Open Source Security Guide

A guide covering Security, including the applications, libraries and tools that will make you better and more efficient at securing your system operations and networks.

TABLE OF CONTENTS

1. Getting Started with Open Source Security

Back to the Top

Open Source Security Foundation (OpenSSF) is a cross-industry collaboration that brings together leaders to improve the security of open source software by building a broader community, targeted initiatives, and best practices. The OpenSSF brings together open source security initiatives under one foundation to accelerate work through cross-industry support. Along with the Core Infrastructure Initiative and the Open Source Security Coalition, and will include new working groups that address vulnerability disclosures, security tooling and more.

Security Tutorials & Resources

Back to the Top

- Microsoft Open Source Software Security
- Cloudflare Open Source Security
- The Seven Properties of Highly Secure Devices
- How Layer 7 of the Internet Works
- The 7 Kinds of Security
- The Libgcrypt Reference Manual
- The Open Web Application Security Project(OWASP) Foundation Top 10
- Common Weakness Enumeration (CWE) Top 25
- Best Practices for Using Open Source Code from The Linux Foundation
- awesome-cyber-security
- macOS Security and Privacy Guide
- macOS Security Compliance Project
- GitGuardian API Security Best Practice
- Open Source Security Foundation (OpenSSF) npm Best Practices Guide
- Open Source Security Foundation (OpenSSF) Best Practices for Open Source Developers
- Open Source Security Foundation (OpenSSF) Identifying Security Threats in Open Source Projects
- Securing The Software Supply Chain: Recommended Practices Guide for Developers | CISA, NSA, and ODNI (PDF)

Security Certifications

Back to the Top

- AWS Certified Security - Specialty Certification
- Microsoft Certified: Azure Security Engineer Associate

- Google Cloud Certified Professional Cloud Security Engineer
- Cisco Security Certifications
- The Red Hat Certified Specialist in Security: Linux
- Linux Professional Institute LPIC-3 Enterprise Security Certification
- Cybersecurity Training and Courses from IBM Skills
- Cybersecurity Courses and Certifications by Offensive Security
- RSA Certification Program
- Check Point Certified Security Expert(CCSE) Certification
- Check Point Certified Security Administrator(CCSA) Certification
- Check Point Certified Security Master (CCSM) Certification
- Certified Cloud Security Professional(CCSP) Certification
- Certified Information Systems Security Professional (CISSP) Certification
- CCNP Routing and Switching
- Certified Information Security Manager(CISM)
- Wireshark Certified Network Analyst (WCNA)
- Juniper Networks Certification Program Enterprise (JNCP)
- Security Training Certifications and Courses from Udemy
- Security Training Certifications and Courses from Coursera
- Security Certifications Training from Pluarlsight

2. Security Standards, Frameworks and Benchmarks

Back to the Top

Security Benchmarks

Back to the Top

- STIGs Benchmarks - Security Technical Implementation Guides
- CIS Benchmarks - CIS Center for Internet Security
- CIS Top 18 Critical Security Controls
- OSSTMM (Open Source Security Testing Methodology Manual) PDF
- NIST Technical Guide to Information Security Testing and Assessment (PDF)
- NIST - Current FIPS

Security Standards & Frameworks

Back to the Top

- ISO Standards Catalogue

Common Criteria for Information Technology Security Evaluation (CC) is an international standard (ISO / IEC 15408) for computer security. It allows an objective evaluation to validate that a particular product satisfies a defined set of security requirements.

ISO 22301 is the international standard that provides a best-practice framework for implementing an optimised BCMS (business continuity management system).

ISO27001 is the international standard that describes the requirements for an ISMS (information security management system). The framework is designed to help organizations manage their security practices in one place, consistently and cost-effectively.

ISO 27701 specifies the requirements for a PIMS (privacy information management system) based on the requirements of ISO 27001. It is extended by a set of privacy-specific requirements, control objectives and controls. Companies that have implemented ISO 27001 will be able to use ISO 27701 to extend their security efforts to cover privacy management.

SOC 2 is an auditing procedure that ensures your service providers securely manage your data to protect the interests of your comapny/organization and the privacy of their clients.

NIST CSF is a voluntary framework primarily intended for critical infrastructure organizations to manage and mitigate cybersecurity risk based on existing best practice.

EU GDPR (General Data Protection Regulation) is a privacy and data protection law that supersedes existing national data protection laws across the EU, bringing uniformity by introducing just one main data protection law for companies/organizations to comply with.

CCPA (California Consumer Privacy Act) is a data privacy law that took effect on January 1, 2020 in the State of California. It applies to businesses that collect California residents' personal information, and its privacy requirements are similar to those of the EU's GDPR (General Data Protection Regulation).

Payment Card Industry (PCI) Data Security Standards (DSS) is a global information security standard designed to prevent fraud through increased control of credit card data.

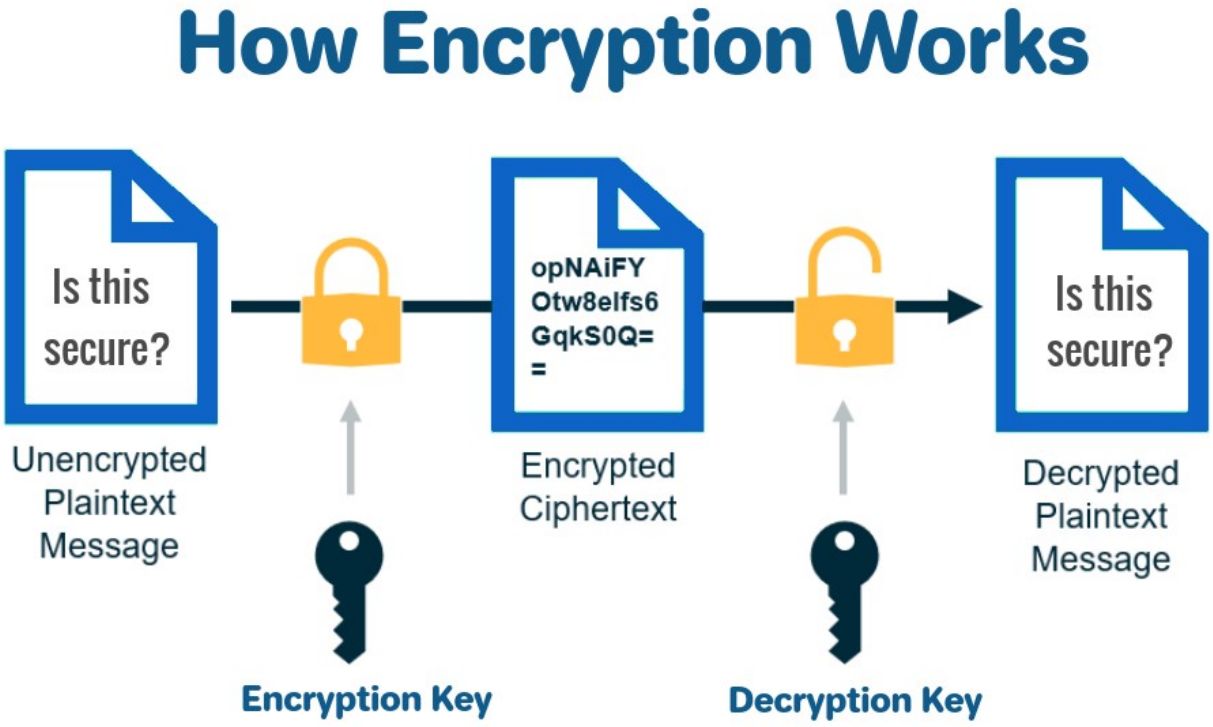
Landlock LSM(Linux Security Module) is a framework to create scoped access-control (sandboxing). Landlock is designed to be usable by unprivileged processes while following the system security policy enforced by other access control mechanisms (DAC, LSM, etc.).

Secure boot is a security standard developed by members of the PC industry to help make sure that a device boots(Unified Extensible Firmware Interface (UEFI) BIOS) using only software(such as bootloaders, OS, UEFI drivers, and utilities) that is trusted by the Original Equipment Manufacturer (OEM).

Security Encryption

Back to the Top

How Encryption Keys work



- **Symmetric** is a data encryption method whereby the same private key is used to encode and decode information.
- **Asymmetric** is a data encryption method that allows users to encrypt information using shared keys. For example, if you need to send a message across the internet, but you don't want anyone but the intended recipient to see what you've written.

Types of Encryption

- **Triple DES (Triple Data Encryption Algorithm)** is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block(contains 64 bits of data).
- **AES (Advanced Encryption Standard)** is an algorithm that encrypts and decrypts data in blocks of 128 bits. It can do this using 128-bit, 192-bit, or 256-bit keys.
- **RSA (Rivest–Shamir–Adleman)** is a type of public-key cryptography used for secure data transmission of e-mail and other digital transactions over the Internet.
- **Twofish** is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. It is an advanced version of Blowfish encryption.
- **Format Preserving Encryption (FPE)** is a valid encryption algorithm to be used for compliance with NIST standards. It is mostly used in on-premise encryption and tokenization solutions.

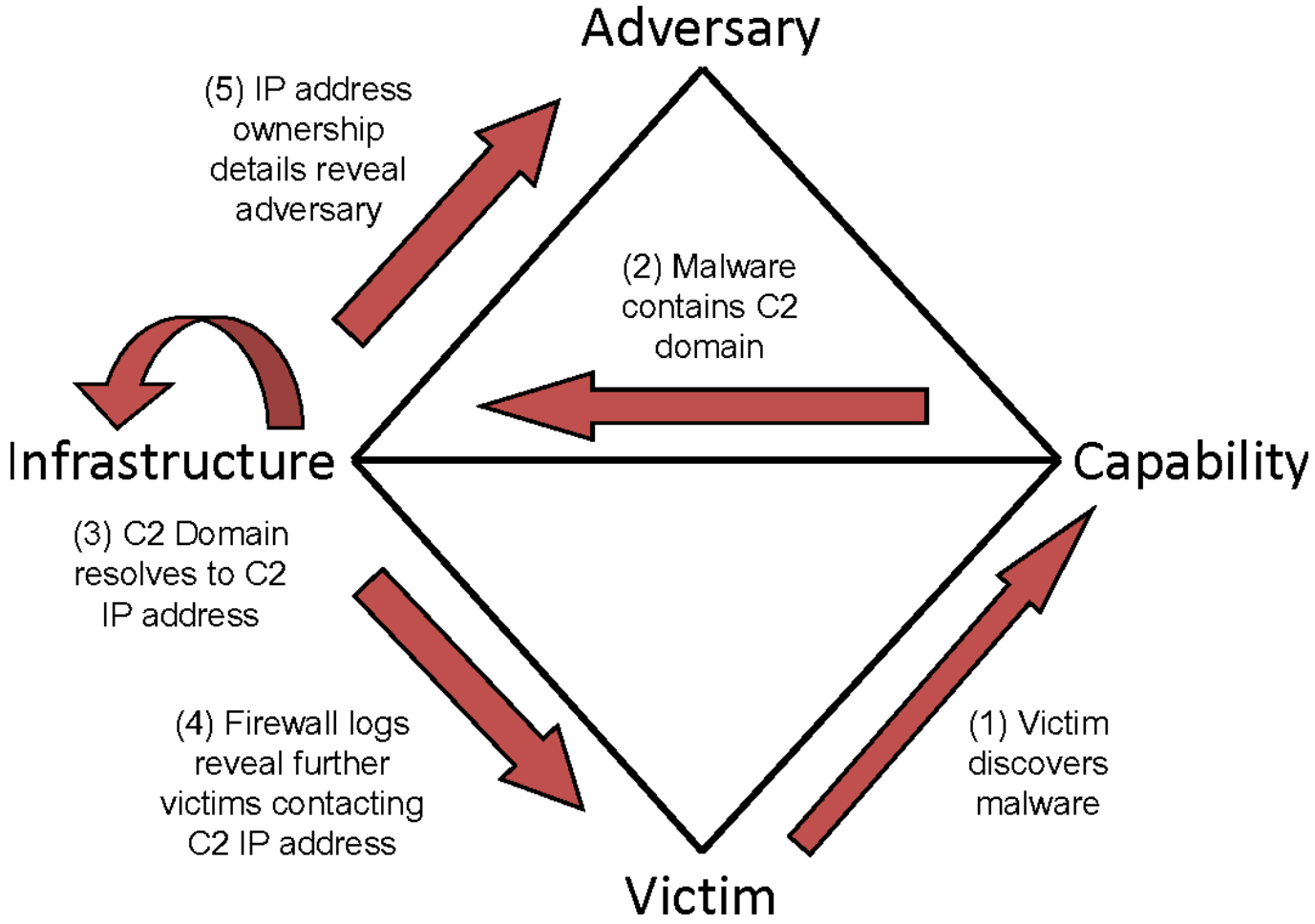
Application Level Encryption

- **Hashes** is a function that converts an input of letters and numbers into an encrypted output of a fixed length. For example, algorithms such as MD5 (Message Digest 5) or SHA (Secure Hash Algorithm).
- **Digital Certificates** is a file that verifies the identity of a device or user and enables encrypted connections. A digital signature is a hashing approach that uses a numeric string to provide authenticity and validate identity. Digital certificates are typically issued by a **certificate authority (CA)**, which is a trusted third-party entity that issues digital certificates for use by other parties.

Security Threat Models

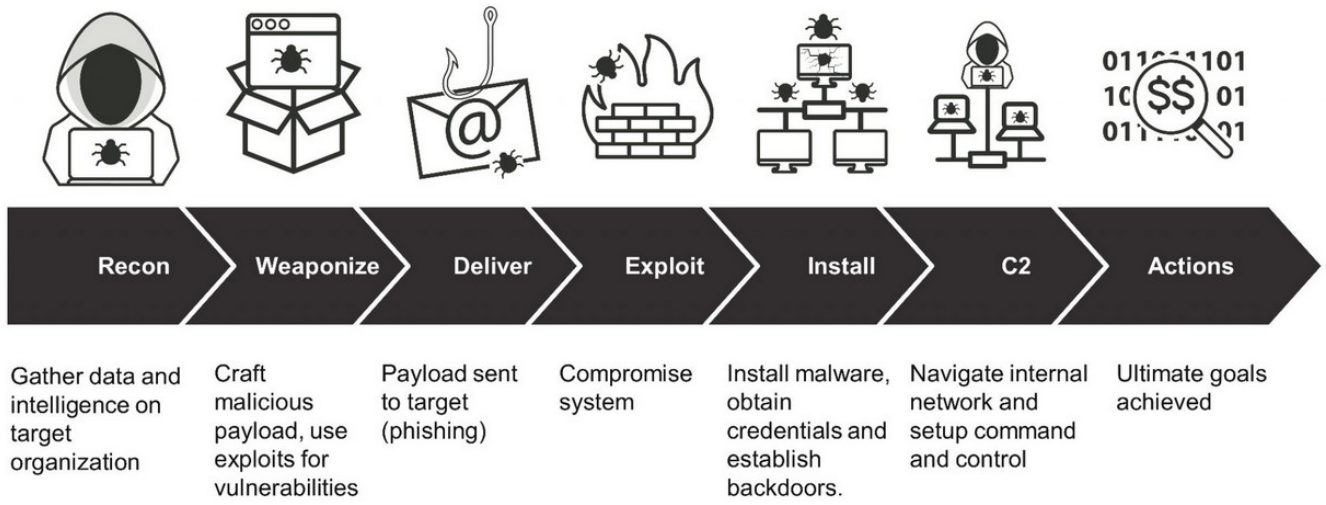
Back to the Top

Diamond Model of Intrusion Analysis is a model to describe cyber attacks. It contains 4 parts - adversary, infrastructure, capability, and target.



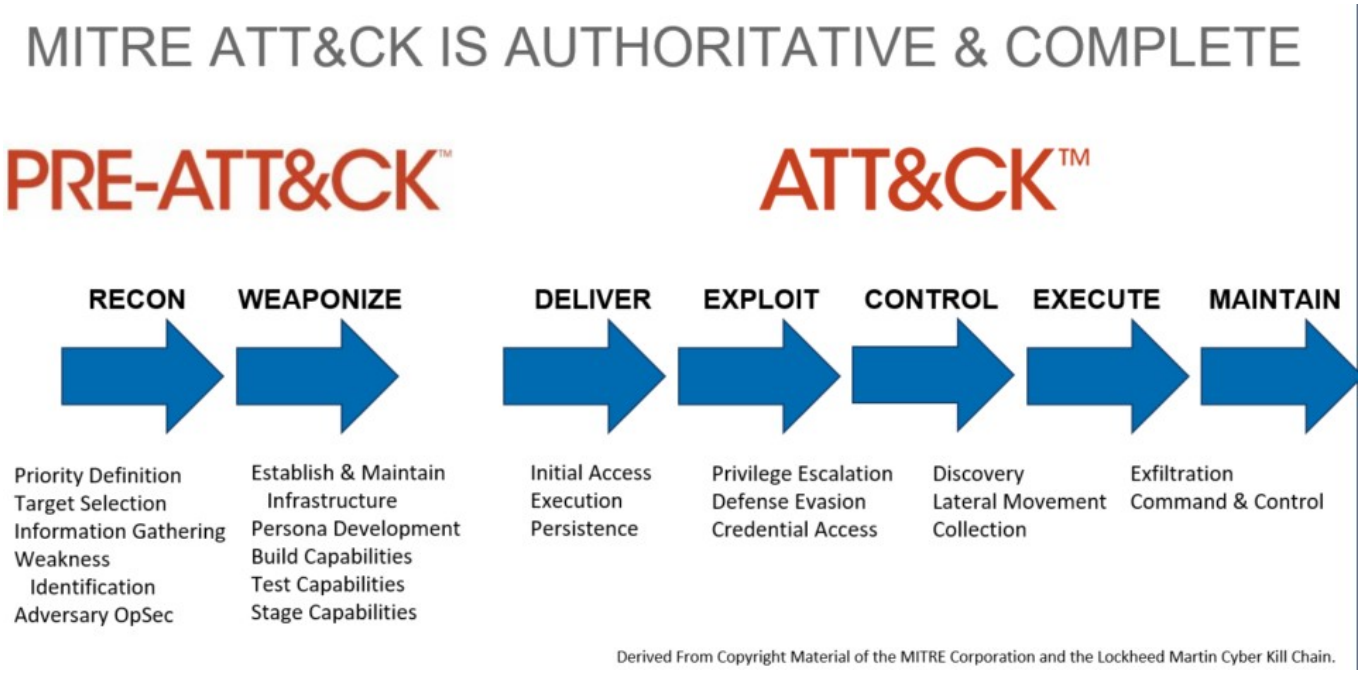
Diamond Model of Intrusion Analysis security model

Cyber Kill Chain framework is part of the Intelligence Driven Defense model for identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete in order to achieve their objective.



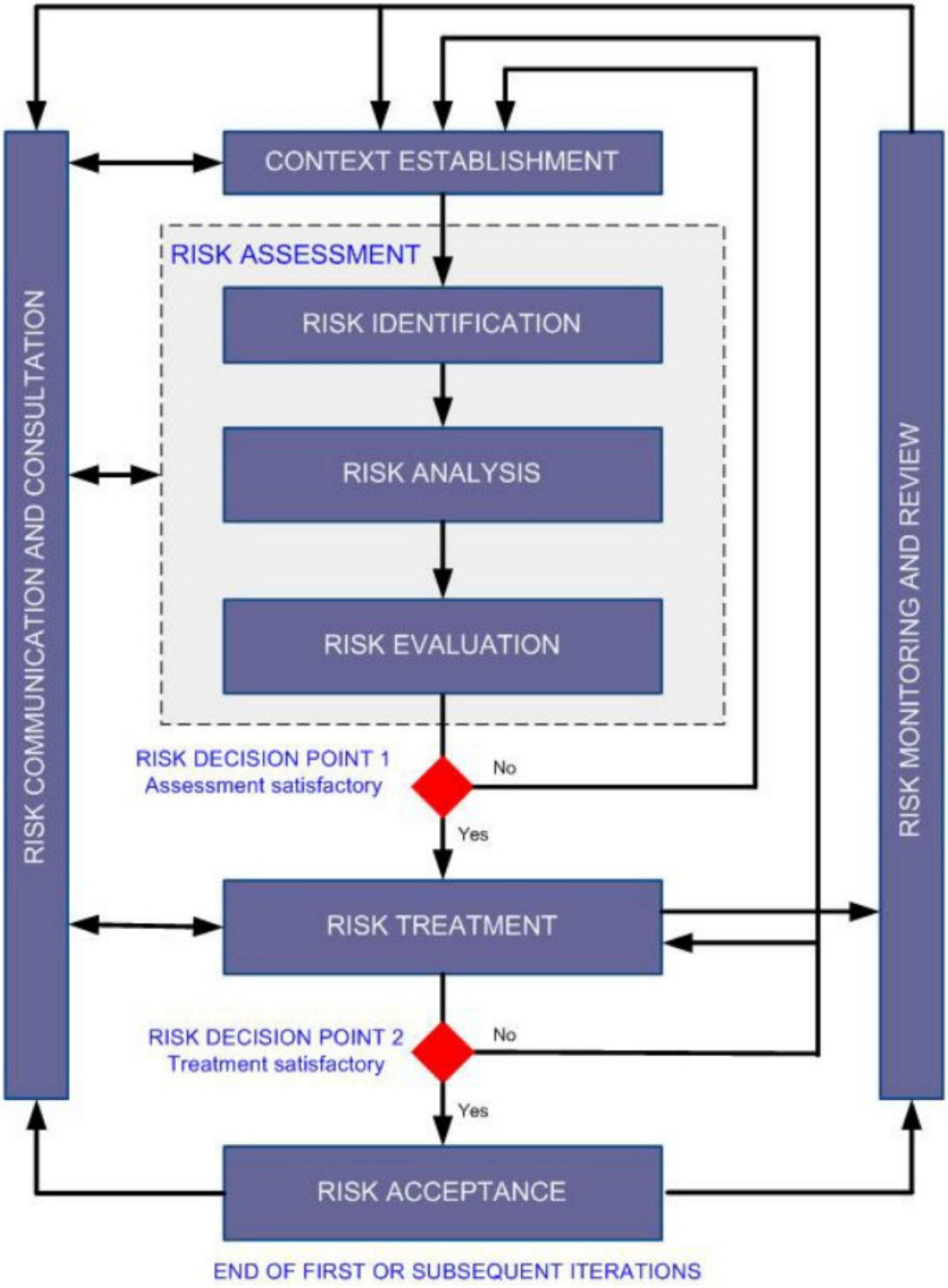
Cyber Kill Chain security Model

MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.



MITRE ATT&CK security model

ISO/IEC 27005 InfoSec Risk Management is an international standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) providing good practice guidance on managing risks to information.

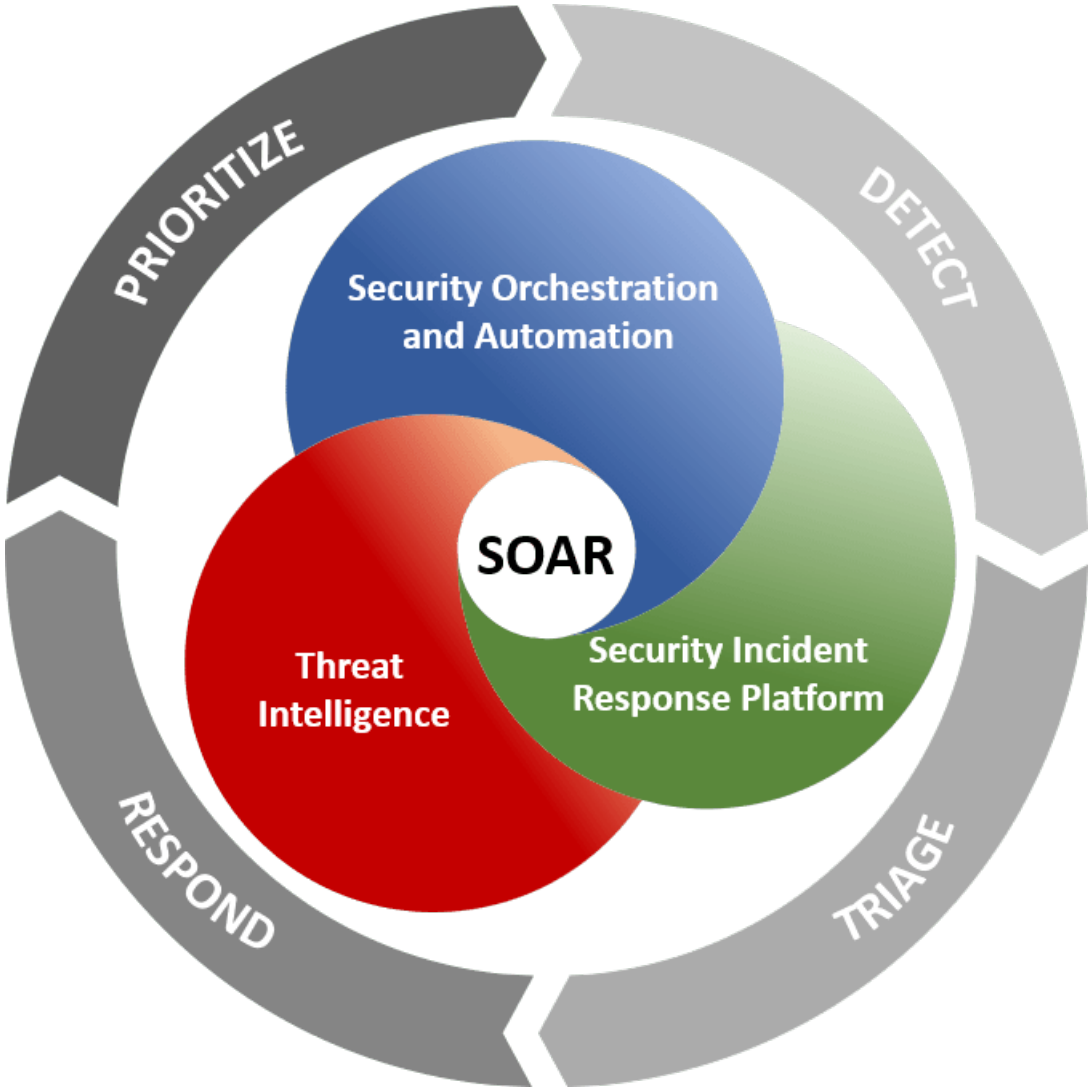


ISO 27005 InfoSec Risk Management

Security Orchestration Automation and Response (SOAR)

Back to the Top

SOAR solutions work by prioritizing and standardizing incident response activities so that security teams can collaborate on investigating and managing incidents. Workflows that can be handled through automation go through standardized response processes defined in playbooks.



SOAR platforms vary depending on vendor, but all of them should include these key features:

- **Orchestration:** A SOAR solution can facilitate the connection between security and productivity tools, such as firewalls and intrusion detection tools.
- **Automation:** A SOAR solution can automate standard cybersecurity workflows, such as the identification of security alerts and possible intrusions.
- **Response:** A SOAR platform can work with both automated and manual processes to support a timely response to security threats.
- **Integration:** A SOAR platform can work with a variety of complementary security products to support the organization's overall security posture.
- **Playbooks and automation:** SOAR helps security teams use collected data to streamline operations through security automation and the use of playbooks.
- **Threat prioritization:** SOAR helps security teams prioritize and group alerts for more efficient threat detection and investigation.
- **Reporting and analysis:** SOAR platforms can generate reports to help security teams identify trends in their organization.
- **Security dashboard:** SOAR platforms can serve as a central dashboard to help security teams monitor and respond to alerts in a collaborative way.

SOAR Tools

Splunk Phantom is a Security Orchestration, Automation, and Response (SOAR) system. It combines security infrastructure orchestration, playbook automation, and case management capabilities to integrate your team, processes, and tools to help you orchestrate security workflows, automate repetitive security tasks, and quickly respond to threats.

IBM IBM Security QRadar SOAR is a Security Orchestration, Automation, and Response (SOAR) system. It's sdesigned to help your security team respond to cyberthreats with confidence, automate with intelligence and collaborate with consistency. It guides your team in resolving incidents by codifying established incident response processes into dynamic playbooks.

Sumo Logic Cloud SOAR is a Security Operations and Automation Incident Response Platform to facilitate and expedite timely management of Incident Response with a rich library of customizable playbooks for different threats and use cases of incident response scenarios expediting and automating response time to incident response events.

Rapid7 Insightconnect is a SOAR solution that integrates with existing solutions to orchestrate vulnerability management processes from notification to remediation. It automations functionality are managed securely end-to-end. Initially, they are encrypted in-transit via TLS and are encrypted at rest in our systems using a public key that's generated by the Orchestrator and sent to the cloud.

LogRhythm RespondX is a seamlessly integrated security orchestration, automation, and response (SOAR) that enables your team to. effectively collaborate, qualify, and manage incidents with. improved quality and speed.

Exabeam incident responder is a SOAR solution that comes with pre-defined playbooks for common incident types such as malware, phishing, and data exfiltration. These playbooks include actions that can automatically run (e.g. go get reputation data for this IP address) or guide a team member (reset this user’s password).

ServiceNow Security Operations is a security orchestration, automation, and response (SOAR) engine built on the Now Platform. It helps security and IT teams respond faster and more efficiently to incidents and vulnerabilities, Security Operations uses intelligent workflows, automation, and a deep connection with Security Operations and IT to streamline response.

SIRP is a no-code risk-based SOAR platform that was built in response to the real-world needs of our customers. Specifically, the need to base security decisions on something more relevant than generic industry systems. Some of the leading enterprises and MSSPs trust SIRP for their security automation.

Chronicle SOAR is a Security Orchestration Automation and Response (SOAR) solution that enables enterprises and MSSPs to gather data and security alerts from different sources by combining the following:

- Orchestration and automation
- Threat intelligence
- Incident response

Palo Alto Networks Cortex XSOAR is a Security Orchestration Automation and Response (SOAR) solution that comes with prebuilt bundles of integrations, playbooks, dashboards, fields, subscription services and all the dependencies needed to support specific security orchestration

use cases.

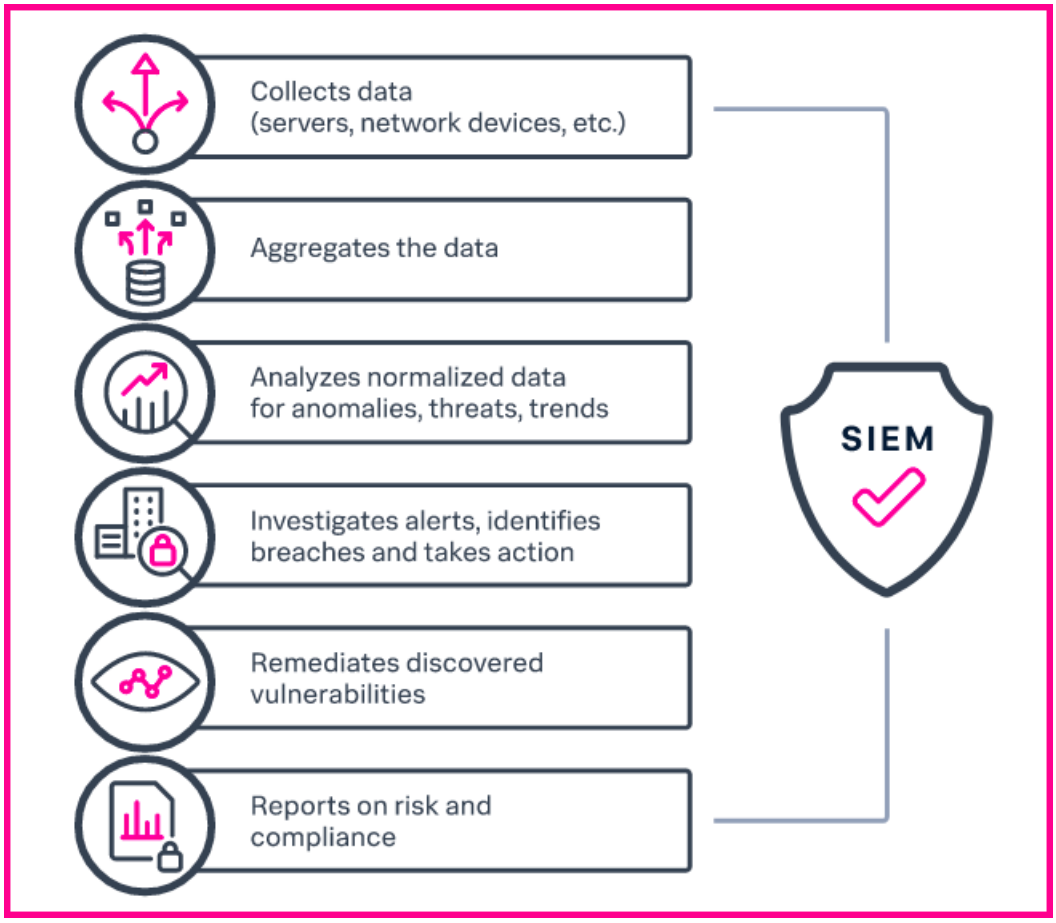
Fortinet FortiSOAR is a security orchestration, automation and response (SOAR) that provides innovative case management, automation, and orchestration. It pulls together all of an organization's tools, helps unify operations, and reduce alert fatigue, context switching, and the mean time to respond to incidents.

Swimlane SOAR is is a security orchestration, automation and response (SOAR) that helps organizations manage the growing volume of alerts more efficiently by automating time-consuming incident response processes. The solution collects security alert data from previously disparate security platforms and automatically responds to alerts using automated workflows and playbooks. It is also designed to centralize data coming back from investigation tools to allow security teams the ability to view all applicable details right from within Swimlane.

Security Information and Event Management (SIEM)

Back to the Top

Security information and event management (SIEM) software collects log data from an organization and then uses the log data to identify, categorize and analyze incidents and events.



SIEM software goals:

- Report on security incidents and events. The software can provide reports with event data, such as failed logins and malware activity.
- Send alerts about potential security issues. The software can use set parameters to determine whether an event is a potential security issue.

- An overview of notable events in your environment that represent potential security incidents.
- Details of all notable events identified in your environment, so you can undertake triage.
- A workbook of all open investigations, allowing you to track your progress and activity while investigating multiple security incidents.
- Risk analysis that lets you score systems and users across your network to identify risks.
- Threat intelligence designed to add context to your security incidents and identify known malicious actors in your environment.
- Protocol intelligence using captured packet data to provide network insights that are relevant to your security investigations, allowing you to identify suspicious traffic, DNS activity and email activity.
- User intelligence lets you investigate and monitor the activity of users and assets in your environment.
- Web intelligence to analyze web traffic in your network.

SIEM Data sources include:

- **Network devices:** Routers, switches, bridges, wireless access points, modems, line drivers, hubs
- **Servers:** Web, proxy, mail, FTP
- **Security devices:** IDP/IPS, firewalls, antivirus software, content filter devices, intrusion detection appliances
- **Applications:** Any software used on any of the above devices
- **Cloud and SaaS solutions:** Software and services not hosted on-premises
- **Remote workforce:** All devices and activity related to remote work

SIEM Tools

Datadog Security Monitoring is a SIE Security information and event management (SIEM) that comes with real-time security monitoring tool , Datadog analyzes and evaluates security and observability data in order to identify threats and reduce risks. Use configurable out-of-the-box rules—mapped to the MITRE ATT&CK™ framework—to track common attacker techniques, such as a VM enumerating all storage buckets in your account.

Logpoint is the only unified SIEM-SOAR solution that collects, analyzes and prioritizes security incidents to help analysts identify and resolve incidents fast and keep businesses safe. With built-in detection, investigation, and response playbooks,

Graylog is a log management to the cloud and aims at SIEM in the midmarket Log management vendor Graylog has released a SaaS version of its enterprise product as well as a new security offering. It provides answers to your team's security, application, and IT infrastructure questions by enabling you to combine, enrich, correlate, query, and visualize all your log data in one place.

Exabeam Fusion is a powerful and advanced cloud-native SIEM and introduces New-Scale SIEM. It unites the combined capabilities of all Exabeam products such as cloud-native data storage, rapid data ingestion, hyper-quick query performance, powerful behavioral analytics, and automation that changes the way analysts do their jobs.

Elastic Security is a platform that unifies SIEM, endpoint security, and cloud security on an open platform, equipping teams to prevent, detect, and respond to threats. It includes a security news

feed, host and network data, detections, timelines, cases, and an abstracted view into the administration of the Elastic endpoint configuration.

Fortinet FortiSIEM

Splunk Enterprise Security is a SIEM Platofrm solution that brings together visibility, correlation, automated response, and remediation in a single, scalable solution. It reduces the complexity of managing network and security operations to effectively free resources, improve breach detection, and even prevent breaches.

OSSEC The Open-source HIDS Security is a multiplatform, open source and free Host Intrusion Detection System (HIDS). It performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response.

LogRhythm NextGen SIEM Platform is a SIEM platform delivers comprehensive security analytics, UEBA, NTA, and SOAR within a single, integrated platform for rapid detection, response, and neutralization of threats.

3. Security Tools

Back to the Top

Acra is a single database security suite with 9 strong security controls: application level encryption, searchable encryption, data masking, data tokenization, secure authentication, data leakage prevention, database request firewall, cryptographically signed audit logging, security events automation. It is designed to cover the most important data security requirements with SQL and NoSQL databases and distributed apps in a fast, convenient, and reliable way.

Netdata is high-fidelity infrastructure monitoring and troubleshooting, real-time monitoring Agent collects thousands of metrics from systems, hardware, containers, and applications with zero configuration. It runs permanently on all your physical/virtual servers, containers, cloud deployments, and edge/IoT devices, and is perfectly safe to install on your systems mid-incident without any preparation.

Themis is a free open-source high-level cryptographic library for mobile and backend platforms. Recommended by OWASP for application security, it allows protecting sensitive data (PII, locations, messages, etc.). While giving easy-to-use and hard-to-misuse API, Themis works to provide secure data storage, message exchange, socket connections, and authentication in apps across 15 platforms and languages.

OWASP is an online community, produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security.

OpenSCAP is U.S. standard maintained by National Institute of Standards and Technology (NIST). It provides multiple tools to assist administrators and auditors with assessment, measurement, and enforcement of security baselines. OpenSCAP maintains great flexibility and interoperability by reducing the costs of performing security audits. Whether you want to evaluate DISA STIGs, NIST‘s USGCB, or Red Hat’s Security Response Team’s content, all are supported by OpenSCAP.

Open Vulnerability and Assessment Language is a community effort to standardize how to assess and report upon the machine state of computer systems. OVAL includes a language to encode system details, and community repositories of content. Tools and services that use OVAL provide

enterprises with accurate, consistent, and actionable information to improve their security.

Trivy is a comprehensive security scanner for vulnerabilities in container images, file systems, and Git repositories, as well as for configuration issues and hard-coded secrets.

Lynis is a security auditing tool for Linux, macOS, and UNIX-based systems. Assists with compliance testing (HIPAA/ISO27001/PCI DSS) and system hardening. Agentless, and installation optional.

RustScan is a Modern Port Scanner.

gosec is a Golang Security Checker that inspects source code for security problems by scanning the Go AST.

Age is a simple, modern and secure encryption tool (and Go library) with small explicit keys, no config options, and UNIX-style composability.

SOPS is an editor of encrypted files that supports YAML, JSON, ENV, INI and BINARY formats and encrypts with AWS KMS, GCP KMS, Azure Key Vault, age, and PGP.

Tailnet lock is a tool that allows you to verify that no node is added to your tailnet without being signed by trusted nodes in your tailnet. When tailnet lock is enabled, even if Tailscale infrastructure is malicious or hacked, attackers can’t send or receive traffic on your tailnet.

Sandstorm is a self-hostable web productivity suite. It's implemented as a security-hardened web app package manager.

mkcert is a simple zero-config tool to make locally trusted development certificates with any names you'd like.

Universal Radio Hacker (URH) is a complete suite for wireless protocol investigation with native support for many common Software Defined Radios. URH allows easy demodulation of signals combined with an automatic detection of modulation parameters making it a breeze to identify the bits and bytes that fly over the air.

Cloudflare Tunnel client is a tunneling daemon that proxies traffic from the Cloudflare network to your origins. This daemon sits between Cloudflare network and your origin (e.g. a webserver). Cloudflare attracts client requests and sends them to you via this daemon, without requiring you to poke holes on your firewall --- your origin can remain as closed as possible.

Cloudflare WARP client is a tool that allows you to protect corporate devices by securely and privately sending traffic from those devices to Cloudflare’s edge, where Cloudflare Gateway can apply advanced web filtering. It also makes it possible to apply advanced Zero Trust policies that check for a device’s health before it connects to corporate applications.

Prowler is an Open Source security tool to perform AWS security best practices assessments, audits, incident response, continuous monitoring, hardening and forensics readiness. It contains more than 240 controls covering CIS, PCI-DSS, ISO27001, GDPR, HIPAA, FFIEC, SOC2, AWS FTR, ENS and custom security frameworks.

eNgine is an automated reconnaissance framework for web applications with a focus on highly configurable streamlined recon process via Engines, recon data correlation and organization, continuous monitoring, backed by a database, and simple yet intuitive UI.

Osmedeus is a Workflow Engine for Offensive Security. It was designed to build a foundation with the capability and flexibility that allows you to build your own reconnaissance system and run it on a large number of targets.

OWASP Nettacker is a project created to automate information gathering, vulnerability scanning and eventually generating a report for networks, including services, bugs, vulnerabilities, misconfigurations, and other information. This software will utilize TCP SYN, ACK, ICMP, and many other protocols in order to detect and bypass Firewall/IDS/IPS devices.

Terrascan is a static code analyzer for Infrastructure as Code to mitigate risk before provisioning cloud native infrastructure.

Sliver is an open source cross-platform adversary emulation/red team framework, it can be used by organizations of all sizes to perform security testing. Sliver's implants support C2 over Mutual TLS (mTLS), WireGuard, HTTP(S), and DNS and are dynamically compiled with per-binary asymmetric encryption keys.

Payloads All The Things is a list of useful payloads and bypass for Web Application Security and Pentest/CTF.

TheHive is a scalable 3-in-1 open source and free Security Incident Response Platform designed to make life easier for SOCs, CSIRTs, CERTs and any information security practitioner dealing with security incidents that need to be investigated and acted upon swiftly. It is the perfect companion to MISP.

MITRE ATT&CK® is a global knowledge base of adversary tactics and techniques based on real-world security observations. It is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

CALDERA™ is a cyber security platform designed to easily automate adversary emulation, assist manual red-teams, and automate incident response.

Pyrsia is a Decentralized Package Network that aims to secure the software supply chain of open-source dependencies by creating a system that secures open-source builds and distribution.

GitGuardian shield (ggshield) is a CLI application that runs in your local environment or in a CI environment to help you detect more than 350+ types of secrets, as well as other potential security vulnerabilities or policy breaks.

ggshield-action is a GitGuardian Shield GitHub Action to find exposed credentials in your commits.

Atomic Red Team™ is a library of tests mapped to the MITRE ATT&CK® framework. Security teams can use Atomic Red Team to quickly, portably, and reproducibly test their environments.

OpenCTI is an open source platform allowing organizations to manage their cyber threat intelligence knowledge and observables. It has been created in order to structure, store, organize and visualize technical and non-technical information about cyber threats.

Amass is an OWASP Project that performs network mapping of attack surfaces and external asset discovery using open source information gathering and active reconnaissance techniques.

CrowdSec is an open-source and collaborative security stack leveraging the crowd power to generate a global CTI database to protect the user network. It will analyze behaviors, respond to attacks & share signals across the community.

Crowdsec Firewall Bouncer is a tool that will fetch new and old decisions from a CrowdSec API to add them in a blocklist used by supported firewalls.

Supported firewalls:

- iptables (IPv4 heavy_check_mark / IPv6 heavy_check_mark)
- nftables (IPv4 heavy_check_mark / IPv6 heavy_check_mark)
- ipset only (IPv4 heavy_check_mark / IPv6 heavy_check_mark)
- pf (IPV4 heavy_check_mark / IPV6 heavy_check_mark)

Pulse is a powerful logging system for Apple Platforms builtin in SwiftUI. It allows you to record and inspect logs and `URLSession` network requests right from your iOS app. Shared logs and view them in Pulse Pro or use remote logging to see them in real-time. Logs are stored locally and never leave your devices.

tshark.dev is your complete guide to working with packet captures on the command-line.

Nebula is a scalable overlay networking tool with a focus on performance, simplicity and security. It lets you seamlessly connect computers anywhere in the world. Nebula is portable, and runs on Linux, OSX, Windows, iOS, and Android. It can be used to connect a small number of computers, but is also able to connect tens of thousands of computers.

Parca is a tool for continuous profiling for analysis of CPU and memory usage, down to the line number and throughout time. Saving infrastructure cost, improving performance, and increasing reliability.

DeepFlow is a highly automated observability platform for cloud-native developers. Using new technologies such as eBPF, WASM, and OpenTelemetry, DeepFlow innovatively implements core mechanisms such as AutoTracing, AutoMetrics, AutoTagging, and SmartEncoding, which greatly avoids code instrumentation and significantly reduces the resource overhead of back-end data warehouses.

LGTM is a tool that finds and prevents zero-days and other critical bugs, with customizable alerts and automated code review.

Semgrep is a code scanning at ludicrous speed. Find bugs and reachable dependency vulnerabilities. Enforce standards on every commit.

Socket Security is a tool that protects your app from malicious open source dependencies.

Snyk is a tool that find, fix (and prevent!) known vulnerabilities in your code.

GitProtect.io is a free Backup for GitHub that does automatic, daily repo and metadata backup - no maintenance needed: fast restore, DR, AWS, and S3 cloud storage support.

Cloudback Backup is a tool that automatically backups of your repos, metadata and even LFS. Backup to AWS, Azure, OneDrive, GCP, and more. Also, does instant restores.

Mend Bolt isa that detects open source vulnerabilities in real time with suggested fixes for quick remediation.

Rewind Backups for GitHub (Formerly BackHub) is a tool that does daily, automatic backups of your repos & metadata. Restore your backups with metadata in seconds + Sync to your S3 or Azure.

Renovate is a tool that keeps dependencies up-to-date with automated Pull Requests.

GuardRails provides continuous security feedback for modern development teams.

Dnsmasq is a tool that provides network infrastructure for small networks: DNS, DHCP, router advertisement and network boot. It is designed to be lightweight and have a small footprint, suitable for resource constrained routers and firewalls. It has also been widely used for tethering on smartphones and portable hotspots, and to support virtual networking in virtualisation frameworks. Supported platforms include Linux (with glibc and uclibc), Android, BSD, and MacOS.

Hetty is an HTTP toolkit for security research. It aims to become an open source alternative to commercial software like Burp Suite Pro, with powerful features tailored to the needs of the infosec and bug bounty community.

IVRE is a network recon framework. That let's you build your own, self-hosted and fully-controlled alternatives to Shodan, ZoomEye, Censys, and GreyNoise. IVRE can run your Passive DNS service, collect and analyse network intelligence from your sensors, and much more.

MISP is an open source software solution for collecting, storing, distributing and sharing cyber security indicators and threats about cyber security incidents analysis and malware analysis. MISP is designed by and for incident analysts, security and ICT professionals or malware reversers to support their day-to-day operations to share structured information efficiently.

Rapid7 Nexpose is a vulnerability scanner which aims to support the entire vulnerability management lifecycle, including discovery, detection, verification, risk classification, impact analysis, reporting and mitigation. It integrates with Rapid7's Metasploit for vulnerability exploitation.

Nikto is an Open Source web server scanner which performs comprehensive tests against web servers for multiple items, including over 6400 potentially dangerous files/CGIs, checks for outdated versions of over 1200 servers, and version specific problems on over 270 servers.

Scapy is a powerful interactive packet manipulation tool, packet generator, network scanner, network discovery tool, and packet sniffer.

OSSEC HIDS(Host Intrusion Detection System) is an open source security tool that performs log analysis, integrity checking, rootkit detection, time-based alerting and active response. In addition to its IDS functionality, it is commonly used as a SEM/SIM solution.

OpenMPTCProuter is a tool that uses MultiPath TCP (MPTCP) to really aggregate multiple Internet connections and OpenWrt.

Cortex is a Powerful Observable Analysis and Active Response Engine. This solves a common problem frequently encountered by SOCs, CSIRTs and security researchers in the course of threat intelligence, digital forensics and incident response.

Scrummage is an OSINT tool that centralises search functionality from a bounty of powerful, publicly-available, third-party, OSINT websites.

Bettercap is a powerful, easily extensible and portable framework written in Go which aims to offer to security researchers, red teamers and reverse engineers an easy to use, all-in-one solution with all the features they might possibly need for performing reconnaissance and attacking WiFi networks, Bluetooth Low Energy devices, wireless HID devices and Ethernet networks.

Wifiphisher is a rogue Access Point framework for conducting red team engagements or Wi-Fi security testing. Using Wifiphisher, penetration testers can easily achieve a man-in-the-middle position against wireless clients by performing targeted Wi-Fi association attacks.

Attack Surface Analyzer is a Microsoft developed open source security tool that analyzes the attack surface of a target system and reports on potential security vulnerabilities introduced during the installation of software or system misconfiguration.

Intel Owl is an Open Source Intelligence, or OSINT solution to get threat intelligence data about a specific file, an IP or a domain from a single API at scale. It integrates a number of analyzers available online and a lot of cutting-edge malware analysis tools.

Deepfence ThreatMapper is a runtime tool that hunts for vulnerabilities in your cloud native production platforms(Linux, K8s, AWS Fargate and more.), and ranks these vulnerabilities based on their risk-of-exploit.

Dockle is a Container Image Linter for Security and helping build the Best-Practice Docker Image.

SpiceDB is an open source database system for managing security-critical application permissions inspired by Google's Zanzibar paper.

Virtualization-based Security (VBS) is a hardware virtualization feature to create and isolate a secure region of memory from the normal operating system.

Hypervisor-Enforced Code Integrity (HVCI) is a mechanism whereby a hypervisor, such as Hyper-V, uses hardware virtualization to protect kernel-mode processes against the injection and execution of malicious or unverified code. Code integrity validation is performed in a secure environment that is resistant to attack from malicious software, and page permissions for kernel mode are set and maintained by the hypervisor.

eBPF is a technology that can run sandboxed programs in the Linux kernel without changing kernel source code or loading kernel modules. By making the Linux kernel programmable, infrastructure software can leverage existing layers, making them more intelligent and feature-rich without continuing to add additional layers of complexity to the system.

eBPF for Windows is an eBPF implementation that runs on top of Windows. eBPF is a well-known technology for providing programmability and agility, especially for extending an OS kernel, for use cases such as DoS protection and observability.

Coreboot is a replacement for your BIOS / UEFI with a strong focus on boot speed, security and flexibility. It is designed to boot your operating system as fast as possible without any compromise to security, with no back doors.

TianoCore is a community project supporting an open source implementation of the Unified Extensible Firmware Interface (UEFI). EDK II is a modern, feature-rich, cross-platform firmware development environment for the UEFI and UEFI Platform Initialization (PI) specifications.

OWASP Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool being maintained

under the umbrella of the Open Web Application Security Project (OWASP). ZAP is designed specifically for testing web applications and is both flexible and extensible. Great for pentesters, devs, QA, and CI/CD integration. At its core, ZAP is what is known as a "man-in-the-middle proxy."

IDA Pro(Interactive DisAssembler Professional) is a programmable and multi-processor disassembler combined with a local/remote debugger and along with a complete plugin programming environment. It's a great tool for testing and discovering security vulnerabilities.

Ghidra is a software reverse engineering (SRE) framework developed by NSA's Research Directorate for NSA's cybersecurity mission. It helps analyze any malicious code and malware like viruses, and can give cybersecurity professionals a better understanding of potential vulnerabilities in their networks and systems.

Exploit Database is a CVE compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers. The goal is to serve the most comprehensive collection of exploits gathered through direct submissions, mailing lists, as well as other public sources, and present them.

Rapid7 Vulnerability & Exploit Database is a curated repository of vetted computer software exploits and exploitable vulnerabilities. Technical details for over 180,000 vulnerabilities and 4,000 exploits are available for security professionals and researchers to review. These vulnerabilities are utilized by our vulnerability management tool InsightVM.

InsightVM is a data-rich resource that can amplify the other solutions in your tech stack, from SIEMs and firewalls to ticketing systems. Only InsightVM integrates with 40+ other leading technologies, and with an open RESTful API, your vulnerability data makes your other tools more valuable.

DataWave is an ingest/query framework that leverages Apache Accumulo to provide fast, secure data access.

Emissary is a P2P based data-driven workflow engine that runs in a heterogeneous possibly widely dispersed, multi-tiered P2P network of compute resources. Workflow itineraries are not pre-planned as in conventional workflow engines, but are discovered as more information is discovered about the data.

MADCert is a cross-platform tool that consists of a certificate generator, a file system certificate manager, and a command line interface for the purposes of testing.

BLESS(Bastion's Lambda Ephemeral SSH Service) is an SSH Certificate Authority that runs as an AWS Lambda function and is used to sign SSH public keys.

Zuul is an L7 application gateway that provides capabilities for dynamic routing, monitoring, resiliency, security, and more.

Chaos Monkey is a resiliency tool that helps applications tolerate random instance failures. It is fully integrated with Spinnaker, the continuous delivery platform. Chaos Monkey will work with any backend that Spinnaker supports (AWS, Google Compute Engine, Azure, Kubernetes, Cloud Foundry).

Vuls is an agent-less vulnerability scanner for Linux, FreeBSD, Container, WordPress, Programming language libraries, Network devices.

SpiderFoot is an open source intelligence (OSINT) automation tool. It integrates with just about every data source available and utilises a range of methods for data analysis, making that data easy to navigate.

Lynis is a security auditing tool for Linux, macOS, and UNIX-based systems. Assists with compliance testing (HIPAA/ISO27001/PCI DSS) and system hardening. Agentless, and installation is optional.

Priam is a tool/process for backup/recovery, Token Management, and Centralized Configuration management for Cassandra.

Vector is an on-host performance monitoring framework which exposes hand picked high resolution metrics to every engineer's browser.

Atlas is an in-memory dimensional time series database.

SELinux is a security enhancement to Linux which allows users and administrators more control over access control. Access can be constrained on such variables as which users and applications can access which resources. These resources may take the form of files. Standard Linux access controls, such as file modes (-rwxr-xr-x) are modifiable by the user and the applications which the user runs. Conversely, SELinux access controls are determined by a policy loaded on the system which may not be changed by careless users or misbehaving applications.

AppArmor is an effective and easy-to-use Linux application security system. AppArmor proactively protects the operating system and applications from external or internal threats, even zero-day attacks, by enforcing good behavior and preventing both known and unknown application flaws from being exploited. AppArmor supplements the traditional Unix discretionary access control (DAC) model by providing mandatory access control (MAC). It has been included in the mainline Linux kernel since version 2.6.36 and its development has been supported by Canonical since 2009.

Control Groups(Cgroups) is a Linux kernel feature that allows you to allocate resources such as CPU time, system memory, network bandwidth, or any combination of these resources for user-defined groups of tasks (processes) running on a system.

EarlyOOM is a daemon for Linux that enables users to more quickly recover and regain control over their system in low-memory situations with heavy swap usage.

Libgcrypt is a general purpose cryptographic library originally based on code from GnuPG.

Kali Linux is an open source project that is maintained and funded by Offensive Security, a provider of world-class information security training and penetration testing services.

Pi-hole is a DNS sinkhole that protects your devices from unwanted content, without installing any client-side software, intended for use on a private network. It is designed for use on embedded devices with network capability, such as the Raspberry Pi, but it can be used on other machines running Linux and cloud implementations.

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs. It works with any wireless network interface controller whose driver supports raw monitoring mode and can sniff 802.11a, 802.11b and 802.11g traffic.

Burp Suite is a leading range of cybersecurity tools.

KernelCI is a community-based open source distributed test automation system focused on upstream kernel development. The primary goal of KernelCI is to use an open testing philosophy to ensure the quality, stability and long-term maintenance of the Linux kernel.

Continuous Kernel Integration project helps find bugs in kernel patches before they are commited to an upstram kernel tree. We are team of kernel developers, kernel testers, and automation engineers.

Cilium uses eBPF to accelerate getting data in and out of L7 proxies such as Envoy, enabling efficient visibility into API protocols like HTTP, gRPC, and Kafka.

Hubble is a Network, Service & Security Observability for Kubernetes using eBPF.

Istio is an open platform to connect, manage, and secure microservices. Istio's control plane provides an abstraction layer over the underlying cluster management platform, such as Kubernetes and Mesos.

Certgen is a convenience tool to generate and store certificates for Hubble Relay mTLS.

syzkaller is an unsupervised, coverage-guided kernel fuzzer.

SchedViz is a tool for gathering and visualizing kernel scheduling traces on Linux machines.

oss-fuzz aims to make common open source software more secure and stable by combining modern fuzzing techniques with scalable, distributed execution.

OSSEC is a free, open-source host-based intrusion detection system. It performs log analysis, integrity checking, Windows registry monitoring, rootkit detection, time-based alerting, and active response.

Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

Wfuzz was created to facilitate the task in web applications assessments and it is based on a simple concept: it replaces any reference to the FUZZ keyword by the value of a given payload.

Nmap is a security scanner used to discover hosts and services on a computer network, thus building a "map" of the network.

Patchwork is a web-based patch tracking system designed to facilitate the contribution and management of contributions to an open-source project.

pfSense is a free and open source firewall and router that also features unified threat management, load balancing, multi WAN, and more.

Snowpatch is a continuous integration tool for projects using a patch-based, mailing-list-centric git workflow. This workflow is used by a number of well-known open source projects such as the Linux kernel.

Snort is an open-source, free and lightweight network intrusion detection system (NIDS) software for Linux and Windows to detect emerging threats.

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

Tink is a multi-language, cross-platform, open source library that provides cryptographic APIs that are secure, easy to use correctly, and harder to misuse.

ClamAV is an open source antivirus engine for detecting trojans, viruses, malware & other malicious threats.

4. Network Security

Back to the Top

Networking Tools & Concepts

Qt Network Authorization is a tool that provides a set of APIs that enable Qt applications to obtain limited access to online accounts and HTTP services without exposing users' passwords.

cURL is a computer software project providing a library and command-line tool for transferring data using various network protocols(HTTP, HTTPS, FTP, FTPS, SCP, SFTP, TFTP, DICT, TELNET, LDAP LDAPS, MQTT, POP3, POP3S, RTMP, RTMPS, RTSP, SCP, SFTP, SMB, SMBS, SMTP or SMTPS). cURL is also used in cars, television sets, routers, printers, audio equipment, mobile phones, tablets, settop boxes, media players and is the Internet transfer engine for thousands of software applications in over ten billion installations.

cURL Fuzzer is a quality assurance testing for the curl project.

DoH is a stand-alone application for DoH (DNS-over-HTTPS) name resolves and lookups.

Authelia is an open-source highly-available authentication server providing single sign-on capability and two-factor authentication to applications running behind NGINX.

nginx(engine x) is an HTTP and reverse proxy server, a mail proxy server, and a generic TCP/UDP proxy server, originally written by Igor Sysoev.

Proxmox Virtual Environment(VE) is a complete open-source platform for enterprise virtualization. It inlcudes a built-in web interface that you can easily manage VMs and containers, software-defined storage and networking, high-availability clustering, and multiple out-of-the-box tools on a single solution.

Wireshark is a very popular network protocol analyzer that is commonly used for network troubleshooting, analysis, and communications protocol development. Learn more about the other useful Wireshark Tools available.

HTTPie is a command-line HTTP client. Its goal is to make CLI interaction with web services as human-friendly as possible. HTTPie is designed for testing, debugging, and generally interacting with APIs & HTTP servers.

HTTPStat is a tool that visualizes curl statistics in a simple layout.

Wuzz is an interactive cli tool for HTTP inspection. It can be used to inspect/modify requests copied from the browser's network inspector with the "copy as cURL" feature.

Websocat is a ommand-line client for WebSockets, like netcat (or curl) for ws:// with advanced socat-like functions.

- Connection: In networking, a connection refers to pieces of related information that are transferred through a network. This generally infers that a connection is built before the data transfer (by following the procedures laid out in a protocol) and then is deconstructed at the at the end of the data transfer.
- Packet: A packet is, generally speaking, the most basic unit that is transferred over a network. When communicating over a network, packets are the envelopes that carry your data (in pieces) from one end point to the other.

Packets have a header portion that contains information about the packet including the source and destination, timestamps, network hops. The main portion of a packet contains the actual data being transferred. It is sometimes called the body or the payload.

- Network Interface: A network interface can refer to any kind of software interface to networking hardware. For instance, if you have two network cards in your computer, you can control and configure each network interface associated with them individually.

A network interface may be associated with a physical device, or it may be a representation of a virtual interface. The "loop-back" device, which is a virtual interface to the local machine, is an example of this.

- LAN: LAN stands for "local area network". It refers to a network or a portion of a network that is not publicly accessible to the greater internet. A home or office network is an example of a LAN.
- WAN: WAN stands for "wide area network". It means a network that is much more extensive than a LAN. While WAN is the relevant term to use to describe large, dispersed networks in general, it is usually meant to mean the internet, as a whole. If an interface is connected to the WAN, it is generally assumed that it is reachable through the internet.
- Protocol: A protocol is a set of rules and standards that basically define a language that devices can use to communicate. There are a great number of protocols in use extensively in networking, and they are often implemented in different layers.

Some low level protocols are TCP, UDP, IP, and ICMP. Some familiar examples of application layer protocols, built on these lower protocols, are HTTP (for accessing web content), SSH, TLS/SSL, and FTP.

- Port: A port is an address on a single machine that can be tied to a specific piece of software. It is not a physical interface or location, but it allows your server to be able to communicate using more than one application.
- Firewall: A firewall is a program that decides whether traffic coming into a server or going out should be allowed. A firewall usually works by creating rules for which type of traffic is acceptable on which ports. Generally, firewalls block ports that are not used by a specific application on a server.

- NAT: Network address translation is a way to translate requests that are incoming into a routing server to the relevant devices or servers that it knows about in the LAN. This is usually implemented in physical LANs as a way to route requests through one IP address to the necessary backend servers.
- VPN: Virtual private network is a means of connecting separate LANs through the internet, while maintaining privacy. This is used as a means of connecting remote systems as if they were on a local network, often for security reasons.

Network Layers

While networking is often discussed in terms of topology in a horizontal way, between hosts, its implementation is layered in a vertical fashion throughout a computer or network. This means is that there are multiple technologies and protocols that are built on top of each other in order for communication to function more easily. Each successive, higher layer abstracts the raw data a little bit more, and makes it simpler to use for applications and users. It also allows you to leverage lower layers in new ways without having to invest the time and energy to develop the protocols and applications that handle those types of traffic.

As data is sent out of one machine, it begins at the top of the stack and filters downwards. At the lowest level, actual transmission to another machine takes place. At this point, the data travels back up through the layers of the other computer. Each layer has the ability to add its own "wrapper" around the data that it receives from the adjacent layer, which will help the layers that come after decide what to do with the data when it is passed off.

One method of talking about the different layers of network communication is the OSI model. OSI stands for Open Systems Interconnect.This model defines seven separate layers. The layers in this model are:

- Application: The application layer is the layer that the users and user-applications most often interact with. Network communication is discussed in terms of availability of resources, partners to communicate with, and data synchronization.
- Presentation: The presentation layer is responsible for mapping resources and creating context. It is used to translate lower level networking data into data that applications expect to see.
- Session: The session layer is a connection handler. It creates, maintains, and destroys connections between nodes in a persistent way.
- Transport: The transport layer is responsible for handing the layers above it a reliable connection. In this context, reliable refers to the ability to verify that a piece of data was received intact at the other end of the connection. This layer can resend information that has been dropped or corrupted and can acknowledge the receipt of data to remote computers.
- Network: The network layer is used to route data between different nodes on the network. It uses addresses to be able to tell which computer to send information to. This layer can also break apart larger messages into smaller chunks to be reassembled on the opposite end.
- Data Link: This layer is implemented as a method of establishing and maintaining reliable links between different nodes or devices on a network using existing physical connections.

- Physical: The physical layer is responsible for handling the actual physical devices that are used to make a connection. This layer involves the bare software that manages physical connections as well as the hardware itself (like Ethernet).

The TCP/IP model, more commonly known as the Internet protocol suite, is another layering model that is simpler and has been widely adopted.It defines the four separate layers, some of which overlap with the OSI model:

- Application: In this model, the application layer is responsible for creating and transmitting user data between applications. The applications can be on remote systems, and should appear to operate as if locally to the end user. The communication takes place between peers network.
- Transport: The transport layer is responsible for communication between processes. This level of networking utilizes ports to address different services. It can build up unreliable or reliable connections depending on the type of protocol used.
- Internet: The internet layer is used to transport data from node to node in a network. This layer is aware of the endpoints of the connections, but does not worry about the actual connection needed to get from one place to another. IP addresses are defined in this layer as a way of reaching remote systems in an addressable manner.
- Link: The link layer implements the actual topology of the local network that allows the internet layer to present an addressable interface. It establishes connections between neighboring nodes to send data.

Interfaces

Interfaces are networking communication points for your computer. Each interface is associated with a physical or virtual networking device. Typically, your server will have one configurable network interface for each Ethernet or wireless internet card you have. In addition, it will define a virtual network interface called the "loopback" or localhost interface. This is used as an interface to connect applications and processes on a single computer to other applications and processes. You can see this referenced as the "lo" interface in many tools.

Network Protocols

Networking works by piggybacks on a number of different protocols on top of each other. In this way, one piece of data can be transmitted using multiple protocols encapsulated within one another.

Media Access Control(MAC) is a communications protocol that is used to distinguish specific devices. Each device is supposed to get a unique MAC address during the manufacturing process that differentiates it from every other device on the internet. Addressing hardware by the MAC address allows you to reference a device by a unique value even when the software on top may change the name for that specific device during operation. Media access control is one of the only protocols from the link layer that you are likely to interact with on a regular basis.

The IP protocol is one of the fundamental protocols that allow the internet to work. IP addresses are unique on each network and they allow machines to address each other across a network. It is implemented on the internet layer in the IP/TCP model. Networks can be linked together, but traffic

must be routed when crossing network boundaries. This protocol assumes an unreliable network and multiple paths to the same destination that it can dynamically change between. There are a number of different implementations of the protocol. The most common implementation today is IPv4, although IPv6 is growing in popularity as an alternative due to the scarcity of IPv4 addresses available and improvements in the protocols capabilities.

ICMP: internet control message protocol is used to send messages between devices to indicate the availability or error conditions. These packets are used in a variety of network diagnostic tools, such as ping and traceroute. Usually ICMP packets are transmitted when a packet of a different kind meets some kind of a problem. Basically, they are used as a feedback mechanism for network communications.

TCP: Transmission control protocol is implemented in the transport layer of the IP/TCP model and is used to establish reliable connections. TCP is one of the protocols that encapsulates data into packets. It then transfers these to the remote end of the connection using the methods available on the lower layers. On the other end, it can check for errors, request certain pieces to be resent, and reassemble the information into one logical piece to send to the application layer. The protocol builds up a connection prior to data transfer using a system called a three-way handshake. This is a way for the two ends of the communication to acknowledge the request and agree upon a method of ensuring data reliability. After the data has been sent, the connection is torn down using a similar four-way handshake. TCP is the protocol of choice for many of the most popular uses for the internet, including WWW, FTP, SSH, and email. It is safe to say that the internet we know today would not be here without TCP.

UDP: User datagram protocol is a popular companion protocol to TCP and is also implemented in the transport layer. The fundamental difference between UDP and TCP is that UDP offers unreliable data transfer. It does not verify that data has been received on the other end of the connection. This might sound like a bad thing, and for many purposes, it is. However, it is also extremely important for some functions. It’s not required to wait for confirmation that the data was received and forced to resend data, UDP is much faster than TCP. It does not establish a connection with the remote host, it simply fires off the data to that host and doesn't care if it is accepted or not. Since UDP is a simple transaction, it is useful for simple communications like querying for network resources. It also doesn't maintain a state, which makes it great for transmitting data from one machine to many real-time clients. This makes it ideal for VOIP, games, and other applications that cannot afford delays.

HTTP: Hypertext transfer protocol is a protocol defined in the application layer that forms the basis for communication on the web. HTTP defines a number of functions that tell the remote system what you are requesting. For instance, GET, POST, and DELETE all interact with the requested data in a different way.

FTP: File transfer protocol is in the application layer and provides a way of transferring complete files from one host to another. It is inherently insecure, so it is not recommended for any externally facing network unless it is implemented as a public, download-only resource.

DNS: Domain name system is an application layer protocol used to provide a human-friendly naming mechanism for internet resources. It is what ties a domain name to an IP address and allows you to access sites by name in your browser.

SSH: Secure shell is an encrypted protocol implemented in the application layer that can be used to communicate with a remote server in a secure way. Many additional technologies are built around this protocol because of its end-to-end encryption and ubiquity. There are many other protocols that we haven't covered that are equally important. However, this should give you a good overview of some of the fundamental technologies that make the internet and networking possible.

REST(REpresentational State Transfer) is an architectural style for providing standards between computer systems on the web, making it easier for systems to communicate with each other.

JSON Web Token (JWT) is a compact URL-safe means of representing claims to be transferred between two parties. The claims in a JWT are encoded as a JSON object that is digitally signed using JSON Web Signature (JWS).

OAuth 2.0 is an open source authorization framework that enables applications to obtain limited access to user accounts on an HTTP service, such as Amazon, Google, Facebook, Microsoft, Twitter GitHub, and DigitalOcean. It works by delegating user authentication to the service that hosts the user account, and authorizing third-party applications to access the user account.

Virtualization

KVM (for Kernel-based Virtual Machine) is a full virtualization solution for Linux on x86 hardware containing virtualization extensions (Intel VT or AMD-V). It consists of a loadable kernel module, kvm.ko, that provides the core virtualization infrastructure and a processor specific module, kvm-intel.ko or kvm-amd.ko.

QEMU is a fast processor emulator using a portable dynamic translator. QEMU emulates a full system, including a processor and various peripherals. It can be used to launch a different Operating System without rebooting the PC or to debug system code.

Hyper-V enables running virtualized computer systems on top of a physical host. These virtualized systems can be used and managed just as if they were physical computer systems, however they exist in virtualized and isolated environment. Special software called a hypervisor manages access between the virtual systems and the physical hardware resources. Virtualization enables quick deployment of computer systems, a way to quickly restore systems to a previously known good state, and the ability to migrate systems between physical hosts.

VirtManager is a graphical tool for managing virtual machines via libvirt. Most usage is with QEMU/KVM virtual machines, but Xen and libvirt LXC containers are well supported. Common operations for any libvirt driver should work.

oVirt is an open-source distributed virtualization solution, designed to manage your entire enterprise infrastructure. oVirt uses the trusted KVM hypervisor and is built upon several other community projects, including libvirt, Gluster, PatternFly, and Ansible.Founded by Red Hat as a community project on which Red Hat Enterprise Virtualization is based allowing for centralized management of virtual machines, compute, storage and networking resources, from an easy-to-use web-based front-end with platform independent access.

Xen is focused on advancing virtualization in a number of different commercial and open source applications, including server virtualization, Infrastructure as a Services (IaaS), desktop virtualization, security applications, embedded and hardware appliances, and automotive/aviation.

Ganeti is a virtual machine cluster management tool built on top of existing virtualization technologies such as Xen or KVM and other open source software. Once installed, the tool assumes management of the virtual instances (Xen DomU).

Packer is an open source tool for creating identical machine images for multiple platforms from a single source configuration. Packer is lightweight, runs on every major operating system, and is highly performant, creating machine images for multiple platforms in parallel. Packer does not replace configuration management like Chef or Puppet. In fact, when building images, Packer is able to use tools like Chef or Puppet to install software onto the image.

Vagrant is a tool for building and managing virtual machine environments in a single workflow. With an easy-to-use workflow and focus on automation, Vagrant lowers development environment setup time, increases production parity, and makes the "works on my machine" excuse a relic of the past. It provides easy to configure, reproducible, and portable work environments built on top of industry-standard technology and controlled by a single consistent workflow to help maximize the productivity and flexibility of you and your team.

VMware Workstation is a hosted hypervisor that runs on x64 versions of Windows and Linux operating systems; it enables users to set up virtual machines on a single physical machine, and use them simultaneously along with the actual machine.

Back to the Top

License