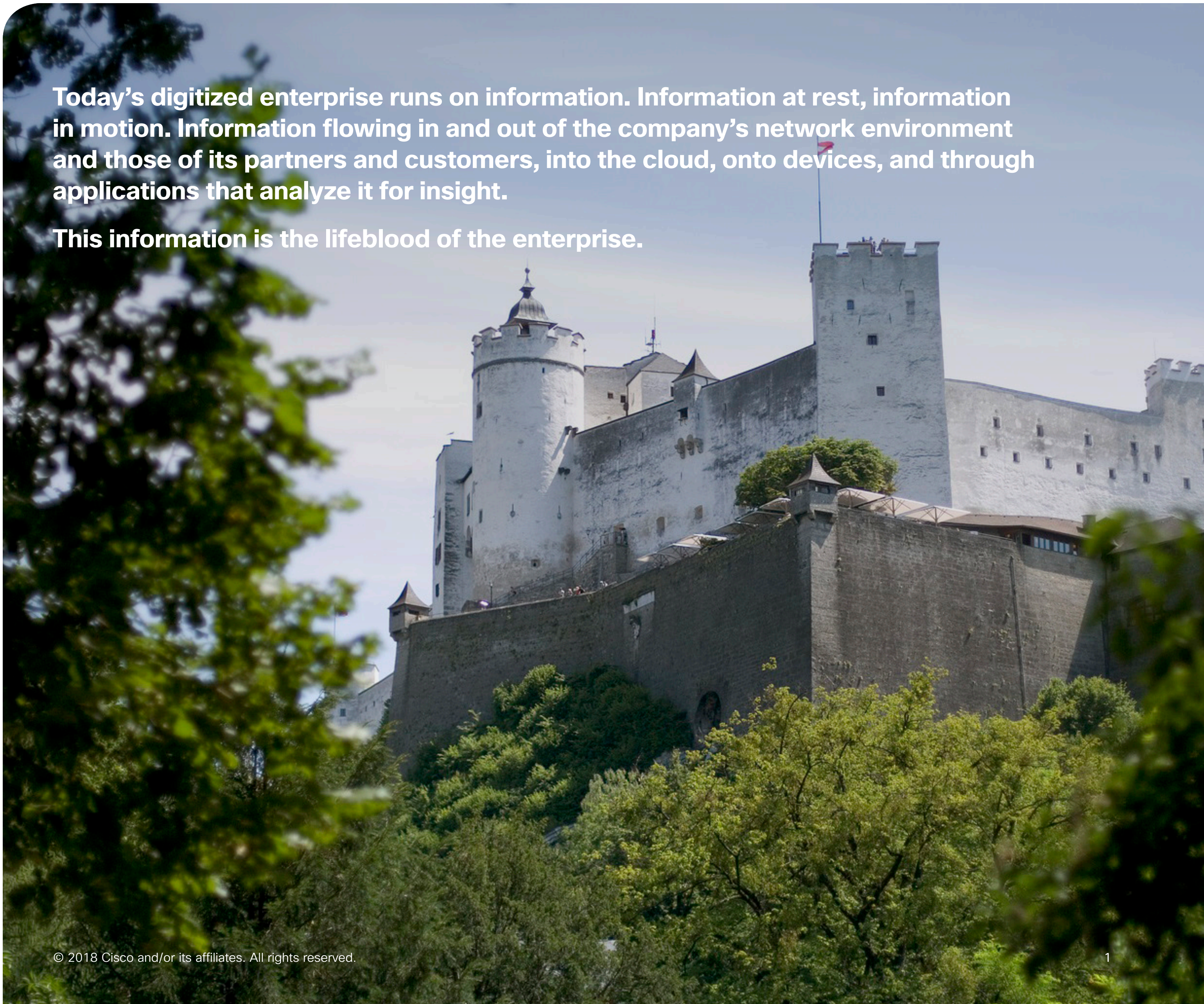
White paper
Cisco Public

Cybersecurity Operations: How to Secure the Digitized Enterprise



Today's digitized enterprise runs on information. Information at rest, information in motion. Information flowing in and out of the company's network environment and those of its partners and customers, into the cloud, onto devices, and through applications that analyze it for insight.

This information is the lifeblood of the enterprise.

We live in a world where change is a constant and the speed of change is accelerating. Companies that can leverage digital technologies to accommodate rapid change succeed. Organizations that can't evolve will fall behind.

Whether information is stored or on the move, it has become a prime target for those with malicious intent. As the threat landscape expands, the need for new skills to address vulnerabilities, respond to breaches, and reduce risk is all-important.

In response, IT departments have set up security operations centers (SOCs), staffed by professionals with a variety of skills and experience. One of the central roles in SOCs is played by security analysts. They monitor IT security systems. They detect and address cyberattacks, insider threats, vulnerabilities, and honest errors. They gather and analyze evidence. They compare, categorize, and correlate information. They direct the center's responses to a wide variety of cybersecurity events.

To be successful, SOCs need experts. For these experts to be successful, they need skills. And we can help.

This white paper outlines the trends in digitization that make it critical to have SOCs staffed with cybersecurity operations experts. It describes the skills needed for cybersecurity success. It also details Cisco's training and certifications for the critical security analyst role. Specific topics covered include these:

- How good cybersecurity practices enable enterprises to protect themselves and foster trust
- SOCs as cornerstones of good cybersecurity programs
- The disturbing state of enterprise cybersecurity event preparedness
- The severe shortage of skilled cybersecurity professionals
- New levels of skill required for securing digital enterprises
- A day in the life of a cybersecurity professional
- Cisco's expansion of security certifications to help close the skills gap

Benefits of good cybersecurity practices

We live in a world where change is a constant and the speed of change is accelerating. Companies that can leverage digital technologies to accommodate rapid change succeed. Organizations that can't evolve will fall behind.

Going digital affects all parts of the organization. Back-office processes, interactions with employees, customers, partners, everything. And the rate of digital adoption is growing.

According to a recent Harvard Business Review survey of 150 large U.S. companies, digitization makes a big difference.[1] Researchers found that "digital leaders" outperform competitors by roughly 10 percent, with the gap between leaders and laggards getting larger.

[1] Manyika, James, et al., Harvard Business Review, "The Most Digital Companies Are Leaving All the Rest Behind," January 2016.

All digital economy stakeholders need to consider how linked assets and processes make a new level of trust necessary.

Digitization is bringing change that is as much revolution as evolution. Mobility, big data, the cloud, collaboration, and the Internet of Things (IoT) are coming together. They are profoundly shifting how organizations operate, how markets are being disrupted, and how countries are growing their economies.

According to the Cisco Global Cloud Index: Forecast and Methodology, 2015-2020, for every single piece of information created or entered by a person, there will be 277 pieces of information automatically created by a machine. Information will be formed at a rate far greater than previously possible, and in much greater volumes. Information created by machines is shared far and wide by networks that connect millions of people, devices, and sensors.

Automated analytics takes that far-flung information and wrings fresh insights from it. The fact that the network is the platform for sharing and analyzing this information makes securing it increasingly important.

That need—to keep expanding networks secure—merits special attention. Digitization is now the way that enterprises operate, grow, and succeed. But digitization also gives bad actors many more ways to disrupt operations and damage trust. The risks and rewards are huge for all. This makes cybersecurity operations a major, if not the dominant, part of overall enterprise risk management.

All digital economy stakeholders need to consider how linked assets and processes make a new level of trust necessary.

The need for trusted transactions across the Internet was created with the advent of e-commerce. Now, trust needs to be embedded in all of the pieces of a digital organization and along the entire chain of transactions, including people, machines, networks, sensors, analytics, applications, information, and controls.

Without trust, a digital organization cannot survive. Efforts to create and ensure trust should be comprehensive in scale and scope.

Everyone needs to be able to trust the systems that manage and process information. They must also be able to trust the people who access, create, and use information. And the systems and controls, and the fundamental technologies and processes that protect that information.

We intuitively know the value of trust. But trust is hard to create, easily broken, and difficult to restore once it is broken.

The impact of broken trust is also magnified in today's high-speed digital economies. Millions of customer records, or an organization's intellectual property, or even critical resources can be compromised with unprecedented speed and stealth.

Ensuring trust is why SOCs are necessities. This is true whether the SOC is internal or is provided by a third party, such as a managed security service provider (MSSP).

Digital technologies provide companies and countries with ongoing advantages. Yet for long-term success, security and trust must be embedded in all parts of the digitized organization, and they must be end-to-end. Trust must become part of enterprise DNA.

SOCs as cornerstones of good cybersecurity programs

Ensuring trust is why SOCs are necessities. This is true whether the SOC is internal or is provided by a third party, such as a managed security service provider (MSSP).

A SOC directs rapid detection and response to cyberthreats around the clock. The SOC is charged with monitoring and protecting many assets. Such as websites. Applications. Databases. Data centers and servers. Networks. Desktops. Other endpoints, such as mobile devices, and IoT entities, including the connected controls found in networked industrial equipment. The SOC assumes overall responsibility for monitoring, assessing, and defending all of these assets against cyberattacks.

A SOC team has many roles. While SOC teams vary, these roles typically include the following:

- **Cybersecurity analyst–**analyzes information from cyberdefense tools to assess events and mitigate threats
- **Incident responder–**investigates, analyzes, and responds to incidents
- **Forensic specialist–**identifies, collects, examines, and preserves evidence using analytical and investigative techniques
- **Cybersecurity auditor–**performs cybersecurity assessments of systems and networks, measures the effectiveness of the cybersecurity architecture against known vulnerabilities, and assesses compliance with regulatory requirements
- **Cybersecurity SOC manager–**manages the SOC personnel, budget, technology, and programs and interfaces with executive-level management, IT management, and the rest of the organization

Three trends have led to the rise of SOCs.

First is the need for centralization. A centralized real-time view of all digital assets and processes makes it possible to detect and fix problems whenever and wherever they occur. Centralization is crucial for IoT systems. The sheer numbers of devices and the likelihood that they are widely dispersed make local monitoring impractical.

Second is the need for an environment where skilled people with the right tools can react quickly and collaborate to remediate both system-wide and local problems.

The good news? Cybersecurity operations can provide benefits that can be measured.

Third is the need to blend cybersecurity tools and people who are skilled in using them with other critical IT functions and business operations. They must align with business objectives and compliance needs for a high-performing operation that is efficient and effective.

A dialog between the SOC and the rest of the enterprise has to be part of overall corporate risk management efforts. Cybersecurity and physical security must have strong voices at the table.

Technology readiness is important. But even as artificial intelligence assumes a larger role in enterprise operations, people still count. Having the right people to protect information will count the most.

Problematic enterprise preparedness

Bad actors are getting smarter and moving faster in stealing digital assets and processes, and they are doing it more often. The results have sometimes been devastating, and the problem will only get worse. A recent Forbes.com article predicts that cybercrime costs will reach US$2 trillion by 2019, up from $450 billion in 2016.[2]

The good news? Cybersecurity operations can provide benefits that can be measured. In addition, spending on protection against cyberthreats, in specific solutions and SOCs, is going up. Still, studies show that investments in protection and people are not keeping pace with the rising risk profile of digitized organizations.

There are several reasons for this problem:

1. **The rising complexity of the security landscape–**The typical enterprise has 30 to 40 different security vendor products in its network. Security teams generally are not 100 percent sure how these devices, solutions, and services work with one another. They also don't know whether there is overlap or, worse, gaps in protection. Or how much work needs to be done to integrate and correlate information coming in from different tools.

2. **The changing nature of cyberattacks–**There are new threats daily. These attacks are coming not just from individuals, but are increasingly led by well-funded organizations, including rogue groups and government-backed sources. The commercialization of hacking is resulting in exploits that are more frequent, better financed, more sophisticated, and more damaging.

   Even just a partial list of damage is sobering:

   - Espionage, including commercial, nation-state, and financial
   - Damage to brand or reputation
   - Damage to systems
   - Ransom demands

[2] Morgan, Steve; Forbes.com, "Cyber Crime Costs Projected to Reach $2 Trillion by 2019," January 2016.

The skills shortage is the biggest cybersecurity challenge the industry is facing.

- Fraud and identity theft
- Attacks on customers made by pivoting through the enterprise
- Stolen customer information and breaches of privacy
- Exploitation and takeover of network-attached resources
- Stolen intellectual property
- Theft of online resources or access credentials
- Gaming of stock prices

3. **The IoT–**It has created a wealth of new opportunities. But the rising number of connected devices provides cybercriminals with new and unforeseen ways to gain access to systems and information. In addition, end-to-end security is not part of legacy IoT systems.

4. **Cybersecurity risk is more than just outright attacks–**Digital organizations need to have a systemic way of evaluating attack risks. As all aspects of IT become more complex, new risks are brought to the table. Lost laptops or phones can result in substantial information breaches, for instance. Another set of issues for the cybersecurity team is unpatched systems or rollouts of new IT technologies not fully vetted for cybersecurity risk.

5. **The need to have experienced IT professionals with up-to-date tools and skills–**This is not just about better engineering and network infrastructure. It is also about having the best ability to monitor, identify, isolate, and proactively mitigate risk.

The skills shortage is the biggest cybersecurity challenge the industry is facing. Not only are there too few bodies to fill the cybersecurity jobs, but a series of research reports from Enterprise Strategy Group indicates that many currently employed cybersecurity professionals are overworked, not managing their careers proactively, and not receiving the proper training to stay ahead of increasingly dangerous threats.[3]

The list of the most in-demand cybersecurity skills is bound to change and grow as digital technologies advance and organizations adopt them. This fluidity makes ongoing training and certification just that much more critical for IT professionals who want to keep their skills current and their careers on track. Certifications in the right cybersecurity skills are one of the best ways for IT professionals to validate their expertise.

New skills for securing the digital enterprise

Right now, organizations face a perfect storm. Rising threats. A growing list of critical assets to protect. The need to invest in security operations. The widening shortage of security professionals with validated skills. Yet, as the

[3] Oltsik, Jon; Enterprise Strategy Group, "High Demand Cybersecurity Skills in 2017," December 2016.

The widening of the gap between supply and demand for these skills is a concern all the way up to enterprise boards.

need for protection has never been greater, the shortage of talent to mitigate risks has never been more severe. The widening of the gap between supply and demand for these skills is a concern all the way up to enterprise boards.

The severity of the situation is manifested in many ways, including the following:

1. **A shortage of talent in critical roles–**These roles include security architect, strategist, and platform, planning, and applications engineers. There are shortages in all these roles, but the security analyst position tops the lists of greatest current and future need.
2. **Higher costs to keep talent–**Staying current is costly. So is competing for scarce certified experts. The pay of certified security analysts starts at over $100,000 a year, and they have many prospects. Almost half of security professionals are solicited about new jobs weekly. And many of them run the risk of burnout from becoming overextended while their organization tries to scale. Turnover of skilled people is a major issue.
3. **The inability of existing staff to keep up with the evolving threat landscape–**Bad actors keep getting better at what they do. This is a leading incentive for keeping existing professionals current.

There has been a sharp rise in the opportunities and rewards for behaving maliciously. This explains the spread of cyber exploitation “how to” guides and illicitly obtained information on the dark web.

Hacking pays off. In some parts of the world, organizations and governments even compete with malicious organizations to hire the most skilled.

Certification demonstrates that you have the appropriate knowledge, skills, and abilities for a cybersecurity job. Cybersecurity skills can be complex and hard to demonstrate in a verbal job interview, especially to nontechnical hiring managers.

Technology alone cannot stem the rising tide of cyberthreats. There is no alternative to having enough people with the right skills.

Cybersecurity: Anything but routine

Security analysts are needed to fill the critical cybersecurity talent gap. As an article on Dark Reading reveals,[4] analysts’ days on the job are anything but predictable or dull. They really never know what will happen or how their workdays will unfold. The day could be slow until, suddenly, an emergency hits. Or the day could begin in a crisis that the analysts manage to contain.

Network security analysts spend their time on the job gathering the bits and bytes of network traffic to figure out what might be suspicious and what isn’t. Other analysts study network traffic behavior and other factors to decide what activity is routine and what is not.

[4] Yasin, Rutrell; Dark Reading, “A Day in the Life of a Security Analyst,” April 2016.

Closing the skills gap is a multipronged challenge. It must involve everyone in an enterprise, not just IT.

The first order of any analyst's day is the handover. The analyst arriving at work gets an update about the network situation from the analyst leaving work. There is a massive amount of traffic and information to watch, so they use tools to focus on priorities and highlight the most important activities.

Some workdays are reactive. There is a threat or an attack, and analysts spend their time and effort locating the intruder or vulnerability and fixing it. This means quick thinking and quick moves to stop cybercriminals in action.

During calmer days, analysts can become proactive detectives, hunting for weak spots in the network, devices, or applications and finding ways to shore up defenses. Analysts need to know their security tools inside out.

Stepping up to fill the cybersecurity skills gap

Closing the skills gap is a multipronged challenge. It must involve everyone in an enterprise, not just IT. Here are the focus points:

1. **Attracting, training, and keeping expertise–**This requirement applies to internal SOC operations as well as outsourced ones. As noted before, achieving this goal is not simple.

2. **Getting the right people–**Skills must be matched with current and planned security infrastructure and tool investments. People also need to be matched against what organizations need to protect: new types of assets, systems, or environments being deployed might require personnel with specialized knowledge or techniques. Given the number of security solutions and vendors serving enterprises, this challenge can be difficult to meet.

3. **Filling the talent pipeline–**This is not just an obligation for individual organizations. It should be a top industry-wide to-do item.

   We are tackling all aspects of the cybersecurity skills shortage. We have new and redesigned security certifications that aim to do the following:

   - Expand the talent pool
   - Provide development opportunities
   - Ensure job readiness
   - Meet the future challenges of network security

CCNA Cyber Ops

It's clear that cybersecurity operations job roles are in high demand. We have introduced the Cisco CCNA Cyber Ops certification to help meet this need.

The CCNA Cyber Ops certification focuses on the role of the security analyst working in a SOC. It introduces IT professionals to valuable skills that lay the foundations for a career in cybersecurity operations.

Earning CCNA Cyber Ops certification provides immediate value.

The Cyber Ops certification is a good starting point for a career in cybersecurity.

Cybersecurity analysts are in demand now across many industries to review the feed of telemetry information provided by a variety of sources and respond to suspicious activity. And analysts frequently move into increasingly responsible job roles in the SOC as they gain experience.

But the certification will continue to pay dividends in the future. The Cyber Ops certification is a good starting point for a career in cybersecurity. The variety of cybersecurity jobs continues to evolve, ranging from application developer, to law enforcement, to architect, to chief information security officer (CISO) for an organization. All these roles begin with a solid grounding in the fundamentals.

CCNA Security

The Cisco CCNA Security certification is another good starting point for a career in cybersecurity. It teaches all of the basics needed to begin a career building and administering a secure network infrastructure as an Associate-level member of a network security team.

This is an attractive option for those who are currently working on building network infrastructure and want to move into a security function, learning how to secure the networks and systems that they are building.

Whether you are interested in building the castle or guarding the castle, these certifications are two very good starting points for a career in cybersecurity.

CCNP Security

The Cisco CCNP Security certification builds further cybersecurity skills at the Professional level. It specifically corresponds to the job role of Cisco network security engineer, who is responsible for securing networks, devices, appliances, and applications. CCNP Security holders are frequently also in charge of choosing, deploying, supporting, and troubleshooting security products and services.

CCIE Security

The Cisco CCIE Security certification is designed to prepare IT personnel for evolving technologies at the Expert level. CCIE Security certification validates skills for managing advanced cybersecurity technologies and solving cybersecurity problems. Holders of this certification “build the castle,” solving problems and designing, deploying, and adapting cybersecurity technology to the widest range of cybersecurity problems facing a digital organization.

The CCIE Security certification has been revised to reflect the latest security technologies. Advanced threat protection. Advanced malware protection. Next-generation intrusion prevention systems (IPSs). Virtualization, automation, and information exchange. The aim is to make sure that candidates show knowledge of and skill in handling evolving technologies like network programmability, cloud, and IoT.

We are committed to making sure that SOCs have the best technology for the protection of digital assets and that they have the people with the right training to staff them.

Looking ahead

These certifications develop and validate the skills that ensure readiness to meet the challenges of cybersecurity risk management, now and in the future. They focus on skills that enable and support SOC maximized performance.

In an increasingly networked world, SOCs are being recognized as the digitized enterprise's front and best line of defense against bad actors within and outside of the organization.

We are committed to making sure that SOCs have the best technology for the protection of digital assets and that they have the people with the right training to staff them. We continue to advance our professional education offerings to help educate, train, and reskill the IT security professionals needed to close the cybersecurity skills gap.

What about you? Does a cybersecurity career intrigue you? Your job will never be the same from one day to the next. You will be chasing down and stopping the bad guys, the cybercriminals who wreak havoc on organizations and people's lives. Act now to start on your way to a challenging and rewarding cybersecurity role backed by the best training and certifications in the industry.

You can become a cybersecurity hero with Cisco's help.

Now is the time to act.

Are you in?

Get mobilized here:

- Cybersecurity training and certifications
- CCNA Cyber Ops certification
- CCNA Security certification
- CCNP Security certification
- CCIE Security certification revisions