment and the devices and endpoints behind them; and seamlessly integrate with third-party solutions, enabling users to ubiquitously collect, share, and correlate threat intelligence.

In this workshop, participants learn about the Fortinet Security Fabric, the first ever architectural security approach designed to dynamically adapt to today's evolving IT infrastructure. This multi-layered approach provides broad, integrated, and automated protection against sophisticated threats.

Participants who attend this workshop will learn how to:

- Introduce the Fortinet Security Fabric and the main business drivers
- Detail specific components that make up the Security Fabric
- Build a comprehensive solution to prevent, detect, and respond to security incidents using the broad, integrated, and automated approach.

WORKSHOP SUMMARY

FORMAT	4-hour technical workshop
OBJECTIVE	Provide a compelling, hands-on learning experience about the Fortinet Security Fabric that teaches participants how to craft a comprehensive security solution that solves the challenges of today's highly adaptive threat landscape while protecting the entire dynamic environment.
WHO SHOULD ATTEND	Anyone, regardless of prior knowledge of Fortinet products
PREREQUISITES	None
COST	Free of charge
INTERESTED?	Contact your local Fortinet representative

What's New in FortiOS?

To address today's risks and deliver the industry's most comprehensive cybersecurity platform that enables digital innovation, Fortinet continues to enhance the Fortinet Security Fabric with the latest version of its operating system, FortiOS. The Fortinet Security Fabric is the result of almost 20 years of innovation, organically built from the ground up to be broad, integrated, and automated. Every element of the Security Fabric—from the next-generation firewalls, to the access points and switches, to the network access control (NAC) solution—is engineered to work together, while also integrating with one of the industry's largest technology alliance partner ecosystems.

Did you know that the new FortiOS features and capabilities were designed to provide broad visibility, integrated threat intelligence, and automated responses that are required for digital business?

In this workshop, participants will learn about the new FortiOS features and capabilities that were designed to provide the broad visibility, integrated threat intelligence, and automated response required for digital business. Participants will have the opportunity to try out these features in the hands-on lab.

Participants who attend this workshop will learn how to:

- Use the Security Fabric improvements to provide IT teams with a holistic view into devices, traffic, applications, and events, in addition to the ability to stop a threat anywhere along its attack chain
- Enable the sharing and correlation of real-time threat intelligence is by integrating devices using open standards, common operating systems, and unified management platforms
- Use the Security Fabric to automatically provide continuous trust assessment and then provide an immediate, coordinated response to detected threats.

WORKSHOP SUMMARY

FORMAT	4-hour technical workshop
OBJECTIVE	Provide a compelling, hands-on learning experience about the new features and capabilities that have been added to FortiOS, including features for expanding the Security Fabric, cloud, SDN, automation, DevOPs, SaaS, and SD-WAN.
WHO SHOULD ATTEND	Anyone, regardless of prior knowledge of Fortinet products
PREREQUISITES	None
COST	Free of charge
INTERESTED?	Contact your local Fortinet representative

Achieve PCI DSS Compliance With FortiWeb

The goal of the Payment Card Industry Data Security Standard (PCI DSS), established in 2004, is to protect cardholder data and reduce credit card fraud. These policies and procedures should be followed by every organization that accepts credit cards.

What are the challenges of achieving PCI DSS compliance?

How can FortiWeb help alleviate these challenges?

FortiWeb is a web application firewall (WAF) that protects hosted web applications from attacks that target known and unknown exploits. Using AI-enhanced multi-layer and correlated detection methods, FortiWeb defends applications from known vulnerabilities and from zero-day attacks.

In this workshop, participants learn how FortiWeb provides the tools and resources to address many specific requirements of PCI DSS compliance.

Participants who attend this workshop will learn how to:

- Understand the PCI DSS compliance requirements
- Use FortiWeb features to address many of the PCI DSS compliance requirements
- Implement specific FortiWeb features to address specific PCI DSS requirements

WORKSHOP SUMMARY

FORMAT	4-hour technical workshop
OBJECTIVE	Provide a compelling, hands-on learning experience about how FortiWeb can help participants reduce the complexities of achieving PCI DSS compliance for their business or customers.
WHO SHOULD ATTEND	Anyone, regardless of prior knowledge of Fortinet products
PREREQUISITES	None
COST	Free of charge
INTERESTED?	Contact your local Fortinet representative

SD-Branch: Securing Your Ethernet Switching Infrastructure with FortiSwitch, FortiAP, and FortiLink

Enterprise networking and security teams are struggling with evolving their WAN and branch office IT architecture to support digital transformation. A typical branch office consists of multiple point products, creating both security and complexity challenges. IT teams are looking to consolidate these point products to increase agility and save money, while improving the security and visibility of network access at the branch office.

How can organizations converge security and network access to reduce complexity while increasing security?

Fortinet secure access architecture powered by FortiLink is uniquely suited to SD-Branch deployments, with Ethernet switch and wireless access point management built into the same platform that drives our Secure SD-WAN solution, the FortiGate and FortiOS.

In this workshop, participants learn how enabling FortiLink between FortiSwitch, FortiAP, and a FortiGate integrates the devices into the FortiGate network security platform. Thus, the FortiSwitch and FortiAP can be managed directly from the familiar FortiGate interface. This single pane of glass management provides complete visibility and control of all users and devices on the network, regardless of how they connect.

Participants who attend this workshop will learn how to:

- Create a FortiLink interface
- Authorize FortiSwitch and FortiAP devices
- Create VLANs and policies
- Create SSIDs
- Configure radio frequency (RF) parameters
- Assign firewall policies to FortiGate interfaces

WORKSHOP SUMMARY

FORMAT	4-hour technical workshop
OBJECTIVE	Provide a compelling, hands-on learning experience about SD-Branch solution with FortiSwitch, FortiAP, and FortiLink to teach participants the benefits of integrating the devices using FortiLink and how to enable a common security policy across the network, extending the protection of the firewall out to the edge.
WHO SHOULD ATTEND	Anyone, regardless of prior knowledge of Fortinet products
PREREQUISITES	None
COST	Free of charge
INTERESTED?	Contact your local Fortinet representative

Advanced Email Security Solution With FortiMail

Email security remains a key productivity tool for today's organizations, as well as a successful attack vector for cyber criminals. According to the Verizon 2019 Data Breach Investigations Report, 94% of malware was delivered via malicious emails. Gartner asserts that "advanced threats (such as ransomware and business email compromise) are easily bypassing the signature-based and reputation-based prevention mechanisms that a secure email gateway (SEG) has traditionally used."

How can you mitigate these high risk and advanced email attacks?

In this workshop, participants learn how FortiMail replaces incumbent secure email gateways with a product tailored for advanced threat defense, including Office 365 integration and Client to Authenticator Protocol (CTAP) program. FortiMail email security shields users, and ultimately data, from a wide range of cyber threats. These include: ever growing volumes of unwanted spam, socially-engineered phishing and business email compromise, accelerating variants of ransomware and other malware, increasingly targeted attacks from adversaries of all kinds, and more. At the same time, FortiMail can be used to protect sensitive data of all types, reducing the risk of inadvertent loss and/or non-compliance with regulations like HIPAA, PCI, GDPR, and more.

Participants who attend this workshop will learn how to:

- Understand how FortiMail can stop advanced threats
- Understand the key benefits of Office 365 integration
- Leverage CTAP for email
- Gain hands-on experience with FortiMail

WORKSHOP SUMMARY

FORMAT	4-hour technical workshop
OBJECTIVE	Provide a compelling, hands-on learning experience about FortiMail and teach participants how to protect their organization from phishing, unwanted spam, social engineering, business email compromise, malware, and advanced targeted attacks via email.
WHO SHOULD ATTEND	Anyone, regardless of prior knowledge of Fortinet products
PREREQUISITES	None
COST	Free of charge
INTERESTED?	Contact your local Fortinet representative

Attack and Defense Methodologies

Cyber criminals are increasingly leveraging advanced tools as part of their cyberattacks, heightening the risk of a security incident or a data breach. In turn, some CISOs are adopting sophisticated solutions, such as AI-powered sandboxing, as an essential component of their security strategy. Developing a suitable defense methodology helps combat previously unknown threats such as ransomware, crypto-malware, and many others.

Who are the threat actors and what tools and methodologies are they using to breach an organization?

How can you effectively break the attack kill chain to protect your critical assets?

To protect an organization, it is key to understand how it can be breached. In this workshop, participants will learn what tools and methodologies threat actors use to breach an organization. The participants will play the role of the threat actor and explore the anatomy of an attack to see how easy it is to penetrate an organization.

Once breached, the participants will then go on to deploy and configure different Fortinet products to understand exactly how these solutions can break the kill chain. Participants will learn how to stop and limit the progression of the very same cyber-attacks they launched earlier.

Participants who attend this workshop will learn how to:

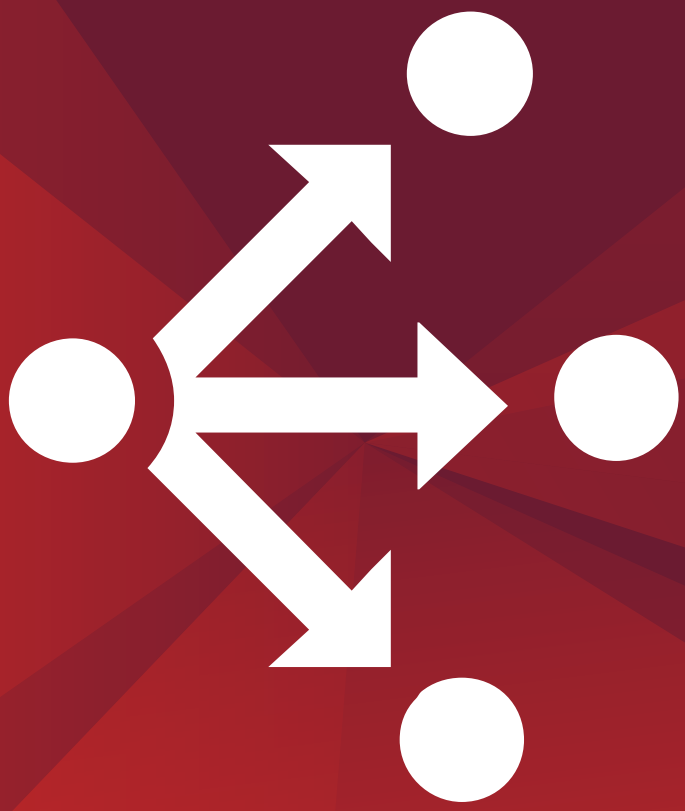
- Understand the anatomy of an attack, also known as the kill chain
- Understand the tools and techniques threat actors use to breach an organization
- Attack a fictitious organization using these tools
- Deploy the Fortinet Security Fabric to protect against known and unknown threats

WORKSHOP SUMMARY

FORMAT	(2) 4-hour technical workshops
OBJECTIVE	Provide a compelling, hands-on learning experience about who threat actors are, what tools and methodologies they use, and how to use the Security Fabric to break the kill chain. Participants will compete in teams against each other to see who can obtain the most points.
WHO SHOULD ATTEND	Anyone, regardless of prior knowledge of Fortinet products
PREREQUISITES	None
COST	Free of charge
INTERESTED?	Contact your local Fortinet representative

Constructing a Secure SD-WAN Architecture

Corporate networks are stretched thin by cloud services, SaaS applications, and mobility. Plus, organizations require better connections to branch offices to deliver higher-quality network services.



Are you looking for an SD-WAN solution that offers Next Generation Firewall (NGFW) capabilities so that you can securely and cost-effectively adopt public cloud applications?

As organizations transition to a digital business model, their network topologies are significantly impacted. The adoption of cloud services, the virtualization of the traditional network, and an increasingly mobile workforce accessing applications in the cloud are accelerating advancements in wide area networking technologies.

The traditional WAN is struggling to keep up because it relies on a static infrastructure of devices that simply can't accommodate shifting and often temporary resource allocation and workloads. In this workshop, participants learn how Secure SD-WAN solves these problems.

Participants who attend this workshop will learn how to:

- Apply software-defined networking (SDN) to wide area networks in an enterprise environment
- Implement application control and traffic shaping over SD-WAN
- Use FortiManager to enable unified policy across thousands of enterprise branches
- Use SD-WAN Orchestrator to deploy devices across regions simply and easily
- Configure virtualized products supporting WAN aggregation while gaining hand-on experience

WORKSHOP SUMMARY

FORMAT	4-hour technical workshop
OBJECTIVE	Provide a compelling hands-on learning experience about SD-WAN and teach participants to understand an agile and cost-effective architectural network solution.
WHO SHOULD ATTEND	Anyone, regardless of prior knowledge of Fortinet products
PREREQUISITES	None
COST	Free of charge
INTERESTED?	Contact your local Fortinet representative

Cybersecurity for Safe, Reliable, Secure Industrial Control Systems (ICS)

Connections between IT and operational technology (OT) systems are no longer air gapped, introducing the potential for hackers to penetrate industrial control systems, risking the safety and availability of critical infrastructure. Security for OT requires visibility, control, and analytics to meet safety and availability requirements.

How can you protect high value assets against the expanding attack surface?

Convergence is blurring the lines between IT and OT, creating an opportunity to improve the visibility, control, and situational awareness necessary for critical systems. Failure to take the wide range of security issues into account when converging these two very different networks and networking philosophies can result in catastrophic network failures that risk critical systems and the life and well-being of workers and communities.

In this workshop, participants learn about the Fortinet Security Fabric, the first ever architectural security approach designed to dynamically adapt to unique needs of legacy OT environments while enabling the move toward modernizing these critical systems. Leveraging the Purdue Model for the security layers needed in OT, the multi-layered approach provided by the Security Fabric provides broad, integrated, and automated protection against sophisticated threats.

Participants who attend this workshop will learn how to:

- Introduce the OT business drivers and security priorities
- Understand the differences between IT and OT and the importance of actively securing OT environments
- Leverage the Purdue Model to support the needs of an OT environment
- Apply the Security Fabric to secure OT
- Expand the Security Fabric and enhance the value of Fabric-ready partners

WORKSHOP SUMMARY

FORMAT	4-hour technical workshop
OBJECTIVE	Provide a compelling, hands-on learning experience about the Security Fabric and teach participants how to craft a comprehensive security solution that solves safety and availability needs of OT and control systems.
WHO SHOULD ATTEND	Anyone, regardless of prior knowledge of Fortinet products
PREREQUISITES	None
COST	Free of charge
INTERESTED?	Contact your local Fortinet representative

Detecting Zero-Day Threats With FortiSandbox

Today, organizations face a dynamic attack surface, due to the rise of IoT and cloud services. It is becoming increasingly clear that no single technology will be able to stop every threat.

How can you protect your network against advanced and emerging threats?

How can you analyze targeted attacks designed to bypass traditional security?

In this workshop, participants learn how to protect an enterprise against sophisticated threats by establishing a comprehensive and cohesive security infrastructure that is broad enough to cover all attack vectors, powerful enough to run the latest security technologies, and automated to keep pace with fast-moving attacks.

Participants who attend this workshop will learn how to:

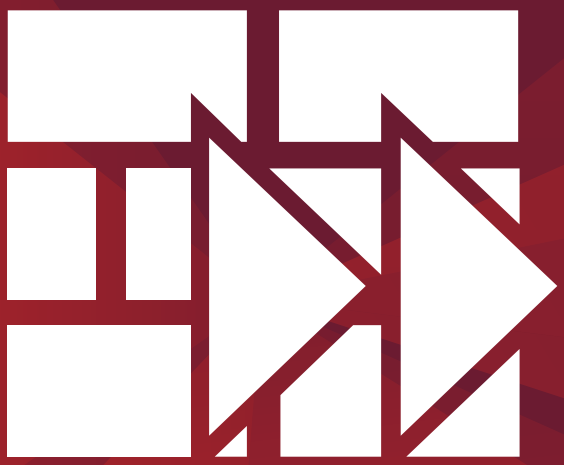
- Recognize the characteristics of malicious documents, scripts, and executables
- Use the FortiSandbox engines, techniques, and services to analyze different file types and catch threats that traditional security devices miss
- Understand the input methods that FortiSandbox supports and how it shares dynamically generated local threat intelligence with both Fortinet and third-party devices

WORKSHOP SUMMARY

FORMAT	4-hour technical workshop
OBJECTIVE	Provide a compelling, hands-on learning experience about FortiSandbox and teach participants how FortiSandbox detects and reports on advanced threats.
WHO SHOULD ATTEND	Anyone, regardless of prior knowledge of Fortinet products
PREREQUISITES	None
COST	Free of charge
INTERESTED?	Contact your local Fortinet representative

Fortifying the Enterprise Network (NGFW Solution)

As security architects consider how to provide comprehensive threat protection for their enterprises—including intrusion prevention, web filtering, anti-malware, and application control—they face a major complexity hurdle managing these point products with no integration and lack of visibility.



How can you manage this high risk and complex issue simply?

In this workshop, participants learn how Fortinet network security leverages a single operating system that works across different network security use cases. FortiGate reduces complexity by integrating various point products using Next Generation Firewall (NGFW) features. FortiGate also provides automated visibility into cloud applications and IoT devices. The Fortinet Security Fabric automatically discovers the end to end topology view of the enterprise network and also protects it from known and unknown attacks via automated action. FortiGate NGFW utilizes purpose-built security processors and threat intelligence security services from FortiGuard labs to deliver top-rated protection and high performance, including encrypted cloud access.

Participants who attend this workshop will learn how to:

- Reduce complexity with industry-leading security effectiveness
- Enhance visibility with automated action
- Simplify SSL performance and complexity issues for encrypted cloud access

WORKSHOP SUMMARY

FORMAT	4-hour technical workshop
OBJECTIVE	Provide a compelling, hands-on learning experience about the Fortinet NGFW and teach participants how to fortify their enterprise network with the Fortinet NGFW solution, which solves the challenges of today's highly adaptive threat landscape, provides enhanced visibility into cloud applications and IoT devices, and protects the entire dynamic environment with automated action.
WHO SHOULD ATTEND	Anyone, regardless of prior knowledge of Fortinet products
PREREQUISITES	None
COST	Free of charge
INTERESTED?	Contact your local Fortinet representative

Empowering Security Operations Leveraging FortiSOAR

To address the constantly evolving threat landscape, the complexity of security products, and the scarcity of cyber security skills/staff, organizations must be able to aggregate and enrich alerts from a wide range of security products. In addition, they need to automate repetitive tasks and leverage well-defined playbooks to guide fast incident response to maximize the efficiency of their security operations team.

How can you address alert fatigue and the cybersecurity skills shortage while reducing overall complexity for your security operations team?

FortiSOAR is a holistic and enterprise-built security orchestration and security automation workbench that empowers security operation teams. FortiSOAR increases a team's effectiveness by increasing efficiency, allowing for response in near real time.

In this workshop, participants learn how FortiSOAR takes your security operation team to the next level by automating the incident response process and facilitating collaboration, all behind a single console.

Participants who attend this workshop will learn how to:

- Address the staff and skills shortage by automating routine tasks to preserve scarce expertise for critical incidents
- Combat complexity with connectors that easily integrate with deployed security controls to ingest information and provide a single, centralized point of visibility and control
- Avoid alert fatigue by aggregating security alerts in one place, enriching them with added context to speed investigation, and including playbooks to guide the triage process

WORKSHOP SUMMARY

FORMAT	4-hour technical workshop
OBJECTIVE	Provide a compelling, hands-on learning experience about the Fortinet Security Fabric and teach participants how to automate repetitive tasks and leverage well-defined playbooks to guide fast incident response to maximize the efficiency of their SOC team.
WHO SHOULD ATTEND	Anyone, regardless of prior knowledge of Fortinet products
PREREQUISITES	None
COST	Free of charge
INTERESTED?	Contact your local Fortinet representative

Fortinet Teleworker Solution Engineered for Remote and Secure Productivity

Preparing for business continuity and disaster recovery is vital for any organization. An important component of this is the ability to support a mostly or fully remote workforce with little or no notice.

When developing business continuity plans, it is essential to ensure that the organization has the resources in place to secure this remote workforce.

Fortinet solutions are easily deployable and configurable and enable an organization to maintain full security, visibility, and control, regardless of their deployment environment.

How can you securely support a remote workforce and maintain business continuity in an ever-changing business environment?

In this workshop, participants learn about how Fortinet solutions offer an integrated solution to support telework. FortiGate Next Generation Firewalls (NGFWs) have built-in support for IPsec VPNs, enabling remote workers to connect securely to the company network. With endpoint protection provided by FortiClient and multi-factor authentication (MFA) with FortiAuthenticator, organizations can securely support remote work and maintain business continuity

Participants who attend this workshop will learn how to:

- Configure two-factor authentication, which is necessary for secure access
- Create an inbound VPN policy on FortiGate that allows teleworkers to tunnel back to corporate headquarters
- Configure the FortiClient Endpoint Management Server (EMS) to protect remote users as effectively as if they were located at the corporate office
- Demonstrate successful operation of these critical functions

WORKSHOP SUMMARY

FORMAT	4-hour technical workshop
OBJECTIVE	Provide a compelling, hands-on learning experience to understand how to easy it is to deploy, configure, and enable an organization to maintain full security, visibility, and control regardless of the deployment environment.
WHO SHOULD ATTEND	Anyone, regardless of prior knowledge of Fortinet products
PREREQUISITES	None
COST	Free of charge
INTERESTED?	Contact your local Fortinet representative

Powerful Security Information and Event Management With FortiSIEM

Cyberattacks are a 24/7 reality. The complexity and growth of the enterprise estate, including infrastructure, applications, VMs, cloud, endpoints, and IoT, means the attack surface grows exponentially. Coupled with a skills shortage and resource constraints, security becomes everybody's problem, but visibility, event correlation, and remediation are other people's responsibility. Effective security requires visibility—all the devices, all the infrastructure in real time—but also requires context: what devices represent a threat and what are their capabilities. All this is necessary to manage the threat the business faces and the noise multiple security tools create.

How can you integrate separate network operations center (NOC) and security operations center (SOC) solutions to automate IT processes and security responses?

In this workshop, participants learn how FortiSIEM, the Fortinet multi-vendor security incident and events management solution, brings it all together by integrating NOC and SOC solutions to automate IT processes and security responses. Visibility, correlation, and remediation all come in a single, scalable solution. Using FortiSIEM, the complexity of managing network and security operations is reduced, freeing resources and improving breach detection. Worldwide, 80% of breaches go undetected because of skills shortage and event information noise. FortiSIEM provides the cross correlation, machine learning, and user and entity behavior analytics (UEBA) to improve overall response and effectively stop breaches before they occur.

Participants who attend this workshop will learn how to:

- Understand FortiSIEM architecture
- Use FortiSIEM features
- Run analytic searches
- Use rapid detection and remediation of security events
- Use security and performance management

WORKSHOP SUMMARY

FORMAT	4-hour technical workshop
OBJECTIVE	Provide a compelling, hands-on learning experience on FortiSIEM and teach participants how to improve security and performance management, plus rapidly detect and remediate security incidents via automated responses.
WHO SHOULD ATTEND	Anyone, regardless of prior knowledge of Fortinet products
PREREQUISITES	None
COST	Free of charge
INTERESTED?	Contact your local Fortinet representative

Reduce the Complexity of Operations with the Fabric Management Center

The Fabric Management Center provides powerful automation-ready, single pane of glass management and visibility, advanced compliance reporting, and network-aware rapid response across on-premises, cloud, and hybrid environments. The Fabric Management Center has been tested for more than a decade and is deployed by thousands of customers around the world across all major industry verticals.

How can you reduce operational complexity and security risk?

How can you decrease threat remediation time?

How can you improve on compliance reporting?

As enterprise networks have morphed and changed with digital transformation, once relied upon tools have become outdated and obsolete. Yet, many are still deployed alongside newer technology stacks, creating a complex environment that does not interoperate. Enterprises deploy an average of 32 different vendor solutions that lack shared threat intelligence—a cybersecurity hurdle that is often compounded with a lack of skilled cybersecurity personnel to manage these networks.

In this workshop, participants gain hands-on experience implementing the key capabilities of the Fabric Management Center and applying them to centrally manage a fictitious organization's HQ and branch networks from a single pane of glass.

Participants who attend this workshop will learn how to:

- Understand the benefits of using the Fabric Management Center
- Reduce operational complexity and security risk by simplifying and automating deployment and network monitoring
- Centrally manage a device's configuration, including policies, IPsec VPN, and SD-WAN, using the GUI and scripts
- Improve time to compliance readiness with pre-built reports, as well as customizing and creating new reports
- Reduce risk by automating response to security events with network-aware response actions

WORKSHOP SUMMARY

FORMAT	4-hour technical workshop
OBJECTIVE	Provide a compelling, hands-on learning experience about how to use the Fabric Management Center to centrally manage and protect networks.
WHO SHOULD ATTEND	Anyone, regardless of prior knowledge of Fortinet products
PREREQUISITES	None
COST	Free of charge
INTERESTED?	Contact your local Fortinet representative

Proactive Advanced Endpoint Protection, Visibility, and Control for Critical Assets

Fortinet strengthens endpoint security through integrated visibility, control, and proactive defense. With the ability to discover, monitor, and assess endpoint risks, organizations can ensure endpoint compliance, mitigate risks, and reduce exposure.

How can you mitigate risks due to limited endpoint visibility?

How can policy-based automation contain threats and control outbreaks?

How do you protect your endpoints pre-and post-infection?

Endpoints are frequently the target of initial compromise or attacks. One recent study found that 30% of breaches involved malware being installed on endpoints. Fortinet endpoint solutions strengthen endpoint security through integrated visibility, control, and proactive defense.

FortiClient can discover, monitor, and assess endpoint risks, so you can ensure endpoint compliance, mitigate risks, and reduce exposure. Its tight integration with the Fortinet Security Fabric enables policy-based automation to contain threats and control outbreaks. FortiClient also provides secure remote access with built-in VPN, single-sign-on, and two-factor authentication for added security.

FortiEDR delivers advanced, real-time threat protection for endpoints both pre- and post-infection. It proactively reduces the attack surface, prevents malware infection, detects and defuses potential threats in real time, and can automate response and remediation procedures with customizable playbooks.

Participants who attend this workshop will learn how to:

- Integrate FortiClient EMS into the Security Fabric
- Use the FortiClient anti-exploit feature to prevent attacks proactively
- Configure FortiClient EMS to apply tags to endpoints that FortiGate can use to dynamically control access to subnets
- Filter, sort, and, view events in FortiEDR
- Perform forensic analysis in FortiEDR

WORKSHOP SUMMARY

FORMAT	4-hour technical workshop
OBJECTIVE	Provide a compelling, hands-on learning experience to understand how to strengthen endpoint security through integrated visibility, control, and proactive defense.
WHO SHOULD ATTEND	Anyone, regardless of prior knowledge of Fortinet products
PREREQUISITES	None
COST	Free of charge
INTERESTED?	Contact your local Fortinet representative

Securely Embrace the IoT Revolution With FortiNAC

Network Access Control (NAC) has come back to the forefront of security solutions to address the challenge presented by IoT. This technology was deployed to assist with bring your own device (BYOD) policies and is now getting renewed focus as a means to safely accommodate headless IoT devices in the network. FortiNAC enables three key capabilities to secure IoT devices:

- Network visibility to see every device and user as they join the network
- Network control to limit where devices can go on the network
- Automated response to speed the reaction time to events from days to seconds

Collectively, these three capabilities provide the tools that network owners need to secure a world that is embracing IoT.

How can you see and protect against a myriad of devices showing up on the network?

The proliferation of IoT devices has made it necessary for organizations to improve their visibility into what is attached to their networks. They need to know every device and every user accessing their networks. IoT devices enable digital transformation initiatives and improve efficiency, flexibility, and optimization. However, they are inherently untrustworthy, with designs that prioritize low-cost over security.

In this workshop, participants learn how FortiNAC provides the network visibility to see everything connected to the network, as well as the ability to control those devices and users, including dynamic, automated responses.

Participants who attend this workshop will learn how to:

- Discuss the business drivers and security challenges that customers face
- Identify the key capabilities, use cases, sales strategies, and competitive advantages of FortiNAC
- Understand the fundamental feature set of FortiNAC

WORKSHOP SUMMARY

FORMAT	4-hour technical workshop
OBJECTIVE	Provide a compelling, hands-on learning experience for FortiNAC and teach participants how to enhance the Fortinet Security Fabric and protect against IoT threats.
WHO SHOULD ATTEND	Anyone, regardless of prior knowledge of Fortinet products
PREREQUISITES	None
COST	Free of charge
INTERESTED?	Contact your local Fortinet representative

Security Operations: Threat Prevention and Detection With FortiDeceptor

FortiDeceptor allows organizations to rapidly create a fabricated deception network that lures attackers into revealing themselves. FortiDeceptor serves as an early warning system by providing accurate detection that correlates an attacker's activity details and lateral movement, indicating that a breach has happened. Threat intelligence gathered from the attacker can be applied automatically to in-line security controls to stop attacks before any real damage is done.

How can you detect if you are being targeted by a threat actor or if your network has already been breached?

To protect an enterprise against sophisticated threats, it is important to establish a comprehensive and cohesive security infrastructure that is broad enough to cover all attack vectors, powerful enough to run the latest security technologies, and automated to keep pace with fast-moving attacks. In this workshop, participants learn how to do this by deploying FortiDeceptor.

Participants who attend this workshop will learn how to:

- Deploy deception hosts in order to uncover attacker activity
- Use the anti-reconnaissance and anti-exploit engine to correlate events into incidents and campaigns, giving SecOps the information they need to act upon
- Take action on discovered threat actor activity by integrating with the Fortinet Security Fabric to quarantine compromised hosts before they can do further damage

WORKSHOP SUMMARY

FORMAT	Half-day technical workshop
OBJECTIVE	Provide a compelling, hands-on learning experience about FortiDeceptor and teach participants how FortiDeceptor detects and reports on attacker activity.
WHO SHOULD ATTEND	Anyone, regardless of prior knowledge of Fortinet products
PREREQUISITES	None
COST	Free of charge
INTERESTED?	Contact your local Fortinet representative

Security, Visibility, and Control of Public Cloud Infrastructure and Workloads

As cloud adoption accelerates, organizations are increasingly reliant on cloud-based services and infrastructures. Yet organizations often end up with a heterogeneous set of technologies in use, with disparate security controls in various cloud environments. Fortinet multi-cloud solutions provide the necessary visibility and control across public cloud infrastructures, enabling secure applications and connectivity from data center to cloud.

How can you easily secure an expanding and highly dynamic attack surface in a multi-cloud environment?

In this workshop, participants learn how to provision and secure public cloud resources using the Fortinet Security Fabric. Participants will create public and private cloud Fabric connectors and apply intent-based segmentation to effectively manage risk in multi-cloud environments.

Lab exercises can be completed using either Google Cloud Platform (GCP) or Microsoft Azure frameworks.

Participants who attend this workshop will learn how to:

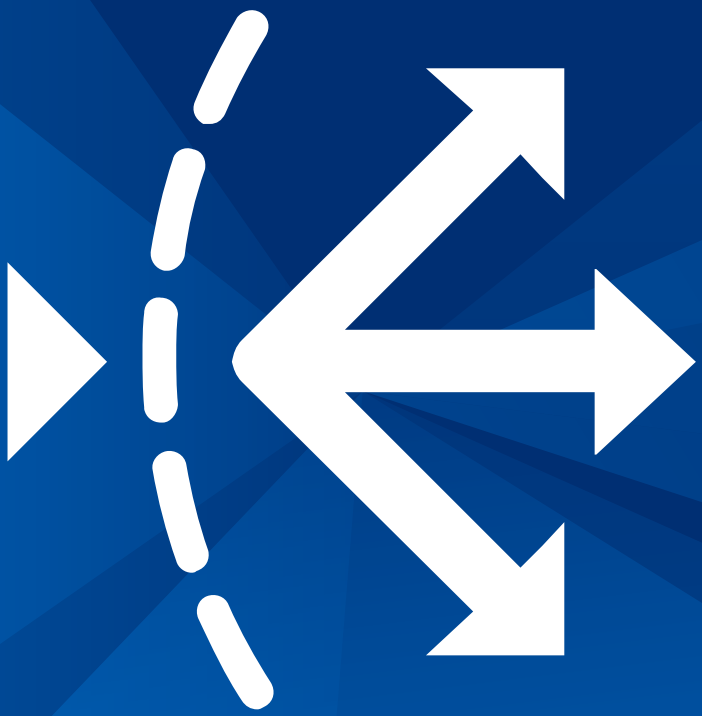
- Use Terraform to programmatically provision resources and Fortinet appliances
- Extend the Security Fabric to cloud based resources
- Use Fabric connectors to define security policies based on asset labels/tags
- Visualize cloud-based activity using FortiView on FortiGate
- Dynamically modify FortiGate configurations with Terraform

WORKSHOP SUMMARY

FORMAT	4-hour technical workshop
OBJECTIVE	Provide a compelling, hands-on learning experience about how to secure multi-cloud environments.
WHO SHOULD ATTEND	Anyone, regardless of prior knowledge of Fortinet products
PREREQUISITES	None
COST	Free of charge
INTERESTED?	Contact your local Fortinet representative

FortiADC Application Delivery Without Limits

With bandwidth demand growing faster than budgets, and with cyberattacks constantly on the rise, it can be challenging to securely, and efficiently, deliver applications at the speed users expect. Using an application delivery controller (ADC) optimizes the availability, user experience, and application security of enterprise applications. FortiADC provides application availability using Layer 4/Layer 7 load balancing, data center resiliency, application optimization, and a web application firewall (WAF) to protect web applications from the OWASP top 10 and many other threats.



How can you manage the need for fast, efficient, reliable, and secure access to your business critical applications?

In this workshop, participants explore the ways in which to deploy FortiADC to provide secure, efficient, scalable, and reliable access to business critical applications. Participants will be able to deploy a single data center ADC, expand to a global load balancing solution, implement SSL offloading, and implement firewall security.

Participants who attend this workshop will learn how to:

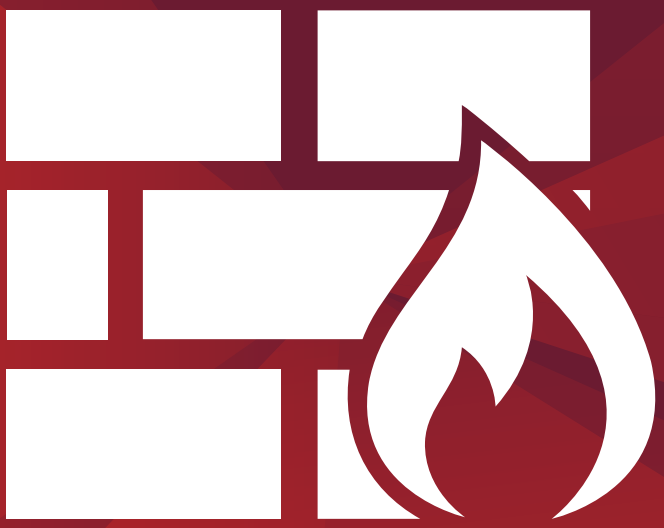
- Introduce the FortiADC product family
- Simplify scalability of web applications within the data center
- Provide global redundancy for web applications
- Improve performance of web applications through mechanisms such as SSL offloading
- Protect and secure web applications with built in firewall, WAF, and more

WORKSHOP SUMMARY

FORMAT	4-hour technical workshop
OBJECTIVE	Provide a compelling, hands-on learning experience about how FortiADC can provide secure, reliable, and scalable access to all web applications, while improving overall performance and responsiveness of those same applications.
WHO SHOULD ATTEND	Anyone, regardless of prior knowledge of Fortinet products
PREREQUISITES	None
COST	Free of charge
INTERESTED?	Contact your local Fortinet representative

Getting Started With the FortiGate Firewall

Today's networks are highly complex environments with borders that are constantly changing. In response to this highly complex environment, firewalls have become robust, multi-functional devices that counter an array of threats to your network.



How can organizations deploy FortiGate to meet the requirements of today's multi-faceted and multi-device networks?

In this workshop, participants learn the basics of how to install a FortiGate and use it to protect a network.

FortiGate enables security-driven networking and consolidates industry-leading security capabilities, such as SSL inspection, antivirus, web filtering, and application control. By doing this, FortiGate meets the performance needs of highly scalable, hybrid IT architectures, enabling organizations to reduce complexity and manage security risks.

FortiGate simplifies security complexity and provides visibility into applications, users, and networks. FortiGate utilizes purpose-built security processing units (SPUs) and threat intelligence services from FortiGuard Labs to deliver top-rated security and high performance threat protection.

Participants who attend this workshop will learn how to:

- Install a FortiGate device in a network
- Configure basic routing
- Create security policies
- Apply security scanning
- Configure local user authentication
- Use the CLI
- Configure the Fortinet Security Fabric

WORKSHOP SUMMARY

FORMAT	4-hour technical workshop
OBJECTIVE	Provide a compelling, hands-on learning experience about the FortiGate that covers the basics of how to install and configure the FortiGate, including security profiles, authentication, and the Fortinet Security Fabric.
WHO SHOULD ATTEND	Anyone, regardless of prior knowledge of Fortinet products
PREREQUISITES	None
COST	Free of charge
INTERESTED?	Contact your local Fortinet representative

Simplify SOC Operations for the Security Fabric with FortiAnalyzer

FortiAnalyzer, part of the Fortinet Security Fabric, addresses the complexity of operations that security teams around the world face. FortiAnalyzer enables an organization to maximize the impact and effectiveness of a lean security team. It does this by providing broad visibility and control of an organization's entire digital attack surface, an integrated solution reducing the complexity of supporting multiple point products, and automation of security workflows that increase the speed of operation.

How can you reduce the complexity of supporting multiple point products?

How can you decrease simplify and automate security operations center (SOC) operations?

How can you improve on compliance reporting?

Security teams around the world are struggling with the complexity of operations. Common issues include: too many consoles, too many alerts, manual and slow response, and a shortage of cybersecurity personnel

FortiAnalyzer, a core part of the Security Fabric, enables teams to simplify security operations, enabling enterprises at any stage of SOC maturity to smoothly integrate security visibility and automation.

In this workshop, participants gain hands-on experience and see how the solution provides organizations with advanced logging and reporting, Security Fabric analytics, and Security Fabric automation.

Participants who attend this workshop will learn how to:

- Understand the benefits of using FortiAnalyzer to simplify SOC operations
- Use playbooks to automate workflows and reduce the workload on the security team
- Use FortiGate event handlers to automate actions via automation stitches
- Work with analytics logs and generate custom reports

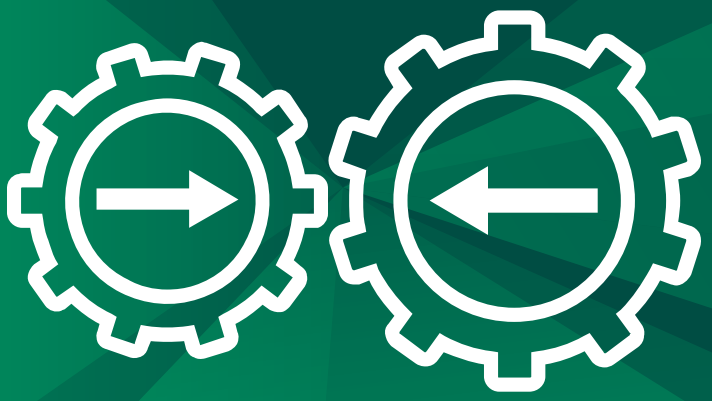
WORKSHOP SUMMARY

FORMAT	4-hour technical workshop
OBJECTIVE	Provide a compelling, hands-on learning experience about how FortiAnalyzer, a core part of the Security Fabric, enables teams to simplify security operations, enabling enterprises to smoothly integrate security visibility and automation.
WHO SHOULD ATTEND	Anyone, regardless of prior knowledge of Fortinet products
PREREQUISITES	None
COST	Free of charge
INTERESTED?	Contact your local Fortinet representative

Streamlining Automation Using Web Services APIs

Automation is key to successfully defending against today's advanced threats. In addition, cloud and hybrid-based architectures require automation to guarantee that management and security are not an inhibitor to these platforms benefits.

Fortinet Web Services APIs are an ideal way to automate repetitive and complex tasks in dynamic environments.



How can you streamline automation efforts and customize deployments to fit organizational need?

As organizations transition to a digital business model, virtualization and cloud technologies play an increasing role. Speed, flexibility, elasticity, and integration are all critical features that cannot be inhibited when implementing an effective security strategy. Ultimately it doesn't matter how fast organizations can deploy an appliance or VM if configuration is a manual process that requires a heavy administrative touch.

In this workshop, participants learn how Web Services APIs enable organizations to fully leverage the benefits of these dynamic architectures while offering an efficient communications method that promotes a robust and automated Fortinet Security Fabric. Understanding the structure, function, and communication mechanisms of these APIs is critical for developing any custom interfaces.

Participants who attend this workshop will learn how to:

- Understand the benefits of various Web Services APIs
- Construct methods to configure and deploy FortiManager policies
- Construct methods to configure and deploy FortiGate policies

WORKSHOP SUMMARY

FORMAT	4-hour technical workshop
OBJECTIVE	Provide a compelling, hands-on learning experience to understand the benefits and power of web services and teach participants how to construct API requests to create customized interfaces and facilitate automation of dynamic security environments.
WHO SHOULD ATTEND	Anyone, regardless of prior knowledge of Fortinet products
PREREQUISITES	None
COST	Free of charge
INTERESTED?	Contact your local Fortinet representative

FORTINET

www.fortinet.com

October 9, 2020 12:42 PM
632182-0-0-EN
Macintosh HD:Users:ckluck:Documents:1-2020:FTNT-Fast-Track-Brochure:R4:Spreads:FTNT-Fast-Track-Brochure-Spreads