Jan-Dec 2020

Vol. 1 Issue 1

Research Review Journal

Published Cybersecurity Research From SANS.edu Graduate Students

Johannes Ullrich, PhD
Dean of Research
SANS Faculty Fellow
JUllrich@sans.edu

Supervising the SANS.edu research process has been a rewarding and humbling opportunity. In this new journal, we provide links to the fantastic work done by our students and their faculty research advisors. I hope it will help you solve, or at least better understand, some of the problems you are facing in the industry.

There is one theme that connects these papers: the problems and solutions discussed in these papers matter. Our students selected these topics from the challenges they face in their jobs as cybersecurity professionals in business, government, and consulting. A lot of sweat (and maybe tears) went into each research project. I hope the outcome - a rigorous analysis of the problem and potential solution - was worth it to our students, and the wider cybersecurity community.

I am grateful for our outstanding research committee and SANS.edu staff who helped guide students through the process of creating these rigorous, academic papers. Please share any articles you find helpful or interesting, and let me know which paper you were able to apply to your work.

Defense Leadership Forensics Cloud ICS

Table of Contents

Defense: Defend, Monitor, Detect

Leadership: Strategy, Architecture, Audit

Table of Contents

Forensics: Digital Forensics, Threat Hunting, Incident Response

Cloud Security

Industrial Control Systems Security

Zeek Log Reconnaissance with Network Graphs Using Maltego Casefile
by Ricky (Xiao) Tan

Many "needle-in-a-haystack" approaches to threat discovery that rely on log examination are resource-intensive and unsuitable for time-sensitive engagements. This reality creates unique difficulties for teams with few personnel, skills, and tools. Such challenges can make it difficult for analysts to conduct effective incident response, threat hunting, and continuous monitoring of a network. This paper showcases an alternative to traditional investigative methods by using network graphs. Leveraging a freely available, commercial-off-the-shelf tool called Maltego Casefile, analysts can visualize key relationships between various Zeek log fields to quickly gain insight into network traffic. This research will explore variations of the network graph technique on multiple packet capture (PCAP) datasets containing known-malicious activity. Continue reading at sans.org/u/1aDN.

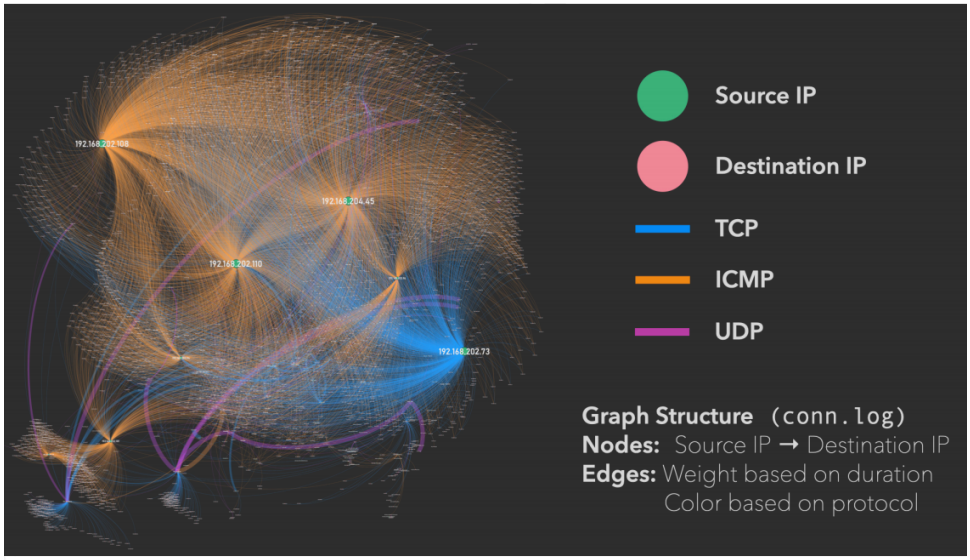


Figure 29. Network activity in the 2012 MACCDC dataset (conn.log)

> *Sifting through mountains of log data can be overwhelming and leave the analyst asking , 'Where should I start?' Ricky's research tries to answer that question by demonstrating how one can create meaningful graphs based on network traffic using Maltego Casefile. Using packet captures or Zeek logs as input, Casefile can create graphs that help the analyst hone in on the data that matters.*
>
> *~Sally Vandeven*
> *Faculty Research Advisor*

More Papers on Defense

Times Change and Your Training Data Should Too: The Effect of Training Data Recency on Twitter Classifiers
by Ryan O'Grady
Read the journal article @ bit.ly/sans_edu_3

Can the "Gorilla" Deliver? Assessing the Security of Google's New "Thread" Internet of Things (IoT) Protocol
by Ken Strayer
Read the journal article @ bit.ly/sans_edu_4

Tracking Penetration Test Activities
by Joshua Arey
Learn more @ sans.org/u/1aCK

Preventing Living Off the Land Attacks
by David Brown
Learn more @ sans.org/u/1aCP

Defend, Monitor, Detect

Creating an Active Defense Powershell Framework to Improve Security Hygiene and Posture by Kyle Snihur

Security professionals are inundated with alerts, and analysts are suffering alert fatigue with no actionable intelligence (Miliard, 2019). Poor priorities and lack of resources put enterprises at risk (Wilson, 2015). In Windows domains, PowerShell can be used to aggregate data and provide actionable reports and alerts for security professionals continuously. This paper explores the viability of creating an Active Defense PowerShell framework for small to medium-sized organizations to improve security hygiene and posture. The benefits include providing actionable alerts and emails that security professionals can quickly address. Aggregated data can also be used to identify and prioritize holes in an organization's security posture. Continue reading at sans.org/u/1aCU.

Many organizations have a continual challenge to gather accurate and current information on the assets within their Windows environments. Kyle created an expandable PowerShell framework that enables the user to collect and report on a wide variety of relevant information, from running processes to installed software. Security professionals can leverage this information for threat hunting, vulnerability management, and general security hygiene.

~Jonathan Risto
Faculty Research Advisor

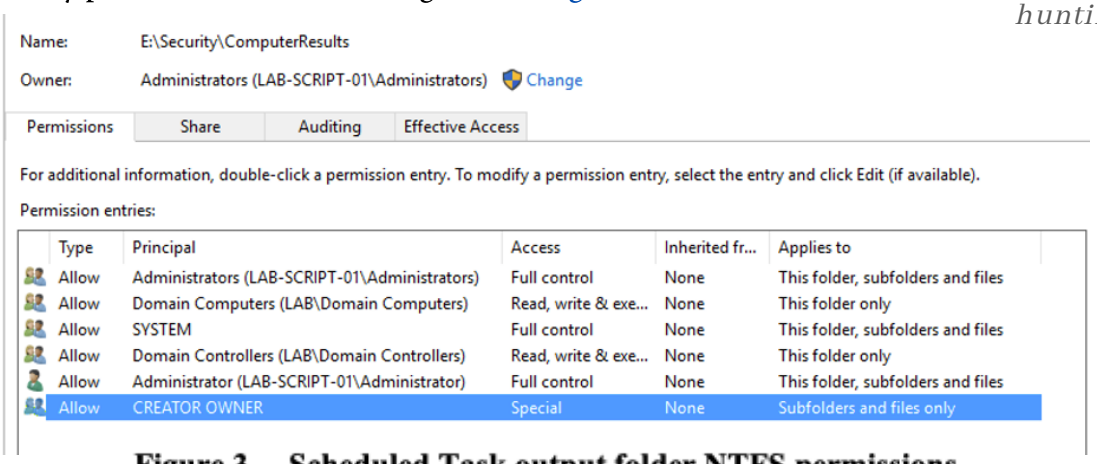


Figure 3. – Scheduled Task output folder NTFS permissions

More Papers on Defense

Continuous Monitoring Effectiveness Against Detecting Insider Threat
by Steven Austin

Learn more @ sans.org/u/1aDX

Defense in Depth: Can Geolocation Help Prevent Tax Fraud?
by Jon Glas

Learn more @ sans.org/u/1aCF

Dealing with DoH: Methods to Increase DNS Visibility as DoH Gains Traction
by Scott Fether

Learn more @ sans.org/u/1aDe

Detection of Malicious Documents Utilizing XMP Identifiers
by Joe Smith

Learn more @ sans.org/u/1aDD

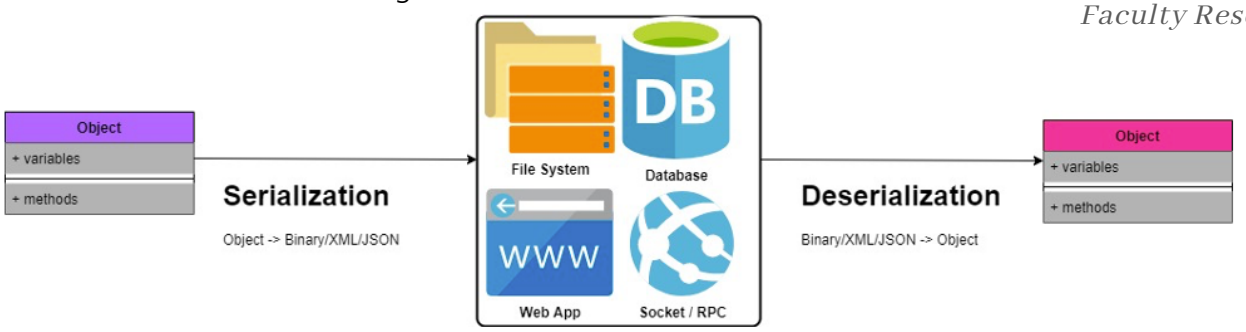
Fear of the Unknown: A Meta-Analysis of Insecure Object Deserialization Vulnerabilities

by Karim Lalji

Deserialization vulnerabilities have gained significant traction in the past few years, resulting in this category of weakness taking eighth place on the OWASP Top 10. Despite the severity, deserialization vulnerabilities tend to be among the less popular application exploits discussed (Bekerman, 2020) and frequently misunderstood by security consultants and penetration testers without a development background. This knowledge discrepancy leaves adversaries with an advantage and security professionals with a disadvantage. This research will aim to demonstrate exploitation techniques using insecure deserialization on multiple platforms, including Java, .NET, PHP, and Android, to obtain a meta-analysis of exploitation techniques and defensive strategies. Continue reading at sans.org/u/1aDS.

"Web Applications can pose a large risk to organizations. Ensuring that a company understands the key vulnerabilities that can exist in web applications is critical for vulnerability and risk management. Karim's research does an excellent job of explaining one of these key vulnerabilities -'Insecure Object Deserialization' vulnerabilities. Karim demystifies these often-misunderstood vulnerabilities.
~Tanya Baccam
Faculty Research Advisor

Figure 1: A basic use case for serialization



Listen to the podcast @ bit.ly/sans_edu_5

Watch the webinar @ sans.org/u/1aOh

More Papers on Defense

Open-Source Endpoint Detection and Response with CIS Benchmarks, Osquery, Elastic Stack, and TheHive
by Christopher Hurless

Learn more @ sans.org/u/1aFa

Listen to the podcast @ bit.ly/sans_edu_7

Securing the Soft Underbelly of a Supercomputer with BPF Probes
by William Wilson

Learn more @ sans.org/u/1aDo

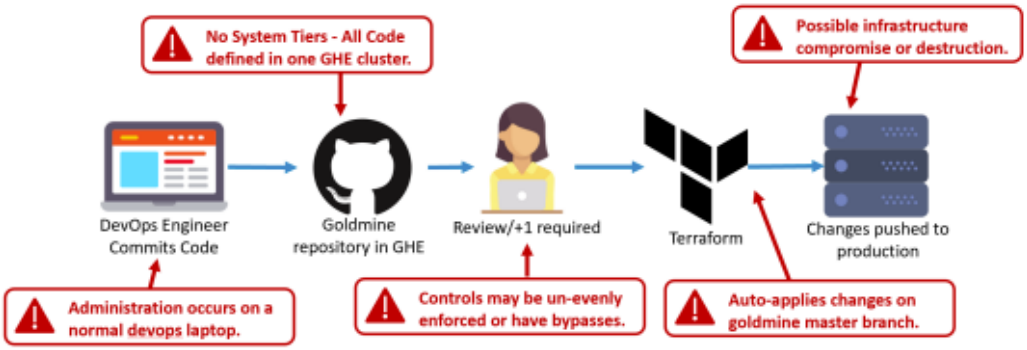
Recognizing Suspicious Network Connections with Python
by Gregory Melton

Learn more @ sans.org/u/1aDt

Defending Infrastructure as Code in GitHub Enterprise by Dane Stuckey

As infrastructure workloads have changed, cloud workflows have been adopted, and elastic provisioning and de-provisioning have become standard, manual processes. As a result, semi-automated infrastructure management workflows have proven insufficient. One of the most widely implemented solutions to these problems has been the adoption of declarative infrastructure as code, a philosophy and set of tools which use machine-readable files that declare the desired state of infrastructure. Unfortunately, infrastructure as code has introduced new attack surfaces and techniques that traditional network defense controls may not adequately cover or account for. This paper examines a common deployment of infrastructure as code via GitHub Enterprise and HashiCorp Terraform, explores an attack scenario, examines attacker tradecraft within the context of the MITRE ATT&CK® framework, and makes recommendations for defensive controls and intrusion detection techniques. Continue reading at sans.org/u/1aCA.

Figure 8 – Security Considerations for Goldmine Infrastructure Workflows.



"Dane's paper does a great job by not just telling you what to do, but also why you should do it. Infrastructure as code is an important concept to manage modern cloud-based workloads. Dane's paper is a great summary of the different controls that you have available to mitigate associated risks, and which attacks they prevent.
~Johannes Ullrich, Faculty Research Advisor

More Papers on Defense

Efficacy of UNIX HIDS
by Janusz Pazgier

Learn more @ sans.org/u/1aD9

Evaluating Open-Source HIDS with Persistence Tactic of MITRE ATT&CK®
by Jon Chandler

Learn more @ sans.org/u/1aCZ

Learning from Learning: Detecting Account Takeovers by Identifying Forgetful Users
by Sean McElroy

Learn more @ sans.org/u/1aE2

Methods to Employ Zeek in Detecting MITRE ATT&CK® Techniques
by Michael McPhee

Learn more @ sans.org/u/1aDy

Examining Sysmon's Effectiveness as an EDR Solution by Christian Vrescak

While Endpoint Detection & Response (EDR) tools are a difference-maker for defenders, the cost of commercial offerings can put them out of reach for many organizations (Infocyte, 2020). Microsoft Sysinternals Sysmon, a free EDR tool, collects detailed information about system activity, including process creations, network connections, file creations, and much more (Russinovich, M. & Garnier, T., 2020). This paper examines the effectiveness of Sysmon as a free EDR tool in providing sufficient visibility into Windows endpoint activity to detect and forensicate attacker techniques such as those listed in MITRE's ATT&CK® knowledge base. Continue reading at sans.org/u/1aEV.

"Christian's research showed that it's possible to detect malicious activities on endpoints even if the company's security budget cannot accommodate a commercial Endpoint Detection and Response (EDR) tool. Christian examined the ability of the free Microsoft Sysmon tool to offer visibility into the suspicious activities on the system, assessing the tool's effectiveness using the MITRE ATT&CK® framework.

~Lenny Zeltser
Faculty Research Advisor

4	Privilege Escalation	T1088	Bypass User Account Control	T1088-2	PowerShell code to bypass User Account Control using Event Viewer and a relevant Windows Registry modification. Upon execution, a command prompt should be launched with administrative privileges.	Detected
5	Defense Evasion	T1107	File Deletion	T1107-6	Delete a single file from the temporary directory using PowerShell.	Not Detected
6	Credential Access	T1003	Credential Dumping	T1003-1	Dumps credentials from memory via PowerShell by invoking a remote mimikatz script.	Detected
7	Discovery	T1135	Network Share Discovery	T1135-3	Network Share Discovery utilizing PowerShell. Upon execution, available network shares will be displayed in the PowerShell session.	Detected

Table 3. Simulated Attack Chain Test Results Matrix

More Papers on Defense

QUIC & The Dead: Which of the Most Common IDS/IPS Tools Can Best Identify QUIC Traffic?
by Lehlan Decker
Learn more @ sans.org/u/1aD4

Natural Language Processing for the Security Analyst
by Daniel Severance
Learn more @ sans.org/u/1aDj

No Strings on Me: Linux and Ransomware
by Richard Horne
Learn more @ sans.org/u/1aDI

Mitigating Attacks on a Supercomputer with KRSI
by Billy Wilson
Listen to the podcast @ bit.ly/sans_edu_6
Learn more @ sans.org/u/1aE7

Replacing WINS in an Open Environment with Policy Managed DNS Servers
by Mark Lucas

In some environments, Windows workstations require placement on the open internet. In order to protect the read-write domain controllers, administrators locate them in a protected enclave behind a firewall, and read-only domain controllers authenticate workstations during day-to-day operations. While this is strong protection for the read-write domain controllers, the configuration breaks the standard dynamic DNS registration of Windows workstations with the read-write domain controller. In our environment, we have maintained WINS servers linked to Windows DNS via the WINS lookup function to continue finding workstations by name. The TechNet page on WINS (Davies, 2011) was last updated almost nine years ago, and Microsoft has been actively encouraging the abandonment of WINS (Ross & Mcillece, 2020). This paper explores Windows DNS Policies to replacing WINS with Dynamic DNS and policy-controlled responses to queries. Utilizing source IP addresses, DNS policies can regulate the provided answers. The operability of DNS Policies and the applicability to this solution is evaluated in depth. Continue reading at sans.org/u/1aFT.

Name	Type	Data
(Default)	REG_SZ	(value not set)
Action	REG_DWORD	0x00000001 (1)
AppliesOn	REG_DWORD	0x00000000 (0)
ClientSubnet	REG_SZ	eq,PublicSubnet2
Condition	REG_DWORD	0x00000000 (0)
Content	REG_SZ	1,InstitutePublicScope
IsEnabled	REG_DWORD	0x00000001 (1)
ProcessingOrder	REG_DWORD	0x00000002 (2)

Figure 2 InstitutePublicResolutionPolicy Registry Entry

“There are some environments where Windows workstations require placement on the open internet. However, there are challenges with typical deployment and standard dynamic DNS registration for Windows workstations and the read-write domain controllers. Mark takes the opportunity to explore Windows DNS Policies to replace WINS with Dynamic DNS and policy-controlled responses to queries.
~Tanya Baccam
Faculty Research Advisor

Listen to the podcast @ bit.ly/sans_edu_15

More Papers in Leadership

Evaluation of Comprehensive Taxonomies for Information Technology Threats
by Steve Launius

Read the article @ bit.ly/sans_edu_2

Answering the Unanswerable Question: How Secure Are We?
by Jason Bohreer

Learn more @ sans.org/u/1aFE

Benefits and Adoption Rate of TLS 1.3
by Ben Weber

Learn more @ sans.org/u/1aFJ

Risk Management with Automated Feature Analysis of Software Components

by Steven Launius

Organizations developing software need pragmatic risk management practices to prevent malicious code from contaminating their software. Traditional security tools for Static Code Analysis identify vulnerabilities, not the presence of backdoors exhibiting unintended actions. Application Inspector is a Microsoft tool released to the open source community that identifies risky features and characteristics of source code libraries. This research will evaluate the accuracy of feature detection in the Application Inspector tool and construct a risk model for automating decisions based on feature analysis of source code. Continue reading at sans.org/u/1aFO.

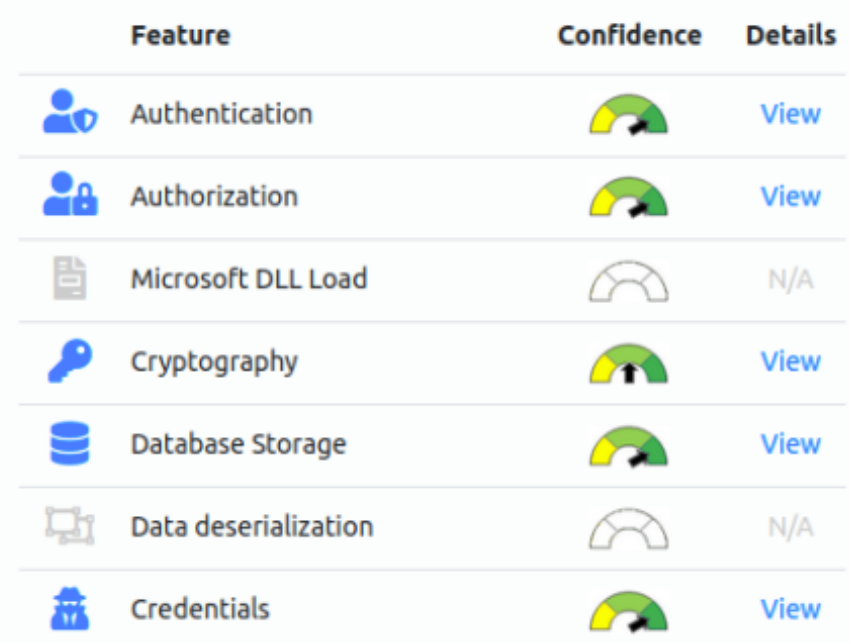


Figure 3. Sample HTML Report of Features in the Credential Dumping Threat Model.

"We always tell our administrators to "know their systems," but this concept should also apply to enterprise software development. Understanding the behaviors and features of software and being able to detect when capabilities change are critical to ensuring the integrity of the software over time. In this paper Steve tests whether the Application Inspector tool from Microsoft can be used to perform this detection. He also introduces techniques for using the tool to conduct software risk assessments.

~Clay Risenhoover
Faculty Research Advisor

More Papers in Leadership

Security Network Auditing: Can Zero-Trust Be Achieved?
by Carl Garrett
Learn more @ sans.org/u/1aFY

Defeat the Dread of Adopting DMARC: Protect Domains from Unauthorized Email
by Tim Lansing
Learn more @ sans.org/u/1aG8

Architecture and Configuration for Hardened SSH Keys
by Scott Ross
Learn more @ sans.org/u/1aG3

Detecting System Log Loss Through One-Way Communication Channels
by Jason Leverton
Learn more @ sans.org/u/1aGd

Real-Time Honeypot Forensic Investigation on a German Organized Crime Network by Karim Lalji

German police raided a military-grade NATO bunker in the fall of 2019, believed to have been associated with a dark web hosting operation supporting a variety of cybercrimes. The organized crime group has gone by the aliases of CyberBunker, ZYZtm, and Calibour (Dannewitz, 2019). While most of the group's assets were seized during the initial raid, the IP address space remained and was later sold to Legaco Networks. Before being shut down, Legaco Networks temporarily redirected the traffic to the SANS Internet Storm Center honeypots for examination. The intention behind this examination was to identify malicious traffic patterns or evidence of illegal activity to assist the information security community in understanding the techniques of a known adversary. Analysis of the network traffic revealed substantial residual botnet activity, phishing sites, ad networks, pornography, and evidence of potential Denial of Service (DoS) attacks. The investigation uncovered a possible instance of Gaudox Malware, IRC botnets, and a wide variety of reconnaissance activities related to Mirai variant IoT exploits. A survey of the network activity has been provided with an emphasis on potential botnet activity and Command and Control (C&C) communication. Continue reading at sans.org/u/1aEL.

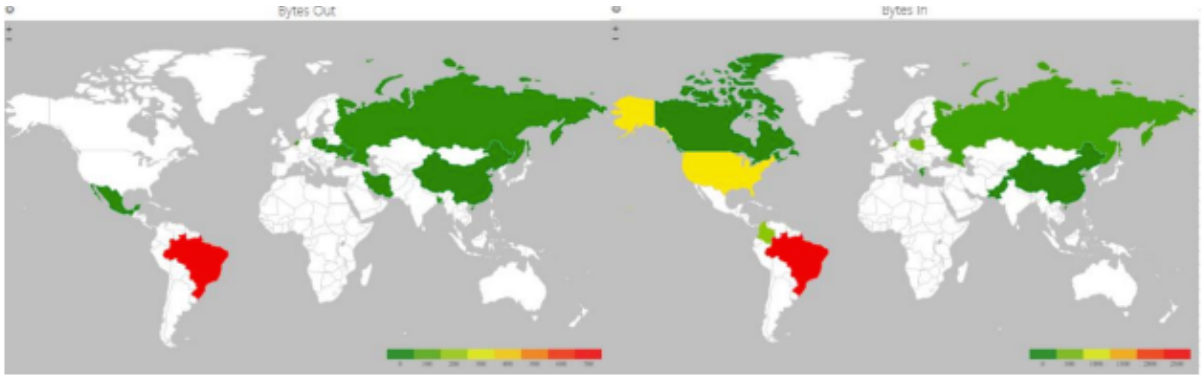


Figure 2 (Global Traffic Heatmap)

"Karim had the unique opportunity to obtain access to the IP address space of a criminal operation ("Cyberbunker") a few months after the group was taken down. The analysis of the traffic gave a unique insight into the activities of the group, and how even a few months later, infected machines and other activity still reached out to the network.
~Johannes Ullrich, Faculty Research Advisor

Read the article @ bit.ly/sans_edu_8

Listen to the podcast @ bit.ly/sans_edu_9

Forensics, Threat Hunting, Incident Response

Verifying Universal Windows Platform (UWP) Signatures at Scale by Joal Mendonsa

Enterprise security teams often use native Windows tools, like PowerShell, to check signatures and quickly establish where a binary is a known-good or is unknown and worthy of further investigation. Unfortunately, a new and growing class of applications – Universal Windows Platform (UWP) applications – incorrectly appear to be unsigned when checked using traditional methods. This paper will demonstrate a way to efficiently validate UWP applications in a networked environment, strictly using Microsoft tools, and without placing additional binaries on remote systems. Continue reading at sans.org/u/1aFf.

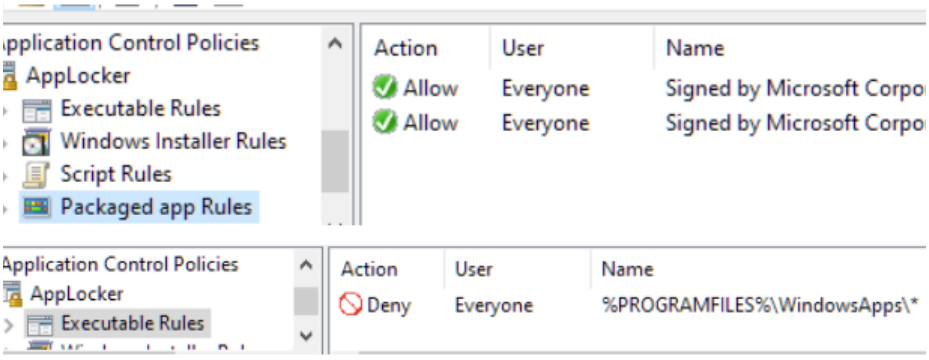


Figure 5-1: Malware blends into "unsigned" binaries

Watch the webinar @ sans.org/u/1aOc

When it comes to incident response and the subsequent investigation of a potentially compromised system, the ability to exclude executables based upon a known, trusted, and validated digital signature can significantly aid in the narrowing down of which executables need to be investigated. The only problem is that there can be a deviation in how executables are digitally signed, in particular as it relates to different operating systems. In a Microsoft Windows environment, while Microsoft digitally signs a large portion of their executables, it turns out there is a difference in how 'regular' executables are signed when compared to Universal Windows Platform (UWP) executables. Joal took on the challenge of determining how to verify UWP signatures, at scale, across a Windows environment; this paper will greatly add to the arsenal of capability that any incident responder must possess when it comes to working with Windows machines.

~Bryan Simon
Faculty Research Advisor

More Papers in Forensics

Mission Implausible: Defeating Plausible Deniability with Digital Forensics
by Michael E. Smith
Learn more @ sans.org/u/1aEw

The All-Seeing Eye of Sauron: A PowerShell Tool for Data Collection and Threat Hunting
by Timothy Hoffman
Learn more @ sans.org/u/1aF5

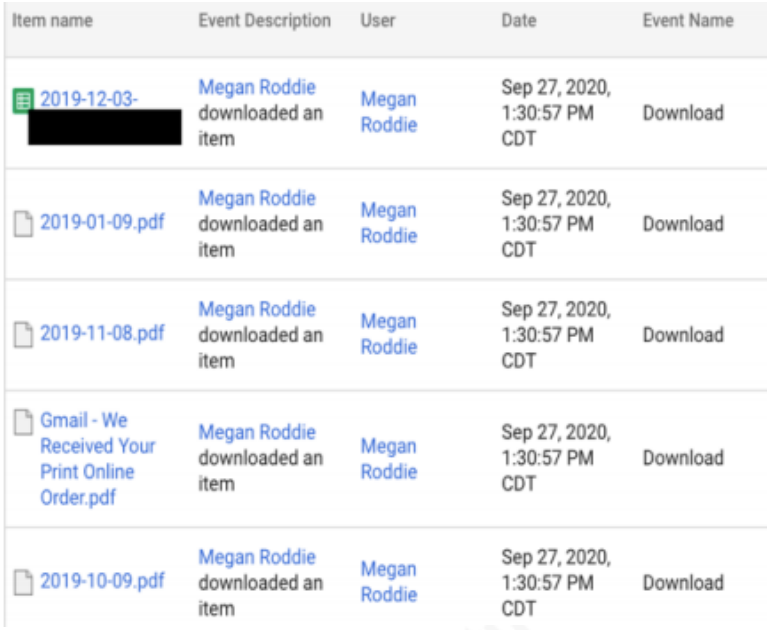
You've Had the Power All Along: Process Forensics with Native Tools
by Trevor McAfee
Learn more @ sans.org/u/1aEQ

Quantifying Threat Actor Assessments
by Andy Piazza
Learn more @ sans.org/u/1aEB
Listen to the podcast @ bit.ly/sans_edu_10

Forensics, Threat Hunting, Incident Response

Automating Google Workspace Incident Response by Megan Roddie

Incident responders require a toolset and resources that allow them to efficiently investigate malicious activity. In the case of Google Workspace, there are an increasing number of subscribers, but resources to assist in the analysis of security incidents are lacking. The goal of this research is to develop a tool that expands on Google's default administrative capabilities with the intent of providing value to incident responders. Through providing both additional context and purposeful views, incident responders can more quickly identify malicious activity and respond accordingly. Continue reading at sans.org/u/1aFp.



Item name	Event Description	User	Date	Event Name
2019-12-03-[redacted]	Megan Roddie downloaded an item	Megan Roddie	Sep 27, 2020, 1:30:57 PM CDT	Download
2019-01-09.pdf	Megan Roddie downloaded an item	Megan Roddie	Sep 27, 2020, 1:30:57 PM CDT	Download
2019-11-08.pdf	Megan Roddie downloaded an item	Megan Roddie	Sep 27, 2020, 1:30:57 PM CDT	Download
Gmail - We Received Your Print Online Order.pdf	Megan Roddie downloaded an item	Megan Roddie	Sep 27, 2020, 1:30:57 PM CDT	Download
2019-10-09.pdf	Megan Roddie downloaded an item	Megan Roddie	Sep 27, 2020, 1:30:57 PM CDT	Download

Figure 6. Google Workspace Audit Logs - Drive

"Cloud computing offers great benefits to large enterprises and small organizations, alike. Unfortunately, one aspect of cloud that could impact any organization, regardless of its size, is its ability (or inability) to perform incident response. In this paper Megan takes on the challenge of determining if incident response could be made more automated, regardless of the licensing an organization pursues, specifically as it pertains to Google's Workspace offerings. Step by step, Megan works through the methodology of incident response, all while tying in the logging information made available natively within Google's offering. In order for the community at large to benefit from the work, Megan focused on the least expensive licensing option for Google Workspace, at the same time building a toolset that can better ingest the relevant data to make it more focused for the incident responder. This paper is an absolute must-read.

~Bryan Simon
Faculty Research Advisor

More Papers in Forensics

Reverse Engineering Virtual Machine File System 6 (VMFS 6)
by Michael E. Smith
Learn more @ sans.org/u/1aFk

Is it Ever Really Gone? The Impact of Private Browsing and Anti-Forensic Tools
by Rick Shroeder
Learn more @ sans.org/u/1aFu

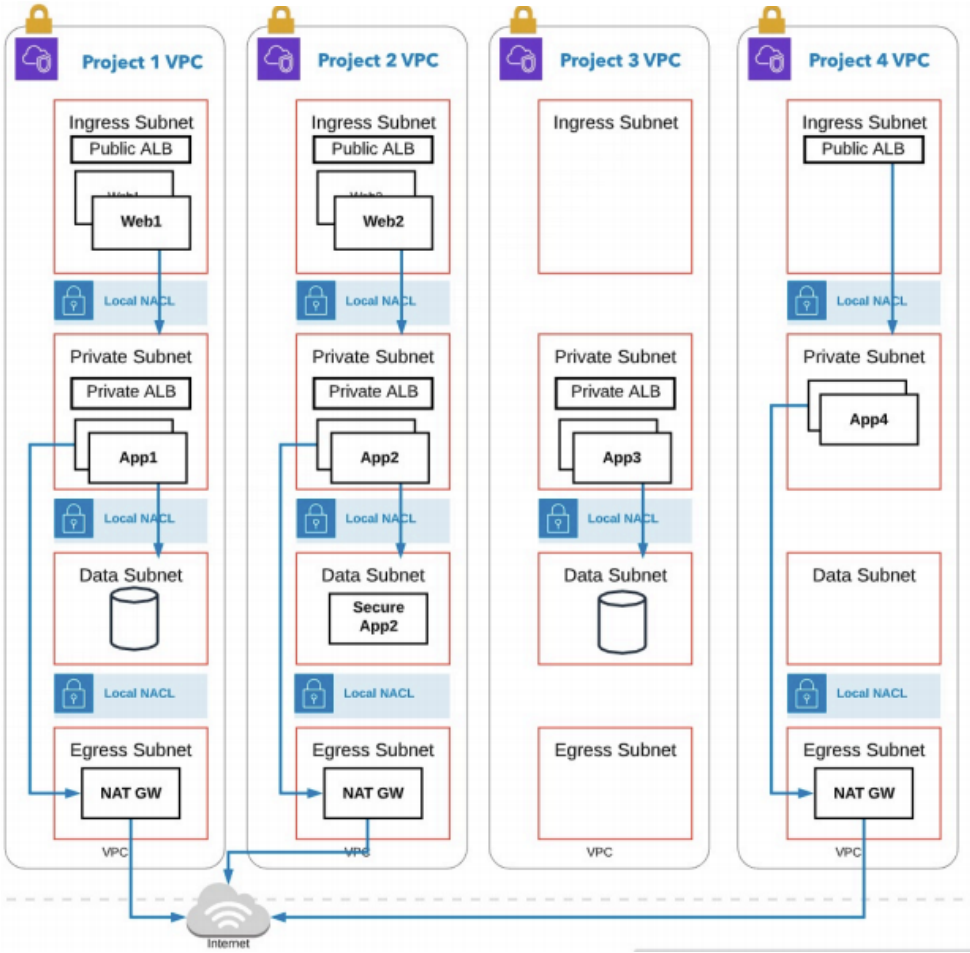
Incident Response in a Zero-Trust World
by Heath Lawson
Learn more @ sans.org/u/1aEr

Ubuntu Artifacts Generated by the Gnome Desktop Environment
by Brian Nishida
Learn more @ sans.org/u/1aFz
Listen to the podcast @ bit.ly/sans_edu_11

Lateral traffic movement in Virtual Private Clouds by Andy Huang

Cloud vendors have introduced virtual private cloud (VPC) structures to bring the benefits of private cloud into the public cloud. These structures provide vertical segmentation and isolation for application projects implemented within them. However, the security context needs to be considered as applications communicate with one another between VPCs using technologies such as peering and privatelinks. Applications are usually highly dependent on each other for data and functionality, leading to cross-connections between VPC structures. The implications between different connection setups need to be vetted to ensure that access is not overly permissive, thus leading to possible lateral movement of traffic. Continue reading at sans.org/u/1aBW.

Figure 2: Complete independent project structures within several isolated VPCs.



"Least privilege principles are often either overlooked or poorly implemented in cloud environments, leaving a real risk of unauthorized access to sensitive data. In this paper, Andy explores application communication architectures and cloud service network configuration options which can mitigate this risk. He compares horizontal and vertical communication stacks and discusses models for permitting appropriate communications between virtual private clouds and give techniques for tracing the access being allowed.
~Clay Risenhoover, Faculty Research Advisor

More Papers in Cloud

ATT&CK-Based Live Response for GCP CentOS Instances
by Allen Cox

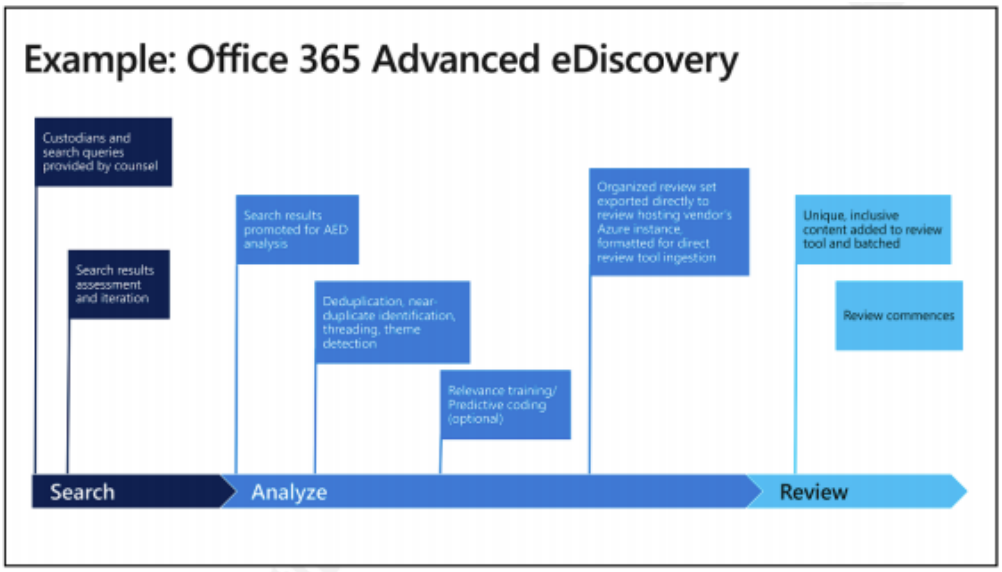
Learn more @ sans.org/u/1aC6

Shall We Play a Game? Analyzing the Security of Cloud Gaming Services
by Adam Knepprath

Learn more @ sans.org/u/1aCl

The Poisoned Postman:Detecting Manipulation of Compliance Features in a Microsoft Exchange Online Environment by Rebel Powell

Modern attack techniques frequently target valuable information stored on enterprise communications systems, including those hosted in cloud environments. Adversaries often look for ways to abuse tools and features in such systems to avoid introducing malicious software, which could alert defenders to their presence (Crowdstrike, 2020). While on-premise detection strategies have evolved to address this threat, cloud-based detection has not yet matched the adoption pace of cloud-based services (MITRE, 2020). This research examines how adversaries can perform feature attacks on organizations that use Microsoft Office 365's Exchange Online by exploring recent advanced persistent threat tactics in Exchange on-premise environments and applying variations of them to Exchange Online's Compliance and Discovery features. It also analyzes detection strategies and mitigations that businesses can apply to their systems to prevent such attacks. Continue reading at sans.org/u/1aCg.



“Modern attackers often look for ways to abuse built-in features and tools to achieve their objectives to evade detection. Rebel investigated one such approach to attacking Exchange Online. Rebel shared practical advice for defending against such attacks by also using built-in capabilities, helping IT and security administrators improve their security posture without spending additional money.

~Lenny Zeltser, Faculty Research Advisor

More Papers in Cloud

Ebb and Flow: Network Flow Logging as a Staple of Public Cloud Visibility or a Waning Imperative?
by Dennis Taggart

Learn more @ sans.org/u/1aC1
Listen to the podcast @ bit.ly/sans_edu_13

Improving Analyst Efficiency in Office365 Business Email Compromise Investigation Scenarios Through the Implementation of Open Source Tools
by Aaron Elyard

Learn more @ sans.org/u/1aEG
Listen to the podcast @ bit.ly/sans_edu_12

Detecting and Preventing the Top AWS Database Security Risks by Gavin Grisamore

Engineers regularly perform risky actions while deploying and operating databases on cloud services like AWS. Engineers are often focused on delivering value to customers and less on the security of the cloud infrastructure. Security teams are increasingly concerned with identifying these cloud-native risks and putting migrations in place to secure their critical data and limit exposure without inhibiting development workflows or velocity. This paper examines several common AWS database security risks and addresses how to implement detection and prevention controls to mitigate the risks. Continue reading at sans.org/u/1aCv.

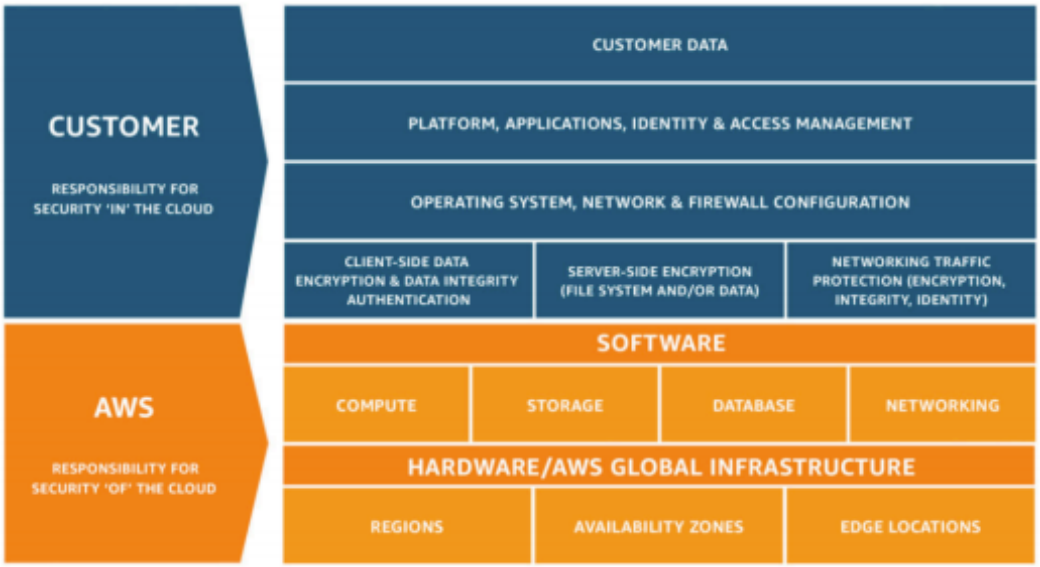


Figure 2: Complete independent project structures within several isolated VPCs.

This paper is useful because organizations are continuing to rush to migrate everything into cloud-based services without giving adequate attention to thoughtful security controls. Gavin's paper lays out a series of concrete actions and considerations that organizations would do well to analyze for new data migrations and existing cloud data deployments.

~David Hoelzer, Faculty Research Advisor

More Papers in Cloud

Prescriptive Model for Software Supply Chain Assurance in Private Cloud Environments
by Robert Wood

Learn more @ sans.org/u/1aCq

Fight or Flight: Moving Small and Medium Businesses into the Cloud During a Major Incident
by Drew Hjelm

Learn more @ sans.org/u/1aF0

Detecting Server-Side Request Forgery Attacks on Amazon Web Service
by Sean McElroy

Read the article @ bit.ly/sans_edu_1

Mitigating Risk with the CSA 12 Critical Risks for Serverless Applications
by Mishka McCowan

Learn more @ sans.org/u/1aCb

Listen to the podcast @ bit.ly/sans_edu_14

Fashion Industry (Securely) 4.0ward by Shawna Turner

The fashion market segment is going through a significant technological upgrade. The need to meet modern consumer expectations and desires requires wholesale changes in the way the fashion ecosystem has historically shared information and manufactured products. Fashion cannot use existing security guidance due to the consumer expectations that a fashion product provides a unified physical experience. The addition of significant new technology increases the risk of intellectual property loss. The fashion industry requires a list of minimum-security controls that address the entire ecosystem of fashion from the fashion houses to the supply chain to the factory floor to address information security concerns. This paper begins the process of developing a minimum viable list of controls by combining controls from the Purdue model with recommended controls from the Verizon 2019 Data Breach Investigation Report (DBIR). The paper focuses on proposed controls for the fashion sector; however, they apply to any manufacturing pivoting to Industry 4.0. Continue reading at sans.org/u/1aEh.

EXPANDED PURDUE MODEL KEY

Non Production Network(s)	This is other networks that may be connected to a production network, but where production data is not stored.
Enterprise Like Zone - L4-5	This are the zones (networks) containing traditional information technology resources (loptops, mail servers, etc.)
Manufacturing Zone AKA Control Plant Ops - L3	This is the zone where data is aggregated from the manufacturing floor to be provided to level 4 systems. Level 3 is where operators monitor floor operations.
Area Zone L1-L3	Area zones allow more granular network traffic control. This may be driven by production processes. Controls Level 0 devices.
Process / Safety Zone L0	Level 0 contains sensors and instruments that directly connect to / control manfuacturing processes.

Shawna investigated shortcomings and security challenges present in the fashion industry. Products in the industry are typically not manufactured by a single organization so control of Intellectual Property (IP) is a challenge in its shared digital form. Application of the Purdue model and Consensus Audit guidelines were investigated and adjustments presented to accommodate distributed IP management and Industrial Internet of Things (IIoT) considerations.
~David Fletcher
Faculty Research Advisor

More Papers in ICS

Vulnerabilities on the Wire: Mitigations for Insecure ICS Device Communication
by Michael Hoffman

Learn more @ sans.org/u/1aEc

Industrial Traffic Collection: Understanding the Implications of Deploying Visibility Without Impacting Production
by Daniel Behrens

Learn more @ sans.org/u/1aEm
Listen to the podcast @ bit.ly/sans_edu_16

Meet the SANS Technology Institute Faculty Research Advisors

Tanya Baccam is a SANS senior instructor and courseware author. With more than 20 years of information security experience, Tanya has consulted with a variety of clients about their security architecture in areas such as perimeter security, network infrastructure design, system audits, web server security, and database security. She has previously worked as a Manager at Deloitte, Director of Assurance Services for a security services consulting firm and the Manager of Infrastructure Security for a healthcare organization. Tanya has played an integral role in developing multiple business applications and currently holds the CPA, GIAC GCIH, GIAC GSEC, CISSP, CISM, CISA, CITP and OCP DBA certifications. Tanya completed a Bachelor of Arts degree with majors in accounting, business administration and management information systems.

Lori Cole began her career as a digital network intelligence analyst at the National Security Agency (NSA). She has also held positions as a STEM educator, Security Operations Manager, and Cyber Threat Intelligence researcher. She currently manages global cyber investigative programs at a Fortune 30 financial firm. Lori holds a BA in English and a master's degree in Educational Leadership from Chaminade University, a MS in Data Analytics from University of Maryland Global Campus, and is a PhD candidate at Monarch Business School.

Domenica "Lee" Crognale is a co-author of SANS FOR585: Advanced Smartphone Forensics. As a co-author, she has been able to share some of her challenges and experiences with students who are interested in the field, something that's been a very rewarding experience. Lee maintains multiple certifications including the GASF, EnCE, CCE, and CISSP. She is also a IACIS CFCE mentor and coach, providing mentorship to candidates enrolled in the IACIS certification process.

Russell Eubanks, owner of Security Ever After and consultant for Enclave Security, is responsible for assessing the cyber security maturity of many diverse organizations and helping them increase the maturity, while decreasing the probability of a breach. He wrote the first paper on how to implement the Critical Security Controls, "A Small Business No Budget Implementation of the SANS 20 Security Controls," and serves on the editorial panel for the Critical Security Controls. As a current handler for the SANS Internet Storm Center and former chief information security officer (CISO), he's especially passionate about helping new or aspiring cyber leaders become more effective.

David Fletcher is the network manager at Selfridge Air National Guard Base in Mount Clemens, MI. Having worked in information technology for the United States Air Force for 20 years, he has extensive experience in information technology and cyber security. Over the course of his career his roles have included network defense and intrusion analysis, network administration, database administration, and web application development. Within the Air Force he has experience supporting the legal, educational, guard/reserve, special operations, and conventional warfighting communities. David has completed a bachelor's degree in Electrical Engineering through the University of West Florida and the Master of Science in Information Security Engineering program through the SANS Technology Institute.

John Hally has had many technical roles specializing in security administration, engineering, design, and architecture in high transaction, 24/365 multi-private, hybrid, and public cloud environments. John led multiple teams dedicated to infrastructure and application security assessment, defense, and response. Additionally, John has held multiple management roles including Technical Director and Vice President of Information Security for a U.S. Top 200 privately held company. He is currently the Principal IT Security Architect for NETSCOUT Systems. John is a graduate of the SANS Technology Institute with a Master of Science in Information Security Engineering, and he also holds the GIAC GPEN, GCIH, GCIA, GCFA, GCWN, GMON, and GSEC certifications.

David Hoelzer is a SANS instructor and course author who has trained security professionals from organizations including NSA, DHHS, Fortune 500 security engineers and managers, various Department of Defense sites, national laboratories, and many colleges and universities. Outside of SANS, David is a research fellow in the Center for Cybermedia Research, a research fellow for the Identity Theft and Financial Fraud Research Operations Center (ITFF/ROC), an adjunct research associate of the UNLV Cybermedia Research Lab, a research fellow with the Internet Forensics Lab, and an adjunct lecturer in the UNLV School of Informatics. David has written and contributed to more than 15 peer reviewed books, publications, and journal articles. David holds a BS in IT and an MS in Computer Science.

Michael Long is a Principal Cyber Adversarial Engineer with the MITRE Corporation and a former U.S. Army Cyber Operations Specialist. Michael has over 12 years of experience in information security disciplines including adversary threat emulation, red teaming, and threat hunting. Michael has served on countless cyber operations for organizations including the Army Cyber Protection Brigade and Army Cyber Command, the results of which he regularly briefed to commanding generals, strategic executives, and congressional staffers. Michael earned a Master of Science in Information Security Engineering from the SANS Technology Institute, and holds many information security certifications including the prestigious GIAC Security Expert certification (GSE).

Dr. Tim Proffitt is a cybersecurity leader and published author with over 28 years of experience in the technology field. Dr. Tim has earned over 25 industry certifications and has experience in all manner of technology security, infrastructure, forensics, compliance, risk management, and security awareness. Dr Tim's current research interest focuses on disaster recovery, malicious insiders, and digital forensics. Dr. Tim is a graduate of the SANS Technology Institute's Master of Science in Information Security Management program. His hobbies include restoring cars from the 1970s, playing golf and SCUBA diving.

Clay Risenhoover is the president of Risenhoover Consulting, Inc., an IT management consulting firm based in Durant, Oklahoma. Founded in 2003, RCI provides IT audit and IT management consulting services to clients in multiple sectors. Clay's past experience includes positions in software development, technical training, LAN and WAN operations, and IT management in both the private and public sector. He has a master's degree in computer science and holds a number of technical and security certifications, including GPEN, GSNA, CISA, CISM, GWEB and CISSP.

Jonathan Risto is a SANS Instructor and co-author. With a career spanning over 20 years that has included working in network design, IP telephony, service development, security and project management, he has a deep technical background that provides a wealth of information he draws upon when teaching. When not teaching for SANS, he primarily works for the Canadian Government performing cyber security research work, in the areas of vulnerability management and automated remediation. Jonathan holds a bachelor's degree in Electrical Engineering, and is a licensed professional Engineer (P.Eng.). He also earned a Master of Science in Information Security Management from the SANS Technology Institute.

Bryan Simon is an internationally recognized expert in cybersecurity and has been working in the information technology and security field since 1991. Over the course of his career, Bryan has held various technical and managerial positions in the education, environmental, accounting, and financial services sectors. Bryan speaks on a regular basis at international conferences and with the press on matters of cybersecurity. He has instructed individuals from organizations such as the FBI, NATO, and the UN in matters of cybersecurity, on three continents. He has received recognition for his work in IT Security, and was profiled by McAfee (part of Intel Security) as an IT Hero. Bryan holds 13 GIAC Certifications including GSEC, GCWN, GCIH, GCFA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, GCUX, GISF, and GMON.

Dr. Johannes Ullrich is currently responsible for the SANS Internet Storm Center (ISC) and the GIAC Gold program. In 2000, he founded DShield.org, which is now the data collection engine behind the ISC. His work with the ISC has been widely recognized, and in 2004, Network World named him one of the 50 most powerful people in the networking industry. Prior to working for SANS, Johannes worked as a lead support engineer for a web development company and as a research physicist. Johannes holds a PhD in physics from SUNY Albany and is based in Jacksonville, Florida. His daily podcast summarizes current security news in a concise format.

Sally Vandeven began her career in the tech arena many years ago as a Fortran application developer. She has also held positions as help desk technician, Linux sysadmin, security analyst and forensic analyst. She is currently a penetration tester at Black Hills Information Security. In addition, Sally has taught computer security courses at a local community college. Sally earned a BS in economics from the University of Michigan and a Master of Science in Information Security Engineering from the SANS Technology Institute.

Lenny Zeltser develops teams, products, and programs that use security to achieve business results. He is the CISO at Axonius and Faculty Fellow at SANS Institute. Over the past two decades, Lenny has been leading efforts to establish resilient security practices and solve hard security problems. As a respected author and speaker, he has been advancing tradecraft and contributing to the community. His insights build upon 20 years of experiences, a CS degree from the University of Pennsylvania, and an MBA degree from MIT Sloan.

SANS TECHNOLOGY INSTITUTE

Cybersecurity is all we teach - and nobody does it better.

All Programs Offer

- Flexible Study Options
- Industry Recognized GIAC Certifications
- World-Class Faculty
- A Powerful Network
- Funding Options Including Veterans' Benefits

"SANS is the Oxford of security studies, so expectations are naturally quite high. Living up to those is not a trivial accomplishment!"

Shawna Turner
Principal Solutions Architect
Nike

Start.

Prepare to launch a cybersecurity career with an undergraduate program in Applied Cybersecurity. The undergraduate certificate and bachelor's degree programs are designed for college students and career changers.

Advance.

Strengthen technical knowledge and job-specific skills with a graduate certificate program. These programs are designed for working InfoSec professionals who are looking to sharpen their skills in a specific area such as Penetration Testing, Purple Teams, or Cloud Security. See the full list of options here.

Lead.

Join the next generation of cybersecurity leaders with our master's degree. This 36-credit program includes 9 GIAC certifications, real-world leadership practicums, and an optional focus area. Alumni of this program serve in leadership positions in Fortune 500 companies, military and government organizations, and leading cybersecurity firms.